



CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Ciudad Autónoma de Buenos Aires, 7 de Octubre del 2026

NOTA ACLARATORIA

ASUNTO: CONCURSO PRIVADO DE PRECIOS CONTRATACION DE SISTEMA DE IDENTIDAD
DIGITAL, AUTENTICACION Y FIRMA BIOMETRICA

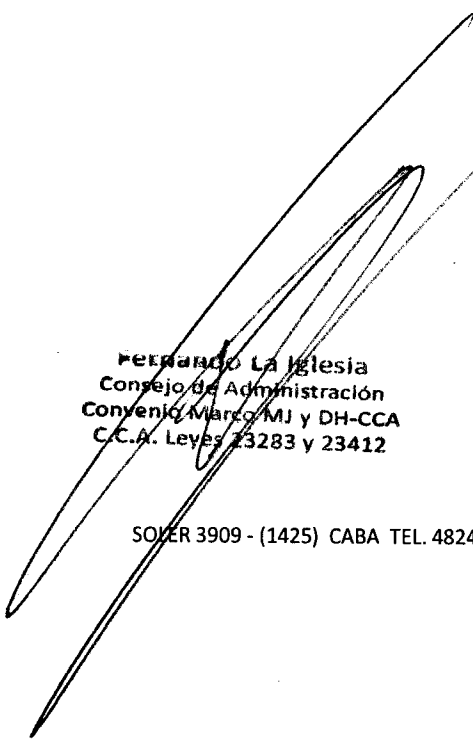
Estimados:

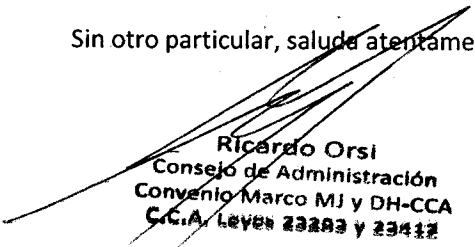
Por la presente, adjuntamos invitación para Concurso Privado de Precios.

A tal efecto, informamos que las ofertas se recibirán hasta el día 29 de Octubre a las 12 hs.

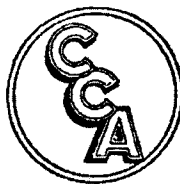
Por e-mail en la casilla de correo: melina@cca.org.ar

Sin otro particular, saluda atentamente.


Fernando La Iglesia
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412


Ricardo Orsi
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

SOLER 3909 - (1425) CABA TEL. 4824-7272 / 9505 / 9498 / 9489 FAX. 4822-7453 4823-1837



CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Ciudad Autónoma de Buenos Aires, 7 de Octubre del 2026

Señores

PROVEEDORES

Presente

**Concurso Privado de Precios Contratación de Sistema de identidad digital,
autenticación y firma biométrica**

EXPEDIENTE: ALC—3405/2026

De nuestra mayor consideración:

Nos dirigimos a Uds. a efectos de invitarlos a participar en la presentación de ofertas para la adquisición del siguiente elemento.

<u>ELEMENTOS</u>	<u>CANTIDAD</u> (LEER ESPECIFICACIONES TECNICAS)
Sistema de identidad digital, autenticación y firma biométrica	12 meses

Fecha Presentación de la Oferta: 29 de Octubre del año 2026.

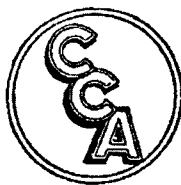
Hora: 12 hs.

Las ofertas deben presentarse con la documentación debidamente firmada, indicando en forma destacada nombre de la firma oferente y fecha del Concurso a realizarse.

Validez de presupuestos: 30 días

Precio: deben indicar el valor total con IVA INCLUIDO.

SOLER 3909 - (1425) BUENOS AIRES TEL. 4824-7272 / 9505 / 9498 / 9489 FAX. 822-7453 823-1837



CONVENIO MARCO MJ Y DH CAMARA DEL COMERCIO AUTOMOTOR- CCA
LEY 23.283 23.412

Firma, Aclaración, Teléfono, Mail, Domicilio, Cuit.

-Mantenimiento de la Oferta: 30 (treinta) días corridos a partir del día de apertura de sobres, renovables automáticamente salvo aviso en contrario con 10 (diez) días de anticipación.

Documentación a Presentar en el Acto de Apertura:

.- **Garantía de Oferta:** Pagaré simple por el 5 % del importe total de la oferta, suscripto por el Apoderado si supera el millón de pesos.

.- **Aceptación de Condiciones:** Se deberá adjuntar a la oferta, la presente invitación firmada por el apoderado de la compañía en todas sus hojas, aceptando las condiciones establecidas en la presente.

Adjudicación: Se adjudicará por renglón al oferente que presente menor precio y cumpla con las especificaciones técnicas. Según conformidad del Ministerio de Justicia y Derechos Humanos.

Forma de Pago: Contra entrega.

Enviar la documentación a las siguientes casillas de correo: melina@cca.org.ar

Sin más, saludamos Atte.

Fernando La Iglesia
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

Ricardo Orsi
Consejo de Administración
Convenio Marco MJ y DH-CCA
C.C.A. Leyes 23283 y 23412

MINISTERIO DE JUSTICIA

Sistema de Identidad Digital, Autenticación y Firma Biométrica

PLIEGO DE ESPECIFICACIONES TÉCNICAS

**SERVICIO DE PLATAFORMA DE IDENTIDAD DIGITAL DESCENTRALIZADA, ONBOARDING
DIGITAL DE PERSONAS FÍSICAS Y FIRMA BIOMÉTRICA DE DOCUMENTOS**

ÍNDICE

1. OBJETO Y ALCANCE	4
2. DETALLE DE LOS RENGLONES	5
3. ESPECIFICACIONES TÉCNICAS GENERALES	6
3.1. Modelo de prestación — Servicio SaaS con capacidad de migración a infraestructura del Contratante (on-premise / híbrido)	6
3.2. Arquitectura de identidad descentralizada (DID/VC) — requisitos mandatorios	8
3.3. Aclaración sobre el concepto passwordless y su relación con la biometría y las credenciales verificables	10
3.4. Plataforma biométrica	10
3.5. Proceso de onboarding omnicanal	12
3.6. Motor de análisis de riesgo conductual y autenticación continua — requisitos mandatorios	13
3.7. Portal de administración, auditoría y evidencia	14
3.8. Dimensionamiento del servicio	15
3.9. Acuerdo de nivel de servicio (SLA)	15
4. RENGLÓN N° 1 — PLATAFORMA SaaS DE ONBOARDING, AUTENTICACIÓN, BIOMETRÍA Y FIRMA DE DOCUMENTOS (CAPACIDAD PARA 1.000.000 DE USUARIOS)	16
4.1. Onboarding de personas físicas desde aplicación web	16
4.2. Firma biométrica de documentos — Formulario 01 (vehículos y motovehículos)	17
4.3. Identificación documental multinacional y verificación de identidad	20
4.4. Implementación, integración y puesta en producción (requisito técnico del proyecto)	22
5. RENGLÓN N° 2 — SERVICIO MENSUAL DE MESA DE AYUDA 7x24 (SERVICIOS TÉCNICOS, SOPORTE FUNCIONAL Y OPERATIVO A USUARIOS Y PROCESOS DE ONBOARDING, CON ESCALAMIENTO A LAS ÁREAS DEL MINISTERIO DE JUSTICIA)	24
5.1. Servicios técnicos y NOC 7x24x365	24
5.2. Soporte funcional y operativo a usuarios y procesos de onboarding	24
6. PLAZOS Y CONDICIONES DE EJECUCIÓN	26
6.1. Hitos contractuales y plazo de prestación	26
6.2. Cronograma de implementación del Renglón N° 1	26
6.3. Aprobación de entregables	26
7. REQUISITOS DE LA OFERTA	27
7.1. Contenido mínimo de la propuesta técnica	27
7.2. Equipo de trabajo mínimo	28
7.3. Antecedentes y experiencia mínima del oferente	28
7.4. Responsabilidad directa y personal afectado	30
7.5. Componentes tecnológicos y planilla de cumplimiento	30
7.6. Condiciones de admisibilidad	31
8. CRITERIOS DE EVALUACIÓN Y ADJUDICACIÓN	32
8.1. Tipo de cotización	32
8.2. Etapas de evaluación	32
8.3. Calificación Final de la Oferta (CFO)	32
8.4. Desempate	33
ANEXO I — MATRIZ DE EVALUACIÓN TÉCNICA	34
Resumen de componentes	34
Componente 1 — Antecedentes y experiencia del oferente (máximo 310 puntos)	34
Componente 2 — Equipo de trabajo (máximo 60 puntos)	36
Componente 3 — Propuesta técnica (máximo 130 puntos)	37
Planilla de puntaje	38
ANEXO II — PLANILLA DE ANTECEDENTES DEL OFERENTE	39
ANEXO III — DECLARACIÓN JURADA DE EXPERIENCIA DEL OFERENTE	40

1. OBJETO Y ALCANCE

El presente pliego tiene por objeto la contratación de un Servicio de Provisión de una Plataforma de Identidad Digital, de acuerdo con el modelo de Identidad Digital Omnicanal, para el Ministerio de Justicia como organismo beneficiario, destinada a los procesos de identificación, onboarding digital de personas físicas, verificación documental y firma biométrica para los diferentes servicios que implementa el citado organismo.

Desde su puesta a disposición, el servicio deberá brindar, como mínimo, las funcionalidades detalladas para el sistema RUNA y para el Sistema de Mediaciones Judiciales, pudiendo ampliarse su utilización a otros casos de uso del Ministerio de Justicia que surjan durante la vigencia del contrato, dentro de las prestaciones y del dimensionamiento contratados.

Modalidad de contratación. La presente contratación tiene por objeto la disponibilidad mensual del servicio y no la ejecución de un proyecto de implementación o desarrollo. El adjudicatario deberá poner a disposición del Ministerio de Justicia la plataforma plenamente operativa, con las funcionalidades e integraciones requeridas en el presente pliego, dentro del plazo máximo de VEINTE (20) días corridos contados desde la notificación de la Orden de Compra (apartado 6.1). A partir de la suscripción del Acta de Inicio del Servicio, ambos renglones se prestarán y abonarán como abono mensual, por cada mes de servicio efectivamente disponible.

La plataforma requerida deberá basarse en un modelo 100% Passwordless, lo cual significa que el 100% de los servicios no requerirán en ningún caso la creación de usuarios o contraseñas, ni la utilización de modelos tradicionales de segundo factor (OTP, SMS, correo electrónico, autenticadores de terceros), en ningún momento del ciclo de vida del usuario, incluyendo especialmente el proceso de onboarding inicial, los procesos posteriores de validación, autenticación y la firma de transacciones y documentos.

La identidad digital deberá basarse en estándares internacionales abiertos y deberá poder gestionarse a través de aplicaciones web provistas como parte de la solución, con soporte de Credenciales Verificables (VC) y modelos Passwordless que cumplan con los requisitos técnicos y de seguridad aquí detallados, ofreciendo la misma experiencia para el usuario en términos de usabilidad, acceso y seguridad en todos los canales.

El servicio deberá consumir Identificadores Digitales Descentralizados (DID) y Credenciales Verificables (VC) en conjunto con la biometría facial brindada por la plataforma, ofreciendo la misma experiencia para el usuario en términos de usabilidad y acceso, con una consideración especial de carácter mandatorio: en ningún caso el dispositivo físico podrá ser un punto de anclaje de las credenciales, de los identificadores o de la información, con el espíritu de que una persona que no posea un teléfono determinado en un momento determinado no lo necesite para sus interacciones con los sistemas alcanzados por el presente pliego.

La plataforma deberá tener la capacidad de integrarse con los actuales sistemas de gestión de identidades y accesos (IAM) del Ministerio de Justicia y soportar los protocolos OpenID Connect y SAML 2.0.

La solución y su operación deberán ajustarse al marco normativo de la República Argentina en materia de protección de datos personales, tratamiento de datos biométricos y validez jurídica de la firma electrónica y digital, incluyendo, de manera enunciativa y no taxativa: la Ley N° 25.326 de Protección de los Datos Personales y su reglamentación; las disposiciones y criterios de la Agencia de Acceso a la Información

Pública (AAIP) aplicables al tratamiento de datos biométricos y datos sensibles; y la Ley N° 25.506 de Firma Digital y su normativa complementaria. El oferente deberá describir de qué manera su arquitectura y sus controles satisfacen dichas exigencias, en particular respecto del tratamiento del dato biométrico como dato sensible, la minimización, disociación y no reidentificación de los datos personales conforme al modelo descripto en el presente pliego, y el encuadre de los mecanismos de firma ofrecidos dentro del régimen legal aplicable.

Estructura del pliego. El apartado 2 detalla los renglones que integran la contratación; el apartado 3 establece las especificaciones técnicas generales, aplicables a ambos renglones; los apartados 4 y 5 contienen las especificaciones particulares de los Renglones N° 1 y N° 2; el apartado 6 fija el plazo de puesta a disposición y las condiciones de prestación del servicio; el apartado 7 reúne la totalidad de los requisitos que debe cumplir y la documentación que debe presentar el oferente; y el apartado 8 establece los criterios de evaluación y adjudicación. Integran el presente pliego el Anexo I (Matriz de Evaluación Técnica), el Anexo II (Planilla de Antecedentes del Oferente), el Anexo III (Declaración Jurada de Experiencia) y el Anexo IV (Planilla de Cumplimiento Técnico).

2. DETALLE DE LOS RENGLONES

La presente contratación comprende los siguientes renglones, que deberán cotizarse en forma conjunta conforme al apartado 8.1:

RENLÓN	BIEN / SERVICIO	CANTIDAD	UNIDAD DE MEDIDA
1	Servicio mensual de Plataforma SaaS de Onboarding, autenticación, Biometría y Firma de Documentos con capacidad para 1 millón de usuarios registrados	12	MES
2	Servicio Mensual de Mesa de Ayuda 7x24 para los servicios técnicos, para el soporte funcional y operativo de los usuarios y para los procesos de onboarding con escalamiento a las áreas del Ministerio de Justicia	12	MES

3. ESPECIFICACIONES TÉCNICAS GENERALES

Las especificaciones del presente apartado son de aplicación a la totalidad de los servicios comprendidos en los Renglones N° 1 y N° 2.

3.1. Modelo de prestación — Servicio SaaS con capacidad de migración a infraestructura del Contratante (on-premise / híbrido)

El servicio deberá prestarse, en su etapa inicial, bajo un modelo SaaS (Software as a Service), gestionado y administrado por el oferente, que permita al Ministerio de Justicia consumir los servicios de identidad digital, verificaciones, validaciones, firmas y transacciones detallados en el presente pliego sin requerir la instalación de infraestructura propia.

No obstante lo anterior, cuando el Ministerio de Justicia así lo defina, el servicio deberá poder migrarse, total o parcialmente, a la infraestructura del Contratante, admitiéndose un modelo on-premise o un modelo híbrido. A tal efecto, el oferente deberá describir en su oferta la **arquitectura propuesta para dicha migración**, incluyendo los componentes involucrados, el empaquetado de la solución, las dependencias de infraestructura, los procedimientos de migración de datos y el plan de transición, de modo de garantizar la continuidad del servicio y la preservación de la evidencia y la trazabilidad durante el cambio de modelo de despliegue.

Se admitirá expresamente un **modelo híbrido**, siempre que se preserve que los **Datos de Identificación Personal (PII)** de los usuarios residan en la infraestructura del Contratante. En particular, se considerará válido y aceptable un esquema en el que los datos personales de los usuarios se alojen en los sistemas del Ministerio de Justicia y los componentes biométricos —templates y procesamiento biométrico— operen en la nube del oferente, en tanto dichos componentes **no contengan ni revelen PII** conforme al modelo de disociación descrito en el presente apartado. La viabilidad de esta separación es, precisamente, consecuencia del requisito de arquitectura biométrica non-PII exigido más adelante.

En cualquiera de los modelos de despliegue (SaaS, on-premise o híbrido), el Ministerio de Justicia deberá contar con un **tenant dedicado y aislado** para la administración de los servicios y de los datos de identidad que consume el sistema RUNA, con segregación lógica completa respecto de otros clientes de la plataforma.

Atento a que, en el modelo SaaS e híbrido, los componentes biométricos se prestarán desde la nube del oferente, éste deberá demostrar técnicamente cómo su solución y la arquitectura propuesta **no implican el manejo de Datos de Identificación Personal (PII) en los componentes biométricos**: el acceso a la plataforma biométrica no deberá revelar información alguna más allá de la fotografía y el template biométrico de una persona, sin exponer ningún dato que permita conocer quién es esa persona, a excepción del servicio que la consume. La demostración de este modelo será **condición de admisibilidad de la oferta técnica**.

Se requiere que la plataforma ofrezca un mínimo de cuatro (4) ambientes: Producción en alta disponibilidad, Pre-Producción, Testing y Desarrollo. El oferente deberá ofrecer un modelo de disaster recovery detallando su funcionamiento, con indicación expresa de los valores de RTO y RPO comprometidos.

Se deberá ofrecer un servicio de monitoreo 7x24x365 conforme al apartado 5.1 (Renglón N° 2) y garantizar una disponibilidad mínima del 99,95% para los servicios de producción, con independencia del modelo de despliegue adoptado.

3.1.1. Requerimientos técnicos de la plataforma

Los siguientes requerimientos técnicos aplican a la plataforma en cualquiera de sus modelos de despliegue (SaaS, on-premise o híbrido). Cuando el servicio opere sobre la infraestructura del Contratante, el oferente deberá acreditar el cumplimiento equivalente de cada requisito sobre dicha infraestructura.

Título del Requisito	Categoría	Descripción del Requisito
Arquitectura	Requisitos Técnicos	Debe contar con una infraestructura escalable para el motor biométrico (Kubernetes).
Arquitectura	Requisitos Técnicos	Debe contar con servicios en alta disponibilidad y multizona.
Arquitectura	Requisitos Técnicos	Debe contar con servicios que puedan escalar horizontalmente.
Arquitectura	Requisitos Técnicos	Debe contar con disponibilidad de 99,95% en los servicios de producción.
Arquitectura	Requisitos Técnicos	Debe contar con balanceadores de carga globales para los endpoints públicos principales.
Arquitectura	Requisitos Técnicos	La infraestructura deberá estar dimensionada y configurada de acuerdo a pruebas de estrés sobre el producto.
Portabilidad	Requisitos Técnicos	La solución deberá poder desplegarse sobre la infraestructura del Contratante (on-premise) o en un modelo híbrido, empaquetada en contenedores y sin dependencias de servicios propietarios de un único proveedor de nube que impidan su portabilidad.
Portabilidad	Requisitos Técnicos	El oferente deberá proveer la documentación de arquitectura, los artefactos de empaquetado (imágenes de contenedores y manifiestos de orquestación) y los procedimientos operativos necesarios para migrar el servicio a la infraestructura del Contratante cuando éste lo defina.
Residencia de Datos	Requisitos Técnicos	En el modelo híbrido, los Datos de Identificación Personal (PII) de los usuarios deberán residir en la infraestructura del Contratante; los componentes biométricos (templates y procesamiento) podrán operar en la nube del oferente en tanto no contengan ni revelen PII, conforme al presente apartado.
Despliegue	Requisitos	Debe contar con distintos ambientes para el pasaje

Título del Requisito	Categoría	Descripción del Requisito
	Técnicos	a producción de los cambios (Desarrollo, Testing, Pre-Producción y Producción).
Despliegue	Requisitos Técnicos	Debe contar con automatización del ciclo de vida del código de las aplicaciones (CI/CD) y escáneres de seguridad integrados al pipeline.
Base de Datos	Requisitos Técnicos	Las bases de datos deben contar con alta disponibilidad y backups automáticos.
Monitoreo	Requisitos Técnicos	Debe contar con alertas de infraestructura (uptime, umbrales de CPU y memoria) y observabilidad de métricas, trazas y logs.
Seguridad	Requisitos Técnicos	Debe contar con firewalls que restrinjan el tráfico externo e interno, permitiendo solo conexiones específicas con reglas detalladas para destinos, orígenes y puertos estrictamente necesarios.
Seguridad	Requisitos Técnicos	Debe contar con una política de red privada y cifrado HTTPS (TLS 1.2 o superior) en todos los endpoints expuestos a Internet.
Acceso	Requisitos Técnicos	Debe poder gestionar permisos de usuario del tipo IAM en recursos cloud y RBAC en Kubernetes, con accesos de administración independientes por ambiente mediante VPN.
Bóveda Digital	Requisitos Técnicos	Debe proveer una solución de gestión de secretos y claves criptográficas centralizada, en alta disponibilidad, con almacenamiento persistente, backups, rotación de claves y auditoría del ciclo de vida completo de las mismas.

3.2. Arquitectura de identidad descentralizada (DID/VC) — requisitos mandatorios

El sistema deberá cumplir con los modelos de SSI (Self-Sovereign Identity / Identidad Digital Autosoberana) y de Biometría Omnicanal de manera integrada. Se requiere que los oferentes demuestren la provisión de una solución totalmente integrada, es decir, donde la plataforma combine los servicios de Identidad, Credenciales Verificables y Biometría, sin resignar la omnicanalidad, y garantizando un modelo donde los usuarios no se vean obligados a disponer de un dispositivo móvil determinado para ejecutar la totalidad de las funcionalidades requeridas en los casos de uso.

En cuanto al modelo de gobernanza, se requiere que las propuestas técnicas sobre la gestión de la identidad y las VC estén basadas sobre la arquitectura del modelo desarrollado por la Fundación Trust Over IP y las recomendaciones de la W3C: Decentralized Identifiers (DIDs) v1.0 o superior (<https://www.w3.org/TR/did-core/>) y Verifiable Credentials Data Model v2.0 (<https://www.w3.org/TR/vc-data-model/>). El cumplimiento de este modelo es mandatorio y su incumplimiento será causal de rechazo de la oferta.

3.2.1. Identificadores Descentralizados (DID)

- Cada actor del sistema —personas físicas, operadores, servicios y componentes de la solución— deberá contar con un DID como identidad raíz, emitido y gestionado por la plataforma conforme al estándar W3C.
- La plataforma deberá proveer emisión y resolución de DIDs, con soporte para métodos estándar, incluyendo al menos did:key, did:peer y did:ethr.
- La clave privada asociada al DID del usuario no podrá ser almacenada en el dispositivo del usuario, con el objeto de garantizar el modelo omnicanal requerido. El oferente deberá detallar un modelo de almacenamiento y custodia de claves privadas independiente del dispositivo (por ejemplo, mediante una bóveda digital), cuyos costos de operación estarán incluidos en el servicio durante toda la vigencia del contrato.
- Las claves privadas no deberán ser exportables, ni residir en dispositivos finales, contenedores personales, tokens físicos o almacenes de certificados externos. Su uso deberá estar explícitamente autorizado mediante un factor biométrico que actuará como mecanismo de desbloqueo o habilitación criptográfica.

3.2.2. Credenciales Verificables (VC) y gestión nativa de roles y atributos

- Todos los roles, permisos y atributos de los usuarios del sistema deberán expresarse y gestionarse de forma nativa como Credenciales Verificables conforme al estándar W3C VC Data Model. No se aceptarán soluciones donde las VC constituyan una capa superficial de presentación sobre un modelo de roles basado en directorios tradicionales (Active Directory, LDAP u otros), debiendo el ciclo de vida completo de la credencial —emisión, presentación, verificación, suspensión y revocación— resolverse en la propia arquitectura descentralizada.
- La plataforma deberá contar con capacidad de revocación de credenciales y con capacidad de verificar credenciales emitidas por terceros, siempre que el emisor cumpla con los estándares correspondientes y haya sido homologado por el Ministerio de Justicia.
- La plataforma deberá soportar revelación selectiva de atributos y pruebas de conocimiento cero (Zero-Knowledge Proofs), permitiendo demostrar la posesión de un atributo sin revelar el resto del contenido de la credencial, conforme al estándar W3C Data Integrity — BBS Cryptosuites v1.0.
- De forma mandatoria, toda verificación de una presentación de VC deberá estar acompañada de la verificación biométrica del usuario provista por la presente plataforma; no será posible la verificación de una presentación de VC sin la correspondiente verificación biométrica del presentador. Esta definición se fundamenta en que el modelo de presentación de credenciales, si bien asegura la integridad de los datos presentados, resulta insuficiente por sí solo para asegurar la identidad de los agentes intervinientes en los eventos de presentación e intercambio.

3.2.3. Mensajería y transporte seguro — DIDComm

- El establecimiento de canales seguros entre las partes deberá realizarse mediante el protocolo DIDComm v2 (Decentralized Identity Communication) para el intercambio de mensajes de autenticación, credenciales, autorización y revocación. El soporte de DIDComm v2 es explícito y mandatorio; no se aceptarán soluciones que lo sustituyan por mecanismos genéricos de mensajería o transporte no conformes al protocolo.

- Deberá aplicarse cifrado de extremo a extremo y firmas digitales para proteger el transporte de credenciales verificables y los mensajes de autenticación, garantizando integridad, confidencialidad y no repudio.
- El oferente deberá describir en su propuesta técnica cómo su servicio resuelve el presente requisito. La experiencia en servicios productivos con DIDComm v2 se acreditará conforme al apartado 7.3 y se evaluará conforme al criterio 1.5 del Anexo I.

3.2.4. Registro de Datos Verificables (DID Registry)

El oferente deberá proponer un DID Registry (Registro de Datos Verificables) como ancla de confianza, ya sea mediante el uso de una red Blockchain, DLT u otro tipo de infraestructura equivalente. Se requiere el servicio de infraestructura necesario para el uso de la plataforma durante todo el período del contrato, contemplando el oferente los costos de utilización y mantenimiento considerando: a) la carga de trabajo prevista, b) la escalabilidad y c) el mantenimiento de tiempos de respuesta aceptables. El Registro será utilizado para respaldar la creación y gestión de los DID de las entidades involucradas y para proporcionar un registro inmutable de las operaciones clave del sistema: emisión, presentación y revocación de credenciales.

3.2.5. Solución nativa e integrada — condición de admisibilidad

Todos los casos de uso requeridos deben ser nativos y propios de la solución, por lo que la totalidad de los componentes de software deberán ser propios del oferente y encontrarse actualmente integrados y en producción sobre la plataforma ofertada.

No se aceptarán ofertas donde la plataforma de biometría y la plataforma que permite la emisión y administración de credenciales verificables sean de un tercero proveedor del oferente que presente la oferta. El incumplimiento de esta condición será causal de desestimación de la oferta técnica.

3.3. Aclaración sobre el concepto passwordless y su relación con la biometría y las credenciales verificables

El término Passwordless hace referencia a un enfoque de autenticación que elimina la necesidad de contraseñas tradicionales, reemplazándolas por mecanismos más seguros y resistentes a ataques como phishing o credential stuffing. En este contexto, la autenticación se basa en tecnologías como biometría, claves criptográficas, Identificadores Digitales Descentralizados (DID) y Credenciales Verificables (VC), junto con protocolos de comunicación segura como DIDComm.

El concepto 100% Passwordless en esta plataforma implica que en ninguna instancia del proceso se generen credenciales tradicionales (usuario/contraseña) ni se utilicen métodos heredados de autenticación (OTP, SMS, correo electrónico). No se considerará "passwordless" a los modelos que utilicen biometría solo como segundo factor o factor alternativo, ni a aquellos que requieran o dependan de PIN, contraseñas de recuperación u otros secretos compartidos como mecanismo habitual de autenticación. El acceso deberá realizarse exclusivamente mediante el modelo de identidad digital solicitado (credenciales verificables más autenticación biométrica fuerte), utilizando pruebas criptográficas de posesión asociadas a las VC emitidas al usuario, y no como complemento, respaldo o alternativa a credenciales tradicionales.

3.4. Plataforma biométrica

El oferente deberá ofrecer un modelo donde la plataforma de validación biométrica que preste los servicios de acceso a la plataforma de identidad digital opere como servicio en la nube del oferente, con la consideración mandatoria de que dichos servicios no mantengan información personal o datos de los usuarios que permitan, mediante el acceso a éstos, conocer quién es esa persona, manteniendo el modelo de interoperabilidad solicitado.

La plataforma de biometría deberá soportar en un mismo motor los modelos 1:1 y 1:n. No se aceptará que el servicio de autenticación biométrica dependa de dispositivos propietarios o de servicios provistos por terceros, tanto para los casos de acceso a aplicaciones web como para cualquier otro canal (por ejemplo, FaceID o biometría de huella nativa de los dispositivos, o motores biométricos propios del hardware), salvo como complemento de usabilidad definible por reglas de negocio, nunca como mecanismo principal de autenticación.

3.4.1. Detección de vida (Prueba de Vivacidad)

- Método: Prueba de Vivacidad pasiva (Passive Liveness), lo cual implica que el usuario no deberá efectuar ningún movimiento específico o gesto para la validación, tanto para aplicaciones web como PWAs.
- La prueba de vida deberá ser 100% por software y operar sobre cámaras estándar de dispositivos de consumo masivo (webcams, cámaras frontales de dispositivos móviles). No se aceptarán soluciones cuya detección de vida dependa de hardware especializado (cámaras binoculares, sensores infrarrojos, térmicos o de profundidad) para los canales web y móvil, por cuanto dichos modelos no entregan un puntaje de confianza auditable por transacción y limitan la omnicanalidad requerida.
- Deberá verificar usuarios con lentes de lectura y deberá poder interpretar distintas condiciones de iluminación.
- El sistema deberá tener la capacidad de verificar la vivacidad de una fotografía mediante la invocación a una API propia, por lo que se requiere poder verificar la vivacidad tanto desde el front-end como desde el back-end, de forma selectiva o complementaria.
- El servicio de detección de ataques de presentación deberá encontrarse conforme a la norma ISO/IEC 30107-3 (PAD), debiendo el oferente acreditar la evaluación de su tecnología en laboratorios independientes (por ejemplo, iBeta) al Nivel 2, con APCER y BPCER menores o iguales al 1%.

El oferente deberá garantizar los siguientes tiempos máximos, considerando dispositivos móviles de gama media con conectividad 4G o Internet asimétrica de al menos 100 Mbps de bajada, 40 Mbps de subida y latencia inferior a 12 ms:

- Validación en dispositivo móvil (mobile SDK): ≤ 2 segundos.
- Validación en una web desde un dispositivo móvil, incluyendo el proceso de Prueba de Vivacidad pasiva: ≤ 3 segundos.

3.4.2. Eficiencia del motor biométrico

Respecto de la eficiencia del motor biométrico, considerando los modelos aplicados por el NIST, el oferente deberá asegurar los siguientes puntajes mínimos en la evaluación NIST FRTE 1:1 (anteriormente denominada FRVT):

- VISA TAR (@FAR 1E-06): 99,60%.
- Mugshot TAR (@FAR 1E-05): 99,70%.
- Border TAR (@FAR 1E-06): 96,00%.

3.4.3. Requerimientos de eficiencia biométrica para modelos 1:n

La plataforma deberá soportar la validación 1:n donde n estará definida en 1.000.000 (un millón) de usuarios registrados, en consistencia con el dimensionamiento del presente servicio. El oferente deberá garantizar los siguientes tiempos máximos:

- Generación del template: ≤ 30 ms.
- Matching 1:n: ≤ 12 ms para $n = 1.000.000$.

3.4.4. Lectura de documentos de identidad

La plataforma deberá incluir, como parte del proceso de onboarding, el servicio de lectura del Documento Nacional de Identidad en sus versiones actualmente vigentes en la República Argentina. El servicio deberá poder realizar el escaneo de dichos documentos en un tiempo no mayor a cinco (5) segundos desde un dispositivo móvil de gama media, tanto desde una aplicación web como desde otros canales soportados. Deberá contar con un modelo de autocaptura que no implique que el usuario deba posicionar el dispositivo en un ángulo determinado, siendo el sistema capaz de leer el documento mientras se encuentre visible en pantalla, sin requerir la rotación del teléfono (lectura en modo portrait).

Deberá devolver, como mínimo, la siguiente información: número de documento, nombre, apellido, sexo, fecha de nacimiento, fecha de emisión, fecha de vencimiento, número de trámite, datos del PDF417, datos del MRZ, extracción de mini foto, comprobación de longitud del MRZ, verificación de la suma de comprobación del MRZ, dígito de verificación del número de documento, dígito de verificación de la fecha de caducidad, y comprobación de ambas caras del documento para validar la integridad de los datos.

3.4.5. Integración con RENAPER — parte del servicio

Es requerimiento del presente llamado que el oferente brinde, dentro de su servicio y sin costo adicional para el Ministerio de Justicia, la verificación de los documentos y datos de las personas contra la base de datos del Registro Nacional de las Personas (RENAPER), siendo el oferente responsable de entregar el servicio totalmente integrado. En virtud de ello, el oferente deberá acreditar su integración vigente y operativa con los servicios del RENAPER; no se aceptarán trámites en curso ni presentaciones temporales, debiendo el oferente acreditar que su servicio se encuentra activo al momento de la presentación de la oferta. El incumplimiento de esta condición será causal de desestimación de la oferta.

3.5. Proceso de onboarding omnicanal

El proceso inicial de onboarding deberá soportar dos métodos: i) la conexión de una identidad previamente creada, alimentándose de Credenciales Verificables emitidas por fuentes cuyo emisor cumpla con los mismos estándares definidos en el presente pliego y sea aceptado por el Ministerio de Justicia; y ii) la creación de la identidad a través de un proceso integrado al Documento Nacional de Identidad válido en la República Argentina, incluyendo la validación de datos contra el RENAPER conforme al apartado 3.4.5.

El proceso completo de onboarding —captura documental, extracción y validación de datos, prueba de vida pasiva, comparación biométrica 1:1 entre la selfie y la fotografía del documento, y validación contra

RENAPER— deberá ejecutarse íntegramente desde la aplicación web, sin requerir la descarga de aplicaciones, la creación de usuarios o contraseñas, ni la utilización de OTP, SMS o correos de verificación en ninguna de sus etapas.

La plataforma, luego del proceso de verificación, deberá crear la identidad digital mediante la asignación de un Identificador Digital Descentralizado (DID) y generar la o las Credenciales Verificables que registren su identidad, sus atributos y sus roles, quedando disponibles para las interacciones futuras y el consumo de los casos de uso, incluyendo su reutilización biométrica en actos posteriores sin repetir el proceso documental.

Para los casos de usuarios que posean una identidad digital en cumplimiento de la normativa y estándares W3C, solo se permitirá vincular su identidad cuando el emisor de dicha credencial haya implementado un proceso biométrico relacionado y homologado por el organismo. Para los demás casos, luego de la presentación de la credencial emitida en otro servicio estandarizado, el sistema requerirá obligatoriamente que el usuario realice el proceso de onboarding digital completo para luego verificar la VC que presenta.

3.6. Motor de análisis de riesgo conductual y autenticación continua — requisitos mandatorios

La plataforma deberá incorporar un motor de análisis de riesgo basado en el comportamiento que complemente —sin reemplazar— la verificación biométrica, los Identificadores Descentralizados (DID), las Credenciales Verificables (VC) y la detección de vida (PAD/liveness), aportando una capa de decisión inteligente que evalúe de forma continua el contexto que rodea a cada evento de identidad. El objeto de este requerimiento es asegurar que, más allá de una validación biométrica exitosa, la plataforma pueda determinar de manera auditable el nivel de confianza del contexto —dispositivo, ubicación, horario, canal y patrón de interacción— asociado a cada acto de onboarding, autenticación, presentación de credenciales y firma. El cumplimiento de los requisitos del presente apartado es de carácter mandatorio y su incumplimiento será causal de rechazo de la oferta.

3.6.1. Evaluación conductual en tiempo real

El motor deberá evaluar cada evento de identidad (onboarding, autenticación, presentación de VC y firma) contra el perfil de comportamiento histórico del propio usuario, considerando como mínimo dispositivo, geolocalización, horario, canal de acceso y patrón de interacción. La evaluación en línea deberá ejecutarse con una latencia máxima de 200 milisegundos (percentil 95) y sin introducir fricción para el usuario cuando el nivel de riesgo sea bajo, preservando la experiencia omnicanal requerida en el presente pliego.

3.6.2. Puntaje de riesgo graduado y explicable

El motor deberá producir, por cada evento, un puntaje de riesgo expresado en una escala numérica con niveles discretos de riesgo, acompañado de una descomposición auditable de los factores que motivaron dicho puntaje. Esta explicación deberá ser consultable por evento desde la consola de administración descrita en el apartado 3.7. No se aceptarán motores de riesgo de tipo "caja negra" que no permitan auditar, por transacción, los factores que determinaron el resultado, por resultar incompatibles con los requisitos de trazabilidad, auditoría y cumplimiento normativo del presente pliego.

3.6.3. Matriz de desafíos configurable (riesgo × canal × sensibilidad)

La plataforma deberá contar con una matriz de desafíos que determine la verificación adicional a solicitar en función de tres dimensiones combinadas: el nivel de riesgo detectado, el canal de acceso utilizado y la

sensibilidad de la acción solicitada. La matriz deberá contemplar desafíos graduales, desde la ausencia de fricción para operaciones de bajo riesgo hasta niveles crecientes que incluyan, como mínimo:

- re-verificación biométrica con prueba de vida pasiva;
- captura biométrica reforzada o verificación multimodal;
- verificación cruzada de canal (confirmación por un canal distinto al de la operación);
- doble control o esquema de cuatro ojos (aprobación de un segundo operador o responsable) para operaciones sensibles;
- bloqueo de la operación con escalamiento y generación de alerta.

La matriz deberá ser administrable por el Ministerio de Justicia desde una interfaz visual de configuración, sin requerir intervención de código, permitiendo definir reglas de excepción con prioridad sobre la matriz, horarios de seguridad reforzada, ajustes por canal y umbrales por tipo de acción. La plataforma deberá proveer plantillas base como punto de partida, personalizables por el organismo.

3.6.4. Retroalimentación con la plataforma biométrica

El motor deberá integrarse de forma bidireccional con la plataforma biométrica: deberá poder consumir los resultados de la detección de ataques de presentación (PAD) y de la prueba de vida, y —en función del riesgo evaluado— ordenar una nueva captura, una prueba de vida reforzada o la restricción de la operación dentro del mismo flujo, sin requerir un proceso separado a cargo del usuario.

3.6.5. Modo de observación previo a la aplicación efectiva

La plataforma deberá soportar un modo de observación en el que el motor evalúe los eventos y genere puntajes y decisiones en paralelo al flujo productivo, sin actuar sobre ellas, a efectos de calibración y validación. El oferente deberá describir las métricas de calibración y los criterios de confianza a partir de los cuales se habilitará la aplicación efectiva de las decisiones del motor.

3.7. Portal de administración, auditoría y evidencia

El módulo de administración deberá permitir gestionar de forma integrada las identidades, los eventos de validación, los servicios y las conexiones con el servicio biométrico, ofreciendo un modelo de administración de la lógica de negocios de la plataforma: seguridad, administración de políticas, administración de servicios y auditoría. La consola deberá ofrecer la capacidad de realizar análisis en tiempo real de la población enrolada, definir reglas y permisos, y vincularlos con eventos y servicios.

- Ver las transacciones realizadas por los usuarios (fecha, hora, canal, permisos, nivel de identidad) con el detalle de su consumo y eventos asociados.
- Administrar permisos de usuarios y sus credenciales, incluyendo la revocación y suspensión de las mismas.
- Analizar la tasa de veracidad antes de una decisión de aceptación o rechazo, contemplando factores adicionales a la biometría, como análisis de comportamiento y otros factores obtenidos por el sistema.
- Ver el tipo de biometría utilizada para cada verificación, los datos de referencia y el puntaje de calidad y de confianza de cada transacción, de forma auditable.

- Bloquear usuarios o dispositivos, y crear o vincular listas de vigilancia que permitan emitir alertas cuando un evento de validación registre a un usuario incluido en ellas, apoyándose en las capacidades 1:n de la plataforma.

Cada acto de identificación, validación, firma, aceptación y revocación deberá generar un registro inmutable de evidencia (bus de eventos y logs de auditoría) con digesto criptográfico y sello temporal, garantizando la trazabilidad procesal completa y la verificación independiente de la evidencia.

3.8. Dimensionamiento del servicio

La plataforma deberá proveer capacidad para un total de 1.000.000 (un millón) de usuarios registrados, considerándose Usuario a todo aquel que participe en los servicios de la plataforma independientemente de su rol y funcionalidades, e independientemente de que consuma uno o más servicios de la misma. El licenciamiento de la totalidad de los usuarios se encuentra incluido en el Renglón N° 1.

3.9. Acuerdo de nivel de servicio (SLA)

La solicitud de asistencia técnica podrá realizarse telefónicamente, por correo electrónico y/o portal de incidentes. Independientemente del canal utilizado, todas las solicitudes deberán ser registradas y gestionadas en un sistema con acceso web para garantizar trazabilidad completa. El horario de atención será de 7 días por 24 horas, los 365 días del año.

Las fallas se clasifican en Falla Mayor —cualquier falla de los componentes del servicio que cause pérdida del 25% o más de la capacidad de operación— y Falla Menor —cualquier falla no comprendida en el criterio anterior—.

Parámetro	Falla Mayor	Falla Menor
Tiempo máximo de respuesta a la solicitud de servicio	1 hora	4 horas
Tiempo máximo de resolución o mitigación	6 horas corridas	48 horas corridas
Disponibilidad mensual mínima del servicio de producción	99,95%	99,95%

El adjudicatario deberá presentar, por cada incidente, un informe en el sistema de gestión indicando la descripción de la tarea realizada para su resolución, y un informe mensual consolidado de disponibilidad, incidentes y cumplimiento de los presentes niveles de servicio.

4. RENGLÓN N° 1 — SERVICIO MENSUAL DE PLATAFORMA SaaS DE ONBOARDING, AUTENTICACIÓN, BIOMETRÍA Y FIRMA DE DOCUMENTOS (CAPACIDAD PARA 1.000.000 DE USUARIOS)

4.1. Onboarding de personas físicas desde aplicación web

Se requiere la provisión de un servicio de onboarding digital remoto de personas físicas para los distintos casos de uso, que deberá incluir mandatoriamente la integración y continuidad de los servicios del sistema RUNA y del Sistema de Mediaciones Judiciales. Para el caso de RUNA, el servicio deberá poder ejecutarse íntegramente desde una aplicación web responsive, sin requerir la descarga de aplicaciones móviles, la creación de usuarios y contraseñas, ni la utilización de OTP, SMS o correos de verificación en ninguna de sus etapas, conforme a lo establecido en el apartado 3 del presente pliego.

Para el Sistema de Mediaciones Judiciales, el servicio deberá incluir una solución web con las mismas características y, adicionalmente, una aplicación móvil de tipo billetera de identidad (wallet ID) que permita ejecutar los mismos procesos. El uso de la aplicación móvil será optativo para el usuario: no podrá constituirse en condición para acceder al servicio ni en punto de anclaje de las credenciales, de los identificadores o de la información, conforme al apartado 1.

El flujo de onboarding deberá comprender, como mínimo, las siguientes etapas:

- Inicio: creación de sesión e identificador de proceso trazable por cada acto de onboarding.
- Captura documental: anverso y reverso del Documento Nacional de Identidad, con validación de calidad en el cliente (foco, recorte, reflejos) y autocaptura conforme al apartado 3.4.4.
- Extracción de datos: lectura del PDF417, QR y del MRZ con OCR como respaldo, validación de checksums, fechas, dígitos verificadores y reglas del emisor, y comprobación cruzada de ambas caras del documento.
- Verificación de presencia: selfie con Prueba de Vivacidad pasiva (Passive Liveness) 100% por software, conforme al apartado 3.4.1.
- Verificación biométrica facial 1:1 entre la selfie y la fotografía del documento, con evaluación PAD.
- Validación de identidad contra el RENAPER, incluida como parte del servicio para el caso de documentos argentinos.
- Decisión: aprobación automática, derivación a revisión humana (back-office) o rechazo, según matriz de puntajes configurable.
- Emisión: creación del DID del usuario, emisión de las Credenciales Verificables firmadas correspondientes y disponibilización para su uso en todos los casos de uso para los que se consuma el servicio provisto por la plataforma.
- Evidencia: publicación de eventos al bus, persistencia en log de auditoría y digesto de evidencia con sello temporal por cada acto de identificación, validación, aceptación y revocación.

La identidad biométrica enrolada deberá ser persistida y gobernada por la plataforma para su reutilización en actos futuros del ciudadano dentro de la plataforma de manera interoperable con consentimiento explícito del usuario final, en sintonía con los modelos de conexión de identidades digitales —incluyendo la firma de documentos del presente renglón—, sin repetir el proceso documental, manteniendo el modelo non-PII descrito en el apartado 3.1.

El servicio deberá incluir el soporte de back-office para la gestión de las identidades de los usuarios: consulta y búsqueda, administración de estados (habilitado/inhabilitado), revisión manual de casos derivados, y auditoría de las decisiones adoptadas.

4.2. Firma biométrica de documentos — Formulario 01 (vehículos y motovehículos)

La plataforma deberá proveer un módulo de firma electrónica biométrica de documentos plenamente integrado al servicio de identidad digital descentralizada, basado en los DID y las VC de los firmantes conforme a los estándares internacionales vigentes, y no sustentado en infraestructuras de clave pública jerárquicas tradicionales. El caso de uso principal es la firma del Formulario 01 para la compraventa de vehículos y motovehículos del sistema RUNA, garantizando que dicha documentación sea firmada realmente por el individuo del que se quiere obtener la firma, utilizando los servicios biométricos de autenticación y aplicando firmas criptográficas y registro sobre una infraestructura de anclaje de confianza (Blockchain, DLT u otra infraestructura equivalente, conforme al apartado 3.2.4) para ofrecer un servicio seguro, rápido, en línea, trazable e inmutable.

La plataforma deberá permitir firmar documentos digitales a través del portal web con la identidad digital del firmante, o permitir la creación o conexión de dicha identidad dentro del propio proceso de firma (onboarding embebido en el flujo de firma), brindando la seguridad de que quien firmó el documento es quien dice ser.

4.2.1. Administración de documentos y plantillas

- Carga, administración y versionado de documentos PDF y de plantillas documentales, incluyendo la plantilla del Formulario 01 con sus campos de datos del trámite (identificación del vehículo o motovehículo, dominio, partes intervinientes y demás datos requeridos por el sistema RUNA).
- Generación de documentos a partir de plantillas con datos provistos por el sistema RUNA vía API, y carga directa de documentos PDF por parte de usuarios autorizados.
- Administración de estados del documento a lo largo de su ciclo de vida (borrador, enviado a firma, parcialmente firmado, firmado, rechazado, vencido, eliminado), con consulta y búsqueda de documentos categorizados entre recibidos y enviados.
- Cada firma deberá generar una nueva versión del documento, manteniendo un historial completo de versionado; cada versión deberá acumular y preservar los comprobantes criptográficos de las firmas anteriores, permitiendo la trazabilidad completa del proceso.

4.2.2. Inserción de campos y etiquetas de firma (tags)

- El módulo deberá permitir la definición e inserción de etiquetas o campos de firma (tags) sobre el documento, con posicionamiento visual sobre las páginas del PDF, tanto desde la interfaz web de administración como mediante marcadores embebidos en las plantillas.
- Los tipos de campo deberán incluir, como mínimo: firma, aclaración, fecha y campos de texto, con asignación individual a cada firmante del circuito.
- Para el Formulario 01, la plantilla deberá contemplar los campos de firma de todas las partes intervinientes en la operación (parte vendedora, parte compradora y, cuando corresponda, cónyuges, apoderados o representantes), cada uno vinculado a la identidad digital del firmante correspondiente.

4.2.3. Circuito de firmas y control de firmantes

- Para documentos con múltiples firmantes, la plataforma deberá permitir definir y administrar la prioridad y secuencia de los firmantes, determinando el orden obligatorio de ejecución de las firmas cuando el flujo lo requiera.
- El sistema deberá permitir invitar a firmantes que no posean identidad digital previa, resolviendo su onboarding completo dentro del mismo flujo de firma, con los mismos requisitos técnicos y de seguridad del apartado 4.1.
- Notificaciones a los firmantes de los requerimientos de firma pendientes, recordatorios, vencimientos configurables y posibilidad de rechazo con registro del motivo.
- Control de quién firmó: cada firma deberá quedar vinculada a la verificación biométrica del firmante ejecutada en el acto de la firma —con prueba de vida pasiva— y a su DID, registrando fecha y hora certificada, canal, y los datos de la transacción biométrica (puntaje de confianza auditable). No se admitirá la firma sin la verificación biométrica satisfactoria del firmante en el mismo acto.
- Auditoría completa de eventos, accesos y acciones sobre cada documento: visualizaciones, envíos, firmas, rechazos y cambios de estado, disponible para consulta y exportación.

4.2.4. Seguridad, inmutabilidad y custodia de los documentos

- Los documentos PDF a firmar deberán contener un texto considerado inmutable. La inmutabilidad deberá verificarse previo a cada proceso de firma y durante los procesos de validación, mediante el cálculo de un digesto criptográfico aplicado sobre el contenido del documento.
- Cualquier modificación posterior al proceso de firma deberá invalidar automáticamente la firma, sin requerir validaciones externas centralizadas.
- Las firmas deberán realizarse utilizando la clave privada asociada al DID del usuario, generada y gestionada dentro de la plataforma de identidad conforme al apartado 3.2.1: no exportable, sin residir en dispositivos finales, y con uso explícitamente autorizado mediante el factor biométrico.
- Las firmas deberán realizarse conforme al estándar W3C Data Integrity, empleando cryptosuites reconocidas para la firma sobre datos (por ejemplo, eddsa-2022 o ecdsa-2019), garantizando integridad criptográfica de los datos firmados, autenticidad del firmante y compatibilidad con modelos de identidad descentralizada. Las capacidades de revelación selectiva y pruebas de conocimiento cero (BBS Cryptosuites) aplicarán a la presentación de Credenciales Verificables conforme al apartado 3.2.2. No se aceptarán esquemas basados exclusivamente en estándares de firma electrónica asociados a PKI jerárquica tradicional.
- Custodia segura: los documentos, sus versiones históricas y los comprobantes criptográficos de firma deberán almacenarse en un esquema de almacenamiento cifrado, distribuido, redundante e interoperable, vinculado a la identidad de los intervinientes y auditado, que no dependa de repositorios centralizados únicos ni de infraestructuras propietarias cerradas.
- El oferente deberá describir en detalle el modelo de custodia, protección y uso controlado de las claves criptográficas, incluyendo controles contra uso indebido, replay y acceso no autorizado, así como el modelo de prueba de inmutabilidad y no repudio aplicado a los documentos firmados y los controles de seguridad de todo el ciclo de vida del documento.

4.2.5. Comprobante de firma y verificación

- El oferente deberá detallar los elementos de datos que componen el comprobante de firma, el cual deberá permitir verificar la inmutabilidad del documento, validar la autenticidad de cada firma y corroborar la identidad digital de cada firmante mediante sus DID y VC.
- El comprobante deberá ser verificable de forma independiente y descentralizada, sin requerir validaciones contra autoridades certificantes, listas de revocación centralizadas (CRL/OCSP) ni servicios de terceros propietarios.
- Deberá proveerse un módulo público de verificación que permita a cualquier interesado verificar un documento y sus firmas, relacionando la identidad digital de los firmantes con las firmas registradas.

4.2.6. Independencia de dispositivo

El proceso de firma deberá ser independiente del dispositivo utilizado por el usuario, y la identificación del firmante deberá sustentarse en su identidad digital descentralizada (DID/VC) y en la verificación biométrica ejecutada en el acto de la firma, y no en la posesión de un dispositivo, token o certificado. En consecuencia, no se aceptarán soluciones que: empleen certificados X.509 emitidos por autoridades certificantes jerárquicas como mecanismo de identificación del firmante o como único sustento probatorio de la firma; dependan de certificados, autenticadores o claves vinculadas a un dispositivo específico; utilicen tokens físicos predeterminados como mecanismo principal de identificación; se basen en modelos de identidad federada tradicionales (correo electrónico, usuario/contraseña); o requieran la integración con proveedores tradicionales de identidad (IdP) como condición de operación. Lo anterior no obsta a que, cuando la normativa registral aplicable así lo exija, el documento firmado pueda complementarse con una firma digital en los términos de la Ley N° 25.506 y su reglamentación; en tal caso, el token criptográfico correspondiente actuará como factor adicional de peso normativo, sin sustituir ni reemplazar el modelo de identificación biométrica descentralizada requerido en el presente pliego.

4.2.7. Portal web del servicio de firma

La plataforma deberá contar con un portal web que ofrezca, como mínimo, los siguientes módulos:

- Usuario actual: onboarding, ingreso y egreso, y perfil con los datos del usuario y el registro de los documentos firmados y su estado.
- Gestión de organizaciones: acceso exclusivo para el personal que defina el Ministerio de Justicia, con consulta y búsqueda de organizaciones registradas, administración de estados (habilitado/inhabilitado) y consulta de documentos subidos y firmas realizadas.
- Gestión de usuarios: para los administradores designados, con consulta y búsqueda de usuarios, administración de estados e invitación de usuarios.
- Documentos: consulta y búsqueda, administración de estados, consulta de las firmas realizadas y visualización del documento.
- Verificación: verificación de los documentos y sus firmas conforme al apartado 4.2.5.

La operación deberá estar disponible tanto desde la interfaz web de administración como mediante APIs documentadas para la integración con el sistema RUNA, incluyendo la creación de documentos, la definición de circuitos de firma, la consulta de estados y la descarga de documentos y comprobantes.

4.3. Identificación documental multinacional y verificación de identidad

4.3.1. Contexto y alcance

El Sistema Nacional de Mediaciones requiere identificar de forma fehaciente a personas físicas provenientes de múltiples jurisdicciones, con una experiencia uniforme, evidencia auditable y trazabilidad procesal de cada acto de identificación. La heterogeneidad documental de la región —pasaportes, cédulas físicas y digitales, DNI electrónicos, cédulas de extranjero y documentos provisorios— hace inviable un onboarding artesanal y exige una capa de confianza tecnológica capaz de absorber esa diversidad sin transferirla al usuario final.

4.3.2. Alcance funcional

- Onboarding remoto de personas físicas, con captura documental y verificación de presencia mediante Prueba de Vivacidad pasiva (Passive Liveness), conforme al apartado 3.4.1.
- Reconocimiento OCR / MRZ / PDF417 según el tipo documental y país emisor.
- Verificación biométrica facial 1:1 (selfie contra la fotografía del documento), con evaluación PAD.
- Verificación biométrica 1:n contra los usuarios previamente enrolados en la plataforma.
- Verificación biométrica 1:n contra listas de vigilancia en tiempo real, conforme al apartado 3.7.
- Enrolamiento de la identidad biométrica del usuario, reutilizable en actos futuros del expediente sin repetir el proceso documental.
- Emisión y custodia de Credenciales Verificables (W3C VC) ancladas a los Identificadores Descentralizados (DID) del usuario y del Ministerio de Justicia como emisor, incluyendo como mínimo las credenciales de documento verificado y de identidad biométrica.
- Registro inmutable de evidencia (bus de eventos y logs de auditoría) por cada acto de identificación, validación, aceptación y revocación, con digesto criptográfico y sello temporal.
- Integración con los flujos de firma electrónica de documentos del apartado 4.2 (firma biométrica de documentos).
- Soporte de back-office para la gestión de las identidades de los usuarios y la revisión humana de los casos derivados por la matriz de puntajes.

4.3.3. Alcance documental

El servicio deberá contemplar el procesamiento de los siguientes documentos, por país:

#	País	Documento(s) incluidos
1	Argentina	Documento Nacional de Identidad (DNI) y Pasaporte argentino
2	Bolivia	Cédula de Identidad, Cédula de Identidad de Extranjero y Pasaporte boliviano
3	Brasil	Carteira de Identidade Nacional (CIN) —física o digital— y Pasaporte brasileño
4	Chile	Cédula de Identidad, Pasaporte chileno y Cédula de Identidad para Extranjeros
5	Colombia	Pasaporte colombiano, Cédula de Identidad y Cédula de extranjería
6	Costa Rica	Pasaporte costarricense

#	País	Documento(s) incluidos
7	Cuba	Carné de Identidad y Documento de Identidad Provisional
8	Ecuador	Pasaporte ecuatoriano y Cédula de identidad
9	El Salvador	Pasaporte salvadoreño
10	Guatemala	Pasaporte guatemalteco
11	Haití	Pasaporte haitiano
12	Honduras	Pasaporte hondureño
13	México	Pasaporte mexicano
14	Nicaragua	Pasaporte nicaragüense
15	Panamá	Pasaporte panameño
16	Paraguay	Cédula de Identidad (nacionales y extranjeros) y Pasaporte paraguayo (Pasaporte Policial)
17	Perú	Documento Nacional de Identidad (DNI/DNle) y Pasaporte electrónico
18	Rep. Dominicana	Pasaporte dominicano
19	Uruguay	Documento Nacional de Identidad y Pasaporte uruguayo
20	Venezuela	Pasaporte venezolano
21	Estados Unidos	Pasaporte estadounidense

Total: TREINTA Y CUATRO (34) tipos documentales: VEINTE (20) pasaportes y CATORCE (14) documentos nacionales de identidad, cédulas y documentos provisorios, con sus variantes.

4.3.4. Estrategia técnica de extracción documental

Cada tipo documental requiere un pipeline de procesamiento propio. La estrategia técnica deberá priorizar las vías deterministas (PDF417, MRZ) por su precisión natural, reservando el OCR para campos no estandarizados o como respaldo:

- Pasaportes (20 países): MRZ ICAO 9303 como fuente primaria; OCR del MRZ y de la VIZ (zona de inspección visual); validación de checksums; consulta a tablas de patrones por país emisor.
- Documentos con PDF417 (Colombia, Argentina, Chile, Uruguay): lectura del código de barras como vía principal, con OCR como respaldo.
- Documentos con MRZ (Perú DNle, Brasil CIN digital, Paraguay): extracción de MRZ ICAO 9303 con OCR especializado.
- Documentos solo OCR (Cuba, casos provisorios): pipeline OCR con anclas estructurales y validación cruzada de campos.

4.3.5. Control de calidad del servicio

El adjudicatario deberá mantener, como parte de la operación mensual del servicio, un esquema de control de calidad que combine, como mínimo, cinco capas: pruebas unitarias por componente, pruebas de integración entre módulos de la plataforma, pruebas funcionales end-to-end por país, pruebas de presentación biométrica conforme ISO/IEC 30107-3, y pruebas no funcionales (performance, seguridad y observabilidad), ejecutadas en pipelines de CI/CD y en un ambiente de pre-producción espejado del productivo. La evidencia de su ejecución sobre la configuración del Ministerio de Justicia se presentará para

la verificación de disponibilidad del apartado 6.2, y los siguientes niveles de cobertura deberán mantenerse en cada release durante toda la vigencia del contrato:

Nivel	Alcance	Cobertura objetivo	Responsable
Unitario	Cada componente y regla país-específica	≥ 85% de líneas	Desarrollo
Integración	Biometría ↔ Identidad ↔ Captura ↔ Emisor VC	100% de los flujos	QA + Desarrollo
E2E funcional	Por tipo documental: 1 caso feliz + 5 casos negativos	Mínimo 204 escenarios (34 × 6)	QA
Biométrico PAD	ISO/IEC 30107-3	APCER/BPCER ≤ 1%	Especialista ML + QA
Performance	Carga: 200 onboardings concurrentes	P95 ≤ 6 s extremo a extremo	DevSecOps
Seguridad	Pentest funcional del módulo	Cero hallazgos críticos	Especialista de Seguridad
Observabilidad	Trazas y eventos en bus	100% de eventos auditables	DevSecOps + QA

Pruebas de regresión por país: para cada tipo documental se deberá mantener un conjunto de muestras de regresión (mínimo 20 por tipo) que se ejecute en cada release. Cualquier modificación de modelos o pipelines requerirá validación contra esa batería antes del despliegue productivo.

4.4. Puesta a disposición del servicio y prestaciones incluidas en el abono

El servicio del Renglón N° 1 se contrata sobre una plataforma ya desarrollada y en producción, que el adjudicatario deberá poner a disposición del Ministerio de Justicia, configurada e integrada, dentro del plazo del apartado 6.1. Las tareas necesarias para ello forman parte de la prestación y se encuentran incluidas en el abono mensual; no constituyen un proyecto de implementación ni serán objeto de cotización, certificación o pago por separado.

4.4.1. Prestaciones incluidas en el abono mensual

El abono mensual del Renglón N° 1 incluye, sin costo adicional ni cargos por única vez, como mínimo, las siguientes prestaciones:

- Configuración y parametrización del tenant dedicado del Ministerio de Justicia y de los cuatro (4) ambientes del apartado 3.1.
- Integración operativa con el sistema RUNA y con el Sistema de Mediaciones Judiciales mediante APIs documentadas, y con los sistemas de gestión de identidades y accesos del organismo mediante OpenID Connect y SAML 2.0.
- Verificación de identidad contra el RENAPER, conforme al apartado 3.4.5.
- Front-end web de onboarding y firma, componentes SDK para su embebido en los canales del organismo y aplicación móvil de tipo wallet ID, conforme al apartado 4.1.
- Plantilla del Formulario 01 y configuración de los circuitos de firma requeridos por el sistema RUNA, conforme al apartado 4.2.

- Pipelines de procesamiento documental para los tipos documentales del apartado 4.3.3 y su actualización ante nuevas versiones de los documentos.
- Mecanismos de seguridad lógica, control de acceso, integridad de la información, auditoría y trazabilidad de operaciones.
- Documentación técnica, funcional y operativa del servicio, y manuales para administradores y usuarios.
- Capacitación a los administradores y operadores designados por el Ministerio de Justicia.
- Actualizaciones, mantenimiento correctivo y mantenimiento evolutivo de la plataforma durante toda la vigencia del contrato.
- Anclaje de los DID en el DID Registry propuesto (apartado 3.2.4), incluyendo la totalidad de los costos de transacción asociados (gas u otros), durante toda la vigencia del contrato.

4.4.2. Forma de cotización

El oferente deberá cotizar exclusivamente un abono mensual por renglón. No se admitirán cotizaciones de horas hombre, cargos de implementación, configuración, licencias iniciales ni otros conceptos por única vez; cualquier tarea necesaria para la puesta a disposición y la operación del servicio se considerará incluida en el abono mensual.

4.4.3. Plataforma en producción — condición de admisibilidad

Atento al plazo de puesta a disposición del apartado 6.1, el servicio deberá prestarse sobre una plataforma que se encuentre en producción a la fecha de apertura de las ofertas, con sus componentes, la integración con el RENAPER y la capacidad requerida ya operativos. No se admitirán ofertas que condicionen la disponibilidad del servicio a desarrollos futuros o a la ejecución de un proyecto previo.

5. RENGLÓN N° 2 — SERVICIO MENSUAL DE MESA DE AYUDA 7x24 (SERVICIOS TÉCNICOS, SOPORTE FUNCIONAL Y OPERATIVO A USUARIOS Y PROCESOS DE ONBOARDING, CON ESCALAMIENTO A LAS ÁREAS DEL MINISTERIO DE JUSTICIA)

5.1. Servicios técnicos y NOC 7x24x365

El oferente deberá proveer un servicio de NOC (Network Operations Center) y soporte técnico de la plataforma en modalidad 7x24x365, que garantice la operación continua de todos los servicios del presente pliego y el cumplimiento de los niveles de servicio establecidos en el apartado 3.9.

5.1.1. Alcance del servicio

- Monitoreo proactivo 7x24x365 de la infraestructura, las aplicaciones y los servicios (disponibilidad, latencia, tasas de error, umbrales de CPU y memoria, colas y eventos), con alertamiento automático y tableros de observabilidad de métricas, trazas y logs.
- Gestión de incidentes conforme a la clasificación de fallas y a los tiempos de respuesta y resolución del SLA (apartado 3.9), con registro y trazabilidad completa en un sistema de gestión con acceso web para el organismo.
- Gestión de problemas, cambios y releases, incluyendo ventanas de mantenimiento coordinadas con el organismo y comunicación previa de todo cambio con impacto potencial en el servicio.
- Mantenimiento correctivo y evolutivo de la plataforma. El oferente deberá detallar el alcance del mantenimiento evolutivo ofrecido, incluyendo la actualización continua de los modelos biométricos y de los pipelines documentales ante nuevas versiones de los documentos soportados.
- Gestión de la seguridad operativa: aplicación de parches, gestión de vulnerabilidades, respuesta ante incidentes de seguridad y notificación al organismo conforme a la normativa aplicable.
- Ejecución periódica de las pruebas del plan de disaster recovery y reporte de sus resultados.

5.1.2. Informes

El adjudicatario deberá presentar informes mensuales de nivel de servicio incluyendo: disponibilidad de cada servicio, incidentes registrados con su clasificación, tiempos de respuesta y resolución, cumplimiento del SLA, capacidad y proyección de crecimiento, y acciones de mejora continua. Asimismo, deberá presentar un informe por cada incidente mayor, con análisis de causa raíz y plan de acción.

5.1.3. Responsable técnico y canales de comunicación

El responsable técnico del adjudicatario será el encargado de recibir y comunicar las órdenes y pedidos del área supervisora del Ministerio de Justicia y de resolver situaciones de urgencia durante la ejecución del contrato en el menor tiempo posible. El adjudicatario deberá informar los canales de comunicación: teléfono fijo, teléfono celular, correo electrónico y portal de incidentes.

5.2. Soporte funcional y operativo a usuarios y procesos de onboarding

El oferente deberá proveer un servicio integral de mesa de ayuda destinado a los ciudadanos usuarios del sistema RUNA y del Sistema de Mediaciones Judiciales, en modalidad 7x24x365, en idioma español, que brinde asistencia completa sobre los procesos de onboarding, verificación de identidad y firma de documentos objeto del presente pliego.

5.2.1. Alcance del servicio

- Atención omnicanal: canal telefónico, chat web integrado a la aplicación de onboarding y firma, y correo electrónico. Se valorará la disponibilidad de canales adicionales de mensajería.
- Soporte de primer nivel: asistencia al ciudadano durante el proceso de onboarding (captura documental, prueba de vida, errores de validación), la firma de documentos y la verificación de los mismos, incluyendo la contención y resolución de las consultas más frecuentes.
- Soporte de segundo nivel: gestión de casos derivados que requieran revisión de back-office sobre la identidad del ciudadano (casos derivados por la matriz de puntajes, actualización de datos, revocación y re-emisión de credenciales), con escalamiento a los servicios técnicos y NOC del apartado 5.1 cuando el caso corresponda a una falla del servicio.
- Registro de la totalidad de los contactos en una herramienta de gestión de tickets con trazabilidad completa, categorización de motivos y vinculación con el identificador de proceso del ciudadano, garantizando la protección de los datos personales conforme a la normativa aplicable.
- Elaboración y mantenimiento de la base de conocimiento, guías de autoayuda y respuestas frecuentes para los ciudadanos, en coordinación con el organismo.

5.2.2. Niveles de servicio de la mesa de ayuda

Indicador	Valor objetivo
Tiempo máximo de espera en canal telefónico (percentil 80)	≤ 60 segundos
Tiempo máximo de primera respuesta en chat	≤ 2 minutos
Tiempo máximo de primera respuesta por correo electrónico	≤ 4 horas
Resolución en primer contacto (FCR)	≥ 75%
Tasa de abandono en canal telefónico	≤ 5%
Satisfacción del ciudadano (CSAT)	≥ 85%

5.2.3. Informes

El adjudicatario deberá presentar informes mensuales con los volúmenes de atención por canal, los motivos de contacto categorizados, el cumplimiento de los indicadores del apartado 5.2.2, y las propuestas de mejora sobre la experiencia del ciudadano derivadas del análisis de los contactos.

6. PUESTA A DISPOSICIÓN Y CONDICIONES DE PRESTACIÓN

6.1. Plazo de puesta a disposición y plazo de prestación

El adjudicatario deberá poner a disposición del Ministerio de Justicia los servicios de ambos renglones, plenamente operativos, dentro de un plazo máximo de VEINTE (20) días corridos contados desde la notificación de la Orden de Compra, conforme a las siguientes condiciones:

- a) **Servicio disponible.** Se considerará que el servicio está disponible cuando se encuentren operativos la totalidad de los componentes de la lista de verificación del apartado 6.2.
- b) **Acta de Inicio del Servicio.** Comunicada la disponibilidad por el adjudicatario y verificada por el Ministerio de Justicia conforme al apartado 6.2, las partes suscribirán el Acta de Inicio del Servicio. A partir de dicha fecha se computará el plazo de prestación de DOCE (12) meses de los Renglones N° 1 y N° 2.
- c) **Facturación.** Los servicios de ambos renglones se facturarán como abono mensual, por mes vencido, previa conformidad del área supervisora sobre la disponibilidad del servicio y el cumplimiento de los niveles de servicio. El primer período se facturará en proporción a los días transcurridos desde la suscripción del Acta de Inicio del Servicio.

6.2. Verificación de disponibilidad del servicio

Dentro de los CINCO (5) días hábiles de comunicada la disponibilidad, el Ministerio de Justicia verificará el funcionamiento de los componentes que se detallan a continuación. Las observaciones que formule deberán ser subsanadas por el adjudicatario dentro de los CINCO (5) días corridos, sin que ello extienda el plazo máximo del apartado 6.1:

N°	Componente y condición de disponibilidad	Verificado (Sí/No)
1	PLATAFORMA Y AMBIENTES Tenant dedicado y los cuatro (4) ambientes del apartado 3.1 operativos, con monitoreo 7x24 activo.	
2	ONBOARDING Y FIRMA — SISTEMA RUNA Onboarding web (apartado 4.1) y firma del Formulario 01 (apartado 4.2) operativos e integrados al sistema RUNA, con verificación contra el RENAPER.	
3	IDENTIFICACIÓN DOCUMENTAL — SISTEMA DE MEDIACIONES Onboarding web y aplicación móvil de tipo wallet ID operativos para el Sistema de Mediaciones Judiciales, con los tipos documentales del apartado 4.3.3.	
4	ADMINISTRACIÓN, AUDITORÍA Y RIESGO Portal de administración (apartado 3.7) operativo con accesos para los administradores del organismo, y motor de riesgo (apartado 3.6) en modo de observación.	
5	SOPORTE Y MESA DE AYUDA NOC y mesa de ayuda 7x24 del Renglón N° 2 operativos, con los canales de contacto informados al organismo.	

6.3. Incumplimiento del plazo de puesta a disposición

La demora en la puesta a disposición del servicio dará lugar a la aplicación de las penalidades previstas en el Pliego de Bases y Condiciones Particulares y en la normativa de contrataciones vigente. Durante la vigencia del contrato, la indisponibilidad del servicio por debajo de los niveles comprometidos en el apartado 3.9 dará lugar a un descuento en el abono mensual proporcional al tiempo de indisponibilidad excedente.

7. REQUISITOS DE LA OFERTA

El presente apartado reúne la totalidad de los requisitos que el oferente deberá cumplir y de la documentación que deberá presentar con su oferta. Las especificaciones de los apartados 1 a 6 que exigen al oferente describir, detallar, acreditar o demostrar un aspecto de su solución se entienden comprendidas en el contenido mínimo de la propuesta técnica del apartado 7.1.

El cumplimiento de estos requisitos se verificará con carácter previo a la evaluación técnica: sólo las ofertas que cumplan con la totalidad de ellos serán evaluadas conforme a la Matriz de Evaluación Técnica del Anexo I.

7.1. Contenido mínimo de la propuesta técnica

A fin de acreditar su capacidad técnica, tecnológica y profesional, el oferente deberá presentar una propuesta técnica que contenga, como mínimo, los siguientes elementos, identificados con el apartado del pliego al que corresponden:

- a) **Descripción de la solución.** Descripción y alcance de la solución propuesta de acuerdo con las especificaciones de los apartados 3, 4 y 5, con el mayor grado de detalle respecto de arquitectura, diseño, seguridad, resguardo de la información, tecnologías utilizadas, documentación, performance y procedimientos de prueba.
- b) **Arquitectura y modelo de despliegue (apartado 3.1).** Arquitectura del servicio SaaS; arquitectura propuesta para la migración a un modelo on-premise o híbrido; demostración técnica de que los componentes biométricos no manejan Datos de Identificación Personal (PII); modelo de disaster recovery con los valores de RTO y RPO comprometidos; y grado de cumplimiento de cada requerimiento del apartado 3.1.1.
- c) **Identidad descentralizada (apartado 3.2).** Modelo de almacenamiento y custodia de claves privadas independiente del dispositivo (apartado 3.2.1); esquema de DIDComm v2 provisto por el servicio (apartado 3.2.3); y DID Registry propuesto, con los costos de utilización y mantenimiento incluidos (apartado 3.2.4).
- d) **Plataforma biométrica (apartado 3.4).** Certificado o informe de evaluación conforme a la norma ISO/IEC 30107-3, Nivel 2, emitido por laboratorio independiente (apartado 3.4.1); resultados publicados en la evaluación NIST FRTE 1:1 que acrediten los valores mínimos exigidos (apartado 3.4.2); y acreditación de la integración vigente y operativa con el RENAPER (apartado 3.4.5).
- e) **Motor de análisis de riesgo (apartado 3.6).** Descripción del motor y de la matriz de desafíos, y métricas de calibración y criterios de habilitación del modo de observación (apartado 3.6.5).
- f) **Firma de documentos (apartado 4.2).** Modelo de custodia y uso controlado de claves y de prueba de inmutabilidad y no repudio (apartado 4.2.4), y detalle de los elementos de datos del comprobante de firma (apartado 4.2.5).
- g) **Marco normativo (apartado 1).** Descripción del modo en que la arquitectura y los controles de la solución satisfacen el marco normativo en materia de datos personales, datos biométricos y firma electrónica y digital.

- h) **Plan de puesta a disposición (apartado 6).** Descripción de las actividades que el oferente ejecutará entre la notificación de la Orden de Compra y la disponibilidad del servicio, con su secuencia, duración y responsables, que garantice el cumplimiento del plazo máximo del apartado 6.1.
- i) **Plataforma en producción (apartado 4.4.3).** Descripción de la infraestructura productiva sobre la que se prestará el servicio, de las integraciones que ya se encuentran operativas y de la capacidad instalada disponible para el dimensionamiento del apartado 3.8.
- j) **Control de calidad del servicio (apartado 4.3.5).**
- k) **Modelo de operación y soporte (apartado 5).** Metodología de reporte y resolución de incidencias críticas, mecanismos de seguimiento y control de las actividades, alcance del mantenimiento evolutivo ofrecido (apartado 5.1.1) y dimensionamiento de la mesa de ayuda.

7.2. Equipo mínimo afectado al servicio

El oferente deberá proponer un equipo de trabajo que comprenda, como mínimo, los siguientes perfiles, con las responsabilidades y la experiencia mínima que se indican:

- **Responsable Técnico del Servicio:** responsable de la operación técnica de la plataforma, de la gestión de actualizaciones y errores del servicio y del cumplimiento de las especificaciones técnicas del presente pliego. Deberá acreditar al menos CINCO (5) años de experiencia profesional en servicios de Identidad Digital, biometría y onboarding digital, y CINCO (5) años liderando equipos técnicos.
- **Gerente del Servicio:** responsable de la puesta a disposición del servicio en el plazo del apartado 6.1, del cumplimiento de los niveles de servicio y de la relación con el organismo. Deberá acreditar al menos DOS (2) años de experiencia en la gestión de servicios de tecnología en el sector público que incluyan biometría e Identidad Digital.
- **Líder de Arquitectura de Servicios:** responsable de la arquitectura del servicio y de las integraciones con los sistemas y aplicaciones del organismo. Deberá acreditar al menos CINCO (5) años de experiencia en proyectos de transformación digital e integración de soluciones tecnológicas que impliquen sistemas de biometría o Identidad Digital, y experiencia directa y comprobable en el liderazgo exitoso de al menos DOS (2) proyectos con la solución propuesta por el oferente.

Para cada integrante del equipo, el oferente deberá presentar:

- Apellido/s y nombre/s, tipo y número de documento de identidad, correo electrónico y teléfono celular de contacto.
- Currículum vitae en idioma español, con la descripción de proyectos, tecnologías, metodologías, clientes, fechas y certificaciones que hacen a la calificación (títulos, publicaciones y acreditaciones).
- Constancia del vínculo laboral o contractual con el oferente, conforme al apartado 7.4.

Los integrantes propuestos no podrán ser reemplazados durante la ejecución del contrato sin la conformidad previa del Ministerio de Justicia, y el reemplazante deberá acreditar una experiencia igual o superior a la exigida al integrante reemplazado.

7.3. Antecedentes y experiencia mínima del oferente

7.3.1. Definiciones

A los efectos del presente pliego y de la Matriz de Evaluación Técnica (Anexo I), se entenderá por:

- a) **Experiencia propia:** aquella en la que el oferente ha sido el prestador directo del servicio, con responsabilidad técnica y operativa sobre el servicio, utilizando la misma solución y productos ofertados, así como recursos propios para su operación, mantenimiento y evolución. No se computará la experiencia de terceros, fabricantes o vendedores de la solución, aun cuando exista entre ellos y el oferente un vínculo de distribución, representación o partner.
- b) **Prestación:** servicio provisto a un cliente (organismo o empresa) determinado, en virtud de un contrato, orden de compra u otro instrumento. Los distintos casos de uso o servicios provistos a un mismo cliente se computarán como una única prestación.
- c) **Producción:** servicio operativo con usuarios finales y transacciones reales a la fecha de apertura de las ofertas, excluyéndose expresamente pilotos, pruebas controladas o pruebas de concepto (POC).
- d) **Misma plataforma:** la plataforma, el motor biométrico y la tecnología de identidad descentralizada ofertados en la presente contratación.

7.3.2. Requisitos mínimos de experiencia

El oferente deberá acreditar experiencia propia, en producción, en:

- R-1 **Identidad Digital Descentralizada (IDD):** al menos UNA (1) prestación en un organismo público de la República Argentina, provista desde la misma plataforma ofertada bajo modelo SaaS, cuyo alcance comprenda tanto a empleados del organismo como a ciudadanos o usuarios externos, y cuya arquitectura incluya DID, Credenciales Verificables y DIDComm conforme a los estándares W3C y a las especificaciones del presente pliego, con el mismo motor biométrico ofertado y un modelo 100% passwordless (sin generación de nombres de usuario ni contraseñas y sin segundos factores tales como OTP, PIN o validación de correo electrónico).
- R-2 **Firma de documentos:** al menos UNA (1) prestación en un organismo público de la República Argentina que utilice el mismo modelo de firma de documentos requerido en el apartado 4.2, en la que las firmas puedan ejecutarse indistintamente desde un navegador web o una aplicación móvil.
- R-3 **Organismos de seguridad:** al menos UNA (1) prestación en un organismo público de seguridad, nacional o extranjero, de identidad digital integrada a modelos de SSO, que utilice la plataforma en los procesos de adquisición de usuarios y de validación de la identidad en reemplazo de OTP, correo electrónico, SMS u otro segundo factor distinto de la verificación facial biométrica, aplicada en entornos omnicanales (como mínimo, aplicación móvil y página web) y provista por el oferente en forma directa bajo modalidad SaaS.

Una misma prestación podrá acreditar más de un requisito cuando reúna las condiciones de cada uno de ellos.

7.3.3. Acreditación de los antecedentes

Los antecedentes se acreditarán mediante:

- Declaración jurada conforme al modelo del Anexo III.
- Planilla de Antecedentes conforme al modelo del Anexo II, indicando para cada prestación los requisitos del apartado 7.3.2 y los criterios del Anexo I que acredita, y la ubicación de la documentación respaldatoria en la oferta.

- Certificación o constancia emitida por el cliente, suscripta por autoridad competente, que indique como mínimo: denominación del cliente, objeto y alcance del servicio, plataforma utilizada, fecha de puesta en producción, estado vigente, cantidad de usuarios registrados, funcionalidades provistas y rol del oferente; acompañada de copia del contrato u orden de compra, cuando corresponda.

Los antecedentes deberán corresponder exclusivamente al oferente como prestador directo de los servicios, acreditar prestaciones reales, productivas y verificables, y guardar coherencia con el alcance y las capacidades de la solución propuesta. No se considerarán válidos los antecedentes que no reflejen una participación directa y comprobable del oferente. El Ministerio de Justicia podrá verificar la información presentada ante los clientes declarados y requerir las aclaraciones que estime necesarias.

7.4. Responsabilidad directa y personal afectado

El oferente deberá asumir en forma **directa, integral y exclusiva** la responsabilidad por la provisión, la puesta a disposición, la operación, el soporte y el mantenimiento de la solución objeto del presente pliego durante toda la vigencia del contrato. Los servicios ofertados deberán ser **prestados directamente por el oferente**, sin delegación, intermediación ni transferencia de responsabilidades técnicas, operativas o contractuales a terceros.

El personal afectado a la prestación, la operación y el soporte deberá:

- Tener **presencia física en el territorio de la República Argentina** durante toda la vigencia del contrato.
- Pertenecer a la nómina del oferente o contar con vínculo contractual vigente con éste por un plazo no menor a la duración del contrato.

Por razones de seguridad de la información y de acceso a sistemas sensibles del organismo, los servicios comprendidos en el presente pliego deberán ser ejecutados por personal bajo responsabilidad directa del oferente.

7.5. Componentes tecnológicos y planilla de cumplimiento

Para cada componente tecnológico será considerado un requisito mínimo la inclusión en la oferta de la identificación del bien/producto que permita verificar con claridad cuál es la provisión ofertada. La omisión de su presentación no será susceptible de subsanación posterior. Deberá entenderse por “identificación del bien”: marca, modelo y/o cualquier otro elemento distintivo del bien/producto. Adicionalmente, se deberán adjuntar folletos técnicos y/o manuales necesarios para una adecuada evaluación de las tecnologías ofrecidas. El oferente deberá dejar expresa constancia respecto del grado de cumplimiento de cada uno de los puntos incluidos en los requisitos técnicos mínimos que deben cumplir los componentes. No se admitirá especificar simplemente “según pliego” como identificación del producto y/o servicio digital ofrecido. La ausencia de información requerida podrá determinar su desestimación. Dicha documentación deberá presentarse en idioma español, o con la correspondiente traducción, la que correrá por cuenta del oferente y será realizada por un traductor matriculado y deberá estar debidamente legalizada conforme artículo 28 del Reglamento de Procedimientos Administrativos aprobado por el Decreto 1759/1972 (T.O. 2017).

El grado de cumplimiento de cada apartado se consignará en la Planilla de Cumplimiento Técnico del Anexo IV, indicando la página o folio de la oferta en que se describe o acredita.

7.6. Condiciones de admisibilidad

Sin perjuicio de las demás causales previstas en la normativa aplicable, será causal de desestimación de la oferta:

- a) el incumplimiento del modelo de gobernanza y de los estándares W3C y Trust Over IP exigidos (apartado 3.2);
- b) el ofrecimiento de una plataforma biométrica o de emisión y administración de credenciales verificables de un tercero, o de componentes que no sean nativos, propios e integrados en producción (apartado 3.2.5);
- c) la falta de demostración técnica del modelo non-PII de los componentes biométricos (apartado 3.1);
- d) la falta de acreditación de la integración vigente y operativa con el RENAPER (apartado 3.4.5);
- e) el incumplimiento de los requisitos mandatorios del motor de análisis de riesgo (apartado 3.6);
- f) la falta de acreditación de una plataforma en producción que permita poner a disposición el servicio dentro del plazo del apartado 6.1 (apartado 4.4.3);
- g) el incumplimiento de los requisitos mínimos de equipo de trabajo (apartado 7.2) o de antecedentes del oferente (apartado 7.3);
- h) las inconsistencias entre los antecedentes presentados y el rol asumido por el oferente, o la ejecución indirecta de los servicios (apartado 7.4);
- i) la omisión de la identificación de los componentes tecnológicos ofertados (apartado 7.5), que no será susceptible de subsanación posterior;
- j) la obtención de un puntaje técnico inferior al mínimo previsto en el apartado 8.2.

La falta o insuficiencia de la documentación respaldatoria podrá ser subsanada en los términos y con los alcances previstos en la normativa aplicable, siempre que ello no implique alterar la oferta ni acreditar antecedentes posteriores a la fecha de apertura.

8. CRITERIOS DE EVALUACIÓN Y ADJUDICACIÓN

8.1. Tipo de cotización

Total	X
Por Renglón	
Por grupo de Renglones	

Siendo el tipo de cotización Total, los oferentes deberán cotizar la totalidad de los renglones del presente pliego y la cantidad total de cada uno de ellos. La falta de cotización de al menos uno de los renglones será causal de desestimación de la totalidad de la oferta.

8.2. Etapas de evaluación

La evaluación de las ofertas se realizará en las siguientes etapas sucesivas:

- Admisibilidad:** verificación del cumplimiento de los requisitos del apartado 7.
- Evaluación técnica:** asignación a cada oferta admisible de un puntaje técnico (PT), conforme a la Matriz de Evaluación Técnica del Anexo I, cuyo puntaje máximo es de QUINIENTOS (500) puntos.
- Preselección:** quedarán preseleccionadas las ofertas que obtengan un PT igual o superior a TRESCIENTOS SETENTA Y CINCO (375) puntos, equivalente al SETENTA Y CINCO POR CIENTO (75%) del puntaje máximo. Las ofertas que no alcancen dicho puntaje serán desestimadas.
- Evaluación económica y calificación final:** sobre las ofertas preseleccionadas se determinará la Calificación Final de la Oferta (CFO) conforme al apartado 8.3.

8.3. Calificación Final de la Oferta (CFO)

La adjudicación recaerá en la oferta más conveniente para el organismo, entendiéndose por tal aquella que, cumpliendo con la totalidad de los requisitos establecidos en los pliegos que rigen el procedimiento, obtenga la mayor CFO, determinada de la siguiente forma:

- Oferta Técnica de Referencia (OTR):** el mayor PT obtenido entre las ofertas preseleccionadas.
- Oferta Económica de Referencia (OER):** el menor precio total cotizado entre las ofertas preseleccionadas.
- Evaluación Técnica Final de la Oferta (ETFO):** $ETFO = PT \text{ de la oferta} / OTR$.
- Evaluación Económica Final de la Oferta (EEFO):** $EEFO = OER / \text{precio total de la oferta}$.
- Calificación Final de la Oferta (CFO):**

$$CFO = (0,75 \times ETFO) + (0,25 \times EEFO)$$

Se entenderá por precio total de la oferta la suma de los abonos mensuales cotizados para los Renglones N° 1 y N° 2, multiplicada por DOCE (12) meses. La ETFO y la EEFO asumen valores entre cero (0) y uno (1), correspondiendo el valor uno (1) a la oferta de mayor puntaje técnico y a la de menor precio, respectivamente. Los valores de ETFO, EEFO y CFO se calcularán con TRES (3) decimales.

8.4. Desempate

En caso de igualdad de CFO entre dos o más ofertas, se invitará a los respectivos oferentes para que formulen la mejora de precios.

Si un oferente no se presentara, se considerará que mantiene su propuesta original.

De subsistir el empate, se procederá al sorteo público de las ofertas empatadas. Para ello se deberá fijar día, hora y lugar del sorteo público y comunicarse a los oferentes llamados a desempatar. El sorteo se realizará en presencia de los interesados, si asistieran, y se labrará el acta correspondiente.

ANEXO I — MATRIZ DE EVALUACIÓN TÉCNICA

La evaluación técnica de las ofertas admisibles se realizará conforme a la presente Matriz. El puntaje técnico máximo es de **QUINIENTOS (500) puntos** y el mínimo requerido para la preselección es el previsto en el apartado 8.2.

Reglas de aplicación:

- Los tramos de un mismo criterio no son acumulativos: se asignará el puntaje del tramo de mayor nivel efectivamente acreditado. Los subcriterios del criterio 1.5 se puntúan en forma independiente y acumulativa.
- Los criterios de antecedentes (1.1 a 1.5) se evalúan sobre prestaciones que cumplan las definiciones del apartado 7.3.1 y se acrediten conforme al apartado 7.3.3. Una misma prestación puede computarse en más de un criterio.
- El primer tramo de los criterios 1.1, 1.3, 1.4, 2.1, 2.2 y 2.3 corresponde al requisito mínimo de los apartados 7.2 y 7.3. Las ofertas que no lo acrediten no son admisibles y no se evalúan.
- Los criterios del componente 3 se evalúan en dos niveles: **Cumple**, cuando la propuesta desarrolla la totalidad de los contenidos mínimos del apartado 7.1 correspondientes al criterio; y **Supera**, cuando además reúne la totalidad de las condiciones indicadas en el criterio.

Resumen de componentes

Componente de evaluación	Puntaje máximo
1. Antecedentes y experiencia del oferente	310
2. Equipo de trabajo	60
3. Propuesta técnica	130
TOTAL	500

Componente 1 — Antecedentes y experiencia del oferente (máximo 310 puntos)

1.1. Prestaciones de Identidad Digital Descentralizada con la plataforma ofertada		
Cantidad de prestaciones propias en producción, en la República Argentina o en el exterior, en organismos públicos o empresas, que reúnan las características técnicas del requisito R-1: misma plataforma bajo modelo SaaS; DID, VC y DIDComm conforme a W3C; mismo motor biométrico; modelo 100% passwordless. Deben incluir la prestación que acredita el requisito R-1. Requisito mínimo relacionado: R-1 (apartado 7.3.2).		
Tramo	Puntaje	Asignado
Una (1) prestación (requisito mínimo)	40	
Dos (2) a cuatro (4) prestaciones	70	
Cinco (5) o más prestaciones	100	

1.2. Escala de la prestación

Cantidad de usuarios registrados en una prestación computada en el criterio 1.1, en producción en la República Argentina, en la que el onboarding, la validación de identidad y la firma de transacciones o documentos se realicen tanto desde aplicaciones web (sin requerir la instalación de aplicaciones nativas) como desde aplicaciones móviles, con detección de vida pasiva en ambos canales y con la identidad digital como factor único de autenticación (no opcional, alternativo ni segundo factor), garantizando trazabilidad y no repudio.

Tramo	Puntaje	Asignado
Una (1) prestación con 500.000 o más usuarios registrados	20	
Una (1) prestación con 1.000.000 o más usuarios registrados	50	
Dos (2) o más prestaciones con 1.000.000 o más usuarios registrados	80	

1.3. Firma electrónica biométrica de documentos

Cantidad de prestaciones propias en producción del modelo de firma de documentos del apartado 4.2 (firma basada en DID/VC con verificación biométrica en el acto de la firma), ejecutable desde navegador web y desde aplicación móvil. Deben incluir la prestación que acredita el requisito R-2.

Requisito mínimo relacionado: R-2 (apartado 7.3.2).

Tramo	Puntaje	Asignado
Una (1) prestación (requisito mínimo)	20	
Dos (2) o más prestaciones	40	

1.4. Identidad digital en organismos de seguridad

Cantidad de prestaciones propias en producción en organismos públicos de seguridad, nacionales o extranjeros, con las características del requisito R-3. Deben incluir la prestación que acredita dicho requisito.

Requisito mínimo relacionado: R-3 (apartado 7.3.2).

Tramo	Puntaje	Asignado
Una (1) prestación (requisito mínimo)	20	
Dos (2) o más prestaciones	40	

1.5. Capacidades específicas acreditadas en producción

Cada subcriterio se asigna en forma independiente y acumulativa cuando la capacidad se acredite en prestaciones computadas en el criterio 1.1.

Tramo	Puntaje	Asignado
a) Canales seguros DID-to-DID mediante DIDComm v2 para autenticación, presentación de credenciales, autorización y revocación, con cifrado de extremo a extremo, en DOS (2) o más prestaciones	15	
b) Verificación de Credenciales Verificables emitidas por terceros con revelación selectiva y pruebas de conocimiento cero, conforme a W3C Data Integrity — BBS Cryptosuites	15	
c) Custodia de las claves privadas del DID independiente del dispositivo, con habilitación biométrica, en una prestación de 1.000.000 o más usuarios	20	

Componente 2 — Equipo de trabajo (máximo 60 puntos)

2.1. Responsable Técnico del Servicio

Experiencia del Responsable Técnico del Servicio propuesto, con vínculo directo y verificable con el oferente (apartado 7.4).

Requisito mínimo relacionado: apartado 7.2.

Tramo	Puntaje	Asignado
Cinco (5) a nueve (9) años de experiencia en servicios de Identidad Digital, biometría y onboarding digital, y cinco (5) o más años liderando equipos (requisito mínimo)	10	
Diez (10) o más años de experiencia y responsabilidad acreditada sobre la operación en producción de la solución ofertada	20	

2.2. Líder de Arquitectura de Servicios

Experiencia del Líder de Arquitectura de Servicios propuesto, con vínculo directo y verificable con el oferente (apartado 7.4).

Requisito mínimo relacionado: apartado 7.2.

Tramo	Puntaje	Asignado
Cinco (5) o más años de experiencia y dos (2) a cuatro (4) proyectos liderados con la solución ofertada (requisito mínimo)	10	
Cinco (5) o más años de experiencia, título de grado en Ingeniería o disciplina afín y cinco (5) o más proyectos liderados con la solución ofertada, de alcance superior a 500.000 usuarios	20	

2.3. Gerente del Servicio

Experiencia del Gerente del Servicio propuesto en la gestión de servicios de tecnología en el sector público que incluyan biometría e Identidad Digital.

Requisito mínimo relacionado: apartado 7.2.

Tramo	Puntaje	Asignado
Dos (2) a cuatro (4) años de experiencia (requisito mínimo)	10	
Cinco (5) o más años de experiencia	20	

Componente 3 — Propuesta técnica (máximo 130 puntos)

3.1. Arquitectura y solución técnica

Contenidos mínimos: apartado 7.1, incisos a) a g). **Supera:** incluye diagramas de arquitectura lógica y de despliegue para los modelos SaaS, híbrido y on-premise; matriz de trazabilidad entre requisitos del pliego y componentes de la solución; y diagrama de flujos de datos con la clasificación de cada dato que evidencie el modelo non-PII.

Tramo	Puntaje	Asignado
Cumple	20	
Supera	40	

3.2. Puesta a disposición y plataforma en producción

Contenidos mínimos: apartado 7.1, incisos h) e i). **Supera:** compromete la disponibilidad del servicio en un plazo igual o inferior a DIEZ (10) días corridos desde la notificación de la Orden de Compra; acredita en producción la totalidad de las prestaciones del apartado 4.4.1 que no dependen de sistemas propios del organismo; e incluye un plan de contingencia ante demoras atribuibles a terceros.

Tramo	Puntaje	Asignado
Cumple	15	
Supera	30	

3.3. Niveles de servicio y control de calidad

Contenidos mínimos: apartado 7.1, inciso j). **Supera:** compromete una disponibilidad mensual superior al 99,95% o tiempos de resolución inferiores a los del apartado 3.9; provee al organismo un tablero en línea de seguimiento de los niveles de servicio; y ejecuta pruebas de regresión automatizadas por tipo documental en cada release.

Tramo	Puntaje	Asignado
Cumple	15	
Supera	30	

3.4. Modelo de operación, soporte y mesa de ayuda

Contenidos mínimos: apartado 7.1, inciso k). **Supera:** incluye procedimientos de escalamiento con tiempos por nivel, herramientas de gestión identificadas, dimensionamiento de la mesa de ayuda por turno y plan de mejora continua con indicadores.

Tramo	Puntaje	Asignado
Cumple	15	
Supera	30	

Planilla de puntaje

Criterio	Descripción	Máximo	Asignado
1.1	Prestaciones IDD con la plataforma ofertada	100	
1.2	Escala de la prestación	80	
1.3	Firma electrónica biométrica de documentos	40	
1.4	Identidad digital en organismos de seguridad	40	
1.5	Capacidades específicas en producción	50	
2.1	Responsable Técnico del Servicio	20	
2.2	Líder de Arquitectura de Servicios	20	
2.3	Gerente del Servicio	20	
3.1	Arquitectura y solución técnica	40	
3.2	Puesta a disposición y plataforma en producción	30	
3.3	Niveles de servicio y control de calidad	30	
3.4	Operación, soporte y mesa de ayuda	30	
	PUNTAJE TÉCNICO TOTAL (PT)	500	

ANEXO II — PLANILLA DE ANTECEDENTES DEL OFERENTE

El oferente deberá consignar cada prestación invocada, los requisitos (apartado 7.3.2) y criterios (Anexo I) que acredita y la ubicación de la documentación respaldatoria en la oferta. Podrán agregarse las filas que resulten necesarias.

Oferente: CUIT:

N°	Cliente / organismo y país	Puesta en producción y usuarios registrados	Funcionalidades acreditadas	Requisitos y criterios que acredita	Documentación (folio)
1					
2					
3					
4					
5					
6					
7					
8					

Firma: Aclaración: Carácter:

ANEXO III — DECLARACIÓN JURADA DE EXPERIENCIA DEL OFERENTE

Lugar y fecha:

Procedimiento N°: Expediente N°:

Quien suscribe, ..., DNI N°, en su carácter de de la firma, CUIT N°, con facultades suficientes para este acto, **DECLARA BAJO JURAMENTO** que:

1. La firma que representa posee experiencia propia, en los términos del apartado 7.3.1 del Pliego de Especificaciones Técnicas, en proyectos tecnológicos de Identidad Digital con servicios de SSO passwordless, control de accesos a servicios lógicos y entornos físicos, modelos de onboarding digital omnicanal y validación de usuarios mediante biometría facial 1:1 y 1:n, en ecosistemas de Identidad Digital Descentralizada bajo los estándares de la W3C exigidos en el pliego.
2. Las prestaciones detalladas en la Planilla de Antecedentes (Anexo II) fueron provistas en forma directa por el oferente, con la misma plataforma, motor biométrico y tecnología ofertados, y se encuentran en producción a la fecha de apertura de las ofertas.
3. La información y la documentación presentadas son veraces y completas, y autoriza al Ministerio de Justicia a verificarlas ante los clientes declarados.
4. El personal propuesto pertenece a la nómina del oferente o cuenta con vínculo contractual vigente con éste por un plazo no menor a la duración del contrato, y tendrá presencia física en la República Argentina durante toda su vigencia.

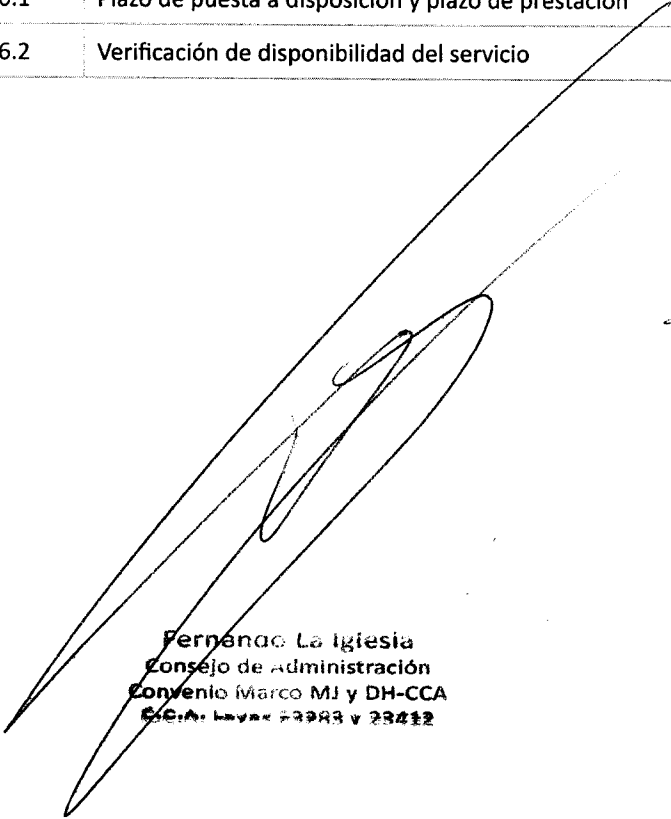
Firma: Aclaración: Carácter:

ANEXO IV — PLANILLA DE CUMPLIMIENTO TÉCNICO

El oferente deberá indicar, para cada apartado, si su oferta cumple con la totalidad de los requisitos allí establecidos y la página o folio de la propuesta técnica en que se describe o acredita su cumplimiento. No se admitirá la expresión «según pliego» como única referencia.

Apartado	Requisito	Cumple (Sí/No)	Referencia en la oferta (folio)
1	Objeto y alcance — marco normativo aplicable		
3.1.1	Requerimientos técnicos de la plataforma		
3.2.1	Identificadores Descentralizados (DID)		
3.2.2	Credenciales Verificables (VC) y gestión nativa de roles y atributos		
3.2.3	Mensajería y transporte seguro — DIDComm		
3.2.4	Registro de Datos Verificables (DID Registry)		
3.2.5	Solución nativa e integrada — condición de admisibilidad		
3.3	Aclaración sobre el concepto passwordless y su relación con la biometría y las credenciales verificables		
3.4.1	Detección de vida (Prueba de Vivacidad)		
3.4.2	Eficiencia del motor biométrico		
3.4.3	Requerimientos de eficiencia biométrica para modelos 1:n		
3.4.4	Lectura de documentos de identidad		
3.4.5	Integración con RENAPER — parte del servicio		
3.5	Proceso de onboarding omnicanal		
3.6.1	Evaluación conductual en tiempo real		
3.6.2	Puntaje de riesgo graduado y explicable		
3.6.3	Matriz de desafíos configurable (riesgo × canal × sensibilidad)		
3.6.4	Retroalimentación con la plataforma biométrica		
3.6.5	Modo de observación previo a la aplicación efectiva		
3.7	Portal de administración, auditoría y evidencia		
3.8	Dimensionamiento del servicio		
3.9	Acuerdo de nivel de servicio (SLA)		
4.1	Onboarding de personas físicas desde aplicación web		
4.2.1	Administración de documentos y plantillas		
4.2.2	Inserción de campos y etiquetas de firma (tags)		
4.2.3	Circuito de firmas y control de firmantes		
4.2.4	Seguridad, inmutabilidad y custodia de los documentos		
4.2.5	Comprobante de firma y verificación		
4.2.6	Independencia de dispositivo		

Apartado	Requisito	Cumple (Sí/No)	Referencia en la oferta (folio)
4.2.7	Portal web del servicio de firma		
4.3.1	Contexto y alcance		
4.3.2	Alcance funcional		
4.3.3	Alcance documental		
4.3.4	Estrategia técnica de extracción documental		
4.3.5	Control de calidad del servicio		
4.4.1	Prestaciones incluidas en el abono mensual		
4.4.2	Forma de cotización		
4.4.3	Plataforma en producción — condición de admisibilidad		
5.1.1	Alcance del servicio		
5.1.2	Informes		
5.1.3	Responsable técnico y canales de comunicación		
5.2.1	Alcance del servicio		
5.2.2	Niveles de servicio de la mesa de ayuda		
5.2.3	Informes		
6.1	Plazo de puesta a disposición y plazo de prestación		
6.2	Verificación de disponibilidad del servicio		


Fernando La Iglesia
 Consejo de Administración
 Convenio Marco MJ y DH-CCA
 E.C.A. Leyes 23283 y 23412


Ricardo Orsi
 Consejo de Administración
 Convenio Marco MJ y DH-CCA
 E.C.A. Leyes 23283 y 23412