RENOVACIÓN DEL CONVENIO DE SERVICIOS DE VALIDACIÓN BIOMÉTRICA Y FIRMA ELECTRÓNICA TRANSACCIONAL PARA EL PROCESO DE CONCESIÓN DE CRÉDITOS QUIROGRAFARIOS Y REGISTRO DE SUPERVIVENCIA PARA AFILIADOS EN LÍNEA

Responsable	Nombre / Cargo	Firma
Elaboración:	Ing. Nelson Santiago Sarzosa Carrillo **Jefe de Cobranzas**	
	Ing. Ana María Castillo Fueltala **Jefe de Crédito**	
	Ing. Carlos Fernández **Oficial Seguridad de Información**	
	Ing. Rosa Oderay Janeta López **Directora de Riesgos**	
	Ing. Jenny Beatriz Gómez Montesdeoca **Jefe de Gestión de Tecnologías de la Información**	
	Ing. Geovanna Ponce **Jefe Oficial de Cumplimiento**	
	Sbte. Jorge Duque **Director de Servicios Sociales (E)**	
	Mayr. Juan Luis Ruales Gamboa **Director Administrativo (E)**	

1. ANTECEDENTES Y SITUACIÓN ACTUAL

1.1 Antecedentes

El Instituto de Seguridad Social de la Policía Nacional (ISSPOL) es una institución aseguradora del Régimen Especial de Seguridad Social de la Policía Nacional, con autonomía de gestión, administrativa y financiera, con finalidad social y sin ánimo de lucro.

La Gestión de Servicios Sociales tiene como misión organizar, dirigir, controlar y evaluar los servicios sociales del Instituto para satisfacer las necesidades de sus asegurados. Dentro de sus atribuciones se encuentra la innovación de productos crediticios en función del mercado financiero y el registro de supervivencia para los afiliados.

Mediante Memorando No. ISSPOL-DG-2026-2092-I-ME, de fecha 09 de marzo del 2026, la Dirección General remitió la propuesta comercial para la renovación del servicio de emisión y administración de certificados de firma electrónica utilizados en la formalización de créditos quirografarios virtuales.

1.2 Situación actual

El ISSPOL administra una cartera crediticia de alta dinámica financiera a través del procedimiento de **Préstamo Ordinario PSS-21** (actualizado al 06 de junio de 2025) integrado en el Sistema de Información **SIISSPOLWEB**. Con el fin de mejorar la agilidad y calidad de atención para grupos prioritarios (personas de la tercera edad, personas con discapacidad y mujeres embarazadas), la institución implementó en abril de 2024 el proceso automatizado de firma electrónica de un solo uso (*One-Shot*) para documentos habilitantes (pagarés, tablas de amortización y autorizaciones de débito).

Esta innovación tecnológica resolvió la problemática de la presencia masiva de afiliados en las coordinaciones provinciales, reduciendo drásticamente los tiempos de gestión. Para garantizar la continuidad operativa de este canal virtual, se requiere **renovar el convenio con un proveedor** acreditado que asegure la autenticación e integridad de las transacciones efectuadas de forma exclusiva por personas naturales.

2. BASE LEGAL Y NORMATIVA

El proceso se rige estrictamente por el marco jurídico ecuatoriano y los estándares internacionales de seguridad aplicables:

- **Constitución de la República del Ecuador:** El Art. 227 establece los principios de eficacia, eficiencia, calidad y transparencia de la administración pública. El Art. 370 faculta el régimen especial de seguridad social de la Policía Nacional.
- **Ley de Seguridad Social de la Policía Nacional:** El Art. 3 ratifica la autonomía del ISSPOL. El Art. 6, literal c), faculta la emisión de normas para asegurar la eficiencia administrativa y la óptima utilización de los recursos.

- **Ley Orgánica de Protección de Datos Personales (LOPDP):** Los Arts. 38, 41 y 47 obligan a implementar medidas técnicas, jurídicas y organizativas permanentes para mitigar riesgos, accesos no autorizados o destrucción de datos personales. El Art. 43 regula la notificación obligatoria de vulneraciones de seguridad.
- **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos:** Otorga a la firma electrónica la misma validez y eficacia jurídica que una firma manuscrita.
- **Ley Orgánica para el Fortalecimiento de la Ciberseguridad:** El Art. 20-G obliga a las entidades públicas la notificación de incidentes de ciberseguridad cuando se comprometa la disponibilidad, confidencialidad o integridad de sistemas o información relevante.
- **Normas de Control Interno de la Contraloría General del Estado:** La Norma 410-07 regula la Administración de Proyectos Tecnológicos. La Norma 410-17 obliga al uso técnico de la firma electrónica, la verificación automatizada de su vigencia y la conservación segura de los archivos electrónicos originales. La 410-11 Seguridad de tecnología de información, garantiza el cumplimiento de la normativa de protección de datos personales, propiedad intelectual del software, seguridad de la información, utilización de estándares, sistemas o plataformas establecidas para el sector público.
- **Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003:** Se expide el Esquema Gubernamental de Seguridad de la Información (EGSI versión 3.0). Es el mecanismo para implementar el Sistema de Gestión de Seguridad de la Información en el Sector Público.
- **Estándares Internacionales de referencia:** Adopción de los controles de seguridad lógicos y organizacionales de la norma **ISO/IEC 27002:2022** y los principios de privacidad para encargados del tratamiento de Información de Identificación Personal (PII) bajo **ISO/IEC 27701:2025**.
- **Requisitos basados en Resolución No. SB-2025-02322:** Normas de Prevención de Lavado de Activos, Financiamiento del Terrorismo y Otros Delitos.- La Resolución No. SB-2025-02322 emitida por la Superintendencia de Bancos establece disposiciones para la implementación de políticas, procedimientos y mecanismos de prevención de lavado de activos, financiamiento del terrorismo y otros delitos, para el conocimiento de proveedores o socios comerciales de las entidades controladas

  Art. 19. Conocimiento de proveedores: En virtud de dicha normativa, las entidades controladas, conforme al análisis de riesgo de cada institución, están obligadas a desarrollar políticas y procedimientos de debida diligencia y conocimiento de proveedores, así como mecanismos de identificación, validación y monitoreo que permitan gestionar adecuadamente los riesgos asociados al lavado de activos, financiamiento del terrorismo y otros delitos conexos.

  El mismo artículo manifiesta que las entidades controladas deberán diseñar un formulario de conocimiento de sus proveedores permanentes, en el que además de la información

contemplada para cualquier persona natural o jurídica, según sea el caso, se incluirá los permisos de operación para desarrollar la actividad propuesta y los certificados que demuestren su experiencia.

Disposición General Segunda: las entidades controladas aplicarán las disposiciones de esta norma en lo relacionado al riesgo de lavado de activos y la financiación de otros delitos, las que prevalecerán sobre otras normas de igual o menor jerarquía que se le opongan.

- **Requisitos basados en Norma ISO 37001 E ISO 37301: Requisito 8.2 Debida Diligencia**
  Apartado A.10.1 El propósito de realizar la debida diligencia sobre ciertas transacciones, proyectos, actividades, socios de negocios o el personal de una organización es evaluar más a fondo el alcance, la escala y la naturaleza de los riesgos de soborno más que bajos identificados como parte de la evaluación de riesgos de la organización. También sirve para el propósito de actuar como un control adicional y específico en la prevención y detección del riesgo de soborno, e informa la decisión de la organización sobre si posponer, interrumpir o revisar esas transacciones, proyectos o relaciones con socios de negocios o personal.

3. OBJETIVOS Y ALCANCE

3.1 Objetivo General

Garantizar la seguridad, legalidad e integridad del proceso de otorgamiento de créditos quirografarios en línea para los afiliados del ISSPOL y servicio de supervivencia en línea, mediante la renovación de un servicio web integrado de validación biométrica de identidad 3D y firma electrónica transaccional.

3.2 Objetivos Específicos

- Integrar los servicios biométricos y de firma electrónica transaccional directo en la plataforma SIISSPOLWEB.
- Asegurar que el algoritmo de reconocimiento facial opere bajo estrictas tasas de fiabilidad técnica y mitigue el riesgo de suplantación de identidad.
- Garantizar la inmutabilidad y el almacenamiento seguro de los documentos comerciales digitales suscritos.
- Capacitar al personal encargado y cumplir al 100% las normativas vigentes de privacidad de datos personales.

3.3 Alcance del Servicio

El convenio comprende la provisión a nivel nacional de una solución técnica integral dirigida a asegurados en servicio activo y pasivo, estructurada en las siguientes etapas:

1. **Validación de identidad por biometría 3D y rostro vivo:** Comparación automatizada contra bases oficiales.

2. **Generación de firmas temporales certificadas:** Emisión automatizada de firmas únicas de un solo uso (*One-Shot*).

3. **Suscripción digital automatizada:** Aplicación de la firma en los siguientes documentos obligatorios: Pagaré a la orden, solicitud de préstamo (Tabla de amortización), autorización de débito bancario y servicio de supervivencia en línea.

4. ESPECIFICACIONES TÉCNICAS Y REQUERIMIENTOS DEL SERVICIO

4.1 Servicio de validación biométrica e identidad

4.1.1 Verificación fotográfica y rostro vivo

La solución informática deberá consumir servicios web para interactuar con la Dirección Nacional de Registros Públicos (**DINARP**), la Dirección General de Registro Civil, Identificación y Cedulación (**DIGERCIC**) u organismos oficiales habilitados. El proceso ejecutará una verificación cruzada entre la fotografía oficial del asegurado y una fotografía tipo "*selfie*" capturada en tiempo real.

- **Algoritmo de rostro vivo:** El sistema ejecutará una prueba de vida técnica interactiva que confirme que el solicitante es la persona natural titular de la identidad expuesta.

- **Métricas de calidad algorítmica:** El motor biométrico debe asegurar de forma mandatorio una **tasa máxima de falso rechazo (FRR) del 0.2%** y una **tasa máxima de falso positivo (FAR) del 0.01%**.

- **Control de excepciones:** Si la validación automática falla o si el asegurado posee una cédula de formato antiguo que imposibilite la comparación digital, la plataforma bloqueará la transacción, generará un código de error específico sin costo de facturación para el ISSPOL y habilitará un canal controlado para la carga manual de documentos bajo perfiles autorizados.

4.1.2 Estructura de datos para validación

Campos de Entrada	Campos de salida
- Tipo de consulta (“Selfie” / Biométrico) - Número cédula del afiliado - Método de comunicación (correo electrónico / mensajería electrónica) - Correo electrónico del afiliado campos de salida - Código de proceso o trámite	- Código de proceso o trámite

Tabla 1: Estructura de datos para validación

4.2 Servicio de Firma Electrónica Transaccional (*One-Shot*)

La empresa proveerá una plataforma con interfaz gráfica web integrada y personalizada para el ISSPOL.

- **Certificación de la firma:** La emisión de las firmas electrónicas de un solo uso deberá cumplir rigurosamente con la Ley de Comercio Electrónico del Ecuador. El proveedor deberá ostentar la calidad de Entidad de Certificación de Información acreditada ante la **ARCOTEL** (o actuar como su Tercer Vinculado legalmente registrado).

- **Flujo de firmado y notificaciones:** Los documentos PDF se suscribirán en la misma sesión transaccional del crédito. Si el afiliado se ausenta o no concluye el firmado dentro de la vigencia temporal del certificado, la plataforma emitirá alertas automatizadas y reintentos vía correo electrónico, los cuales serán parametrizables por el administrador del contrato sin generar recargos económicos adicionales para el ISSPOL.

  El sistema internamente vía web service enviará al proveedor (id_credito, cédula_deudor, cédula_garante, correo_deudor, correo_garante, celular_deudor, celular_garante y una lista de documentos a firmar), seguidamente el proveedor deberá enviar un correo electrónico y mensajería electrónica al afiliado y luego al garante con un link para ingresar al sistema del proveedor a realizar la firma digital.

4.2.1 Estructura de datos para firma Electrónica

Campos de Entrada (*Request*)	Campos de Salida (Response)
• Documentos en formato PDF (sin firmar) • Número de cédula del asegurado • Correo electrónico o celular destino • Descripción técnica del servicio • Cantidad de documentos a procesar	• Código único del trámite o proceso • Código técnico del resultado de la operación • Mensaje descriptivo de estado • Documento PDF con la firma electrónica insertada

Tabla 2: Estructura de datos firma electrónica

4.3 Módulo de Reportes y Monitoreo en Línea

La plataforma pondrá a disposición del ISSPOL un panel administrativo web con búsquedas avanzadas (por cédula, nombres y apellidos) que refleje la trazabilidad de los documentos según los siguientes estados: Generados, Enviados, Revisados, Firmados, Rechazados o Anulados.

Cada reporte consolidará los siguientes campos mandatorios: Número de cédula, número de solicitud, ID del servicio, estado actual, tipo de crédito, correo del afiliado, fechas exactas de creación, activación y suscripción, bitácora de envío de notificaciones y especificación de novedades o motivos técnicos de rechazo.

4.4 Respuesta del requerimiento de firma electrónica

Para el servicio de respuesta de firma electrónica se debe consumir a través del web service establecido por la empresa y el ISSPOL en el cual estarán definidos al menos los siguientes campos:

Campos de Entrada	Campos de salida
- Código del proceso o trámite	- Código de resultado. - Mensaje de resultado. - Documento PDF con firma electrónica del asegurado

Tabla 3: Requerimiento firma electrónica

- El documento firmado electrónicamente debe ser almacenado tanto por el ISSPOL como por la empresa para que se convierta en un documento legal y pueda ser respaldado y utilizado durante al menos la duración del convenio.
- Debe implementarse un mecanismo de contingencia en caso de que ocurra algún incidente con el servidor SFTP o servicio web del ISSPOL. La empresa deberá garantizar que la documentación no se pierda mediante la ejecución de reintentos y el envío de la documentación a un correo institucional del ISSPOL.
- La empresa deberá manejar un control referente al número de archivos enviados, los cuales deben ser devueltos con la firma electrónica.
- La empresa deberá contar con toda la información necesaria para permitir un proceso de trazabilidad y conciliación de las transacciones realizadas.
- La solución debe ser capaz de manejar mensajes o códigos de errores que permitan identificar con precisión cualquier problema que pueda surgir durante el proceso de suscripción de documentos. Estos mensajes o códigos de errores deben ser reportados al ISSPOL para que puedan ser corregidos oportunamente y garantizar la integridad del proceso.
- El responsable del proceso será el encargado de realizar las pruebas respectivas de la provisión de los servicios en el ambiente de desarrollo. Al finalizar las pruebas, se entregará un Informe de Pruebas validado y aprobado por los participantes. Este informe será necesario para garantizar que los servicios cumplan con los requerimientos y funcionalidades solicitados.
- Una vez que el informe de pruebas haya sido aprobado por el responsable del proceso, se iniciará la puesta en producción de los servicios técnicos. La empresa deberá presentar un informe técnico de la puesta en marcha de la solución para garantizar que se lleve a cabo de manera eficiente y sin interrupciones en el servicio.
- El proveedor deberá mediante web service indicará la respuesta que el crédito ha sido finalizado (1,0) y entregará los documentos firmados y un certificado donde se despliegue la fotografía capturada, la fotografía de la cédula de identidad, nombres completos, IP de donde se realizó la firma, país, ciudad, día y hora de la firma (este documento debe contener la firma de la empresa proveedora).

5. REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE DATOS

La empresa adjudicada asume contractualmente la figura de **Encargado del Tratamiento de Datos Personales**. Por tanto, la infraestructura y servicios del proveedor deberán cumplir de forma auditable con los siguientes controles normativos internacionales:

5.1 Requisitos Basados en ISO/IEC 27002:2022 (Seguridad)

- **Seguridad en servicios cloud:** El proveedor garantizará que toda la infraestructura de procesamiento (SAAS / IAAS) cumpla con niveles de aislamiento lógico que impidan la co-mezcla de datos del ISSPOL con otros clientes.
- **Criptografía avanzada:** Cifrado obligatorio de los documentos y datos biométricos mediante algoritmos robustos en tránsito (TLS 1.3) y en reposo (AES de mínimo 256 bits).
- **Prevención de fuga de datos - DLP:** Implementación de controles técnicos inalterables que restrinjan la copia, descarga o reenvío no autorizado de las imágenes de cédulas o plantillas biométricas por parte del personal del proveedor.
- **Aseguramiento del ciclo de vida de software:** Las APIs expuestas para la comunicación con el SIISSPOLWEB deberán carecer de vulnerabilidades críticas y presentar reportes semestrales de análisis de código estático y dinámico (Mitigación OWASP Top 10).

5.2 Requisitos basados en ISO/IEC 27701:2025 (Privacidad de Datos)

- **Limitación de propósito de la PII (Información de Identificación Personal):** Los datos personales compartidos por el ISSPOL o capturados al asegurado (*selfie*, biométricos, correos) se destinarán única y exclusivamente a la validación del crédito correspondiente. Queda prohibido su uso para minería de datos, fines comerciales o cesión a terceros.
- **Ciclo de retención y eliminación de PII:** Una vez transmitido satisfactoriamente el PDF firmado al servidor SFTP del ISSPOL, el proveedor procederá a la destrucción segura e irreversible de las imágenes de origen (fotos de cédulas y *selfies*) en un plazo no mayor a 48 horas, conservando únicamente los metadatos necesarios para la conciliación y auditoría legal mutua durante la vigencia del convenio.
- **Registro Inmutable de Actividades:** Generación de bitácoras (*logs*) logs protegidos contra modificaciones, que registren con precisión qué componente de software o qué operador accedió o procesó la Información de Identificación Personal (PII) de los afiliados.

6. METODOLOGÍA DE TRABAJO Y ENTREGABLES

6.1 Fases del Proyecto

6.1.1 Levantamiento de requerimientos

Definición de peticiones, respuestas y flujos de integración lógica.

- **Entregable 1:** Documento técnico de requerimientos funcionales, arquitectónicos y de integración aprobado por la Comisión Delegada para el proceso.

6.1.2 Integración técnica de servicios

Desarrollo y acoplamiento de las APIs con el sistema SISSPOLWEB y configuración de los canales seguros de comunicación.

- **Entregable 2:** Informe técnico detallado de la integración de servicios web y plataformas de firmado.

6.1.3 Pruebas integrales y de aceptación

Diseño conjunto y ejecución de casos de prueba simulados en ambientes controlados provistos por la Gestión de TI del ISSPOL.

- **Entregable 3:** Matriz y memoria de resultados técnicos de pruebas de aceptación de usuario (UAT) aprobada por las partes.

6.1.4 Puesta en producción

Paso formal al ambiente operativo real coordinado interinstitucionalmente.

- **Entregable 4:** Informe de puesta en producción y activación formal del servicio operativo.

6.1.5 Estabilización del servicio

Acompañamiento post-producción técnico presencial o remoto durante el plazo fijado por el Administrador del Convenio.

- **Entregable 5:** Informe técnico de finalización del periodo de estabilización de la plataforma.

6.1.6 Soporte y resolución de incidentes

El servicio biométrico y de firma operará bajo la modalidad de alta disponibilidad **24/7/365**. Se tipificará como incidente cualquier interrupción o degradación del servicio continuo superior a cinco (5) minutos. Las fallas se reportarán telefónicamente, por correo electrónico o mediante la herramienta del contratista. Tras solventar la falla, el proveedor entregará una memoria técnica en un plazo máximo de 2 días calendario. El incumplimiento en la atención activará las multas contractuales estipuladas.

- **Entregable 6:** Manual de procedimientos para la gestión y resolución de incidentes.
- **Entregable 7:** Informes semanales consolidados de incidencias, análisis de causa raíz y soluciones ejecutadas.

6.1.7 Informes técnicos de servicio

- **Entregable 8:** Informe técnico final del servicio de validación de identidad ejecutado.
- **Entregable 9:** Informe técnico final del servicio de firma electrónica y resguardo transaccional.

6.2 Matriz resumen de entregables - objeto del convenio

No.	Producto / Entregable	Criterio de Aceptación
1	Listado de requerimientos funcionales, técnicos y de integración	Aprobación escrita del Administrador del Convenio
2	Informe técnico detallado de integración de servicios	Verificación de comunicación fluida con SIISSPOLWEB
3	Informe detallado de resultados de pruebas	100% de casos críticos de negocio ejecutados con éxito
4	Informe de la puesta en producción del servicio	Firma de acta conjunta con el equipo técnico de TI ISSPOL
5	Informe de estabilización de los servicios	Cumplimiento del periodo de monitoreo post-producción sin caídas
6	Proceso documentado para la resolución de incidentes	Matriz de escalamiento y ANS validados
7	Informes semanales de resolución de incidentes	Entrega puntual cada 7 días evidenciando atención a fallas
8	Informe del servicio de validación de identidad	Demostración del cumplimiento de tasas de error FRR/FAR
9	Informe del servicio de firma electrónica	Verificación de inmutabilidad y almacenamiento de PDFs firmados

Tabla 4: Matriz entregables

7. CONDICIONES ECONÓMICAS Y CONTRACTUALES

7.1 Estimación de transacciones históricas

Como base de referencia para el dimensionamiento de las propuestas de costos, se presenta el consolidado de transacciones históricas registradas por la institución:

Año	Nro Operaciones	Nro Firmas
2024	5119	8506
2025	8589	12873
2026	4157	5924
Total, general	**17865**	**27303**

7.2 Matriz Económica de la Oferta

Los oferentes cotizarán bajo la estructura de precios unitarios fijos (incluido el IVA), desglosando los costos de acuerdo con la participación de intervinientes:

Un préstamo				Total, por Préstamo
Detalle	Solicitud de crédito	Autorización de debito	Pagaré	

1 Persona Deudor	$	$	$	
2 Personas Deudor / Garante	$	$	$	

Tabla 5: Matriz económica

*(Adicionalmente, el oferente deberá declarar de forma obligatoria el **Porcentaje de fiabilidad de severidad de la firma empastada** en el casillero técnico provisto en los pliegos)*.

Porcentaje de fiabilidad de la firma	

7.3 Plazo de Ejecución y Mecanismos de Terminación

- **Implementación técnica:** Plazo máximo de **15 días laborables** contados a partir de la firma del convenio institucional. En caso de requerir un tiempo adicional (Máximo 5 días laborables), el proveedor justificará técnicamente dicha ampliación.
- **Provisión del servicio continuo:** El plazo de ejecución del servicio operativo será de **730 días**, contados desde la aprobación formal de la fase de estabilización por parte del administrador del convenio.
- **Renovación:** Se contempla la opción de extender el servicio por un periodo adicional de un (1) año, condicionado al informe técnico favorable emitido por el administrador del convenio.
- **Terminación unilateral:** El ISSPOL se reserva la facultad jurídica de dar por terminado el convenio unilateralmente y en cualquier momento mediante comunicación oficial de la Máxima Autoridad. En este escenario, la liquidación económica se computará estrictamente de acuerdo con el volumen de operaciones efectivamente transaccionadas hasta la fecha de finalización indicada.

7.4 Forma y condiciones de pago

Los costos de la firma electrónica e impuestos aplicables serán asumidos por el afiliado beneficiario que accede al trámite crediticio virtual, deduciéndose directamente del monto total del préstamo a desembolsar por el ISSPOL.

1. El proveedor entregará mensualmente un reporte de conciliación junto con las facturas comerciales individuales emitidas a nombre de cada asegurado atendido.
2. El Administrador del Convenio validará y conciliará estos datos contra las bitácoras internas de créditos del ISSPOL.

3. Una vez aprobado satisfactoriamente el informe de control, se tramitará la orden de transferencia de los valores retenidos hacia la empresa proveedora.

8. OBLIGACIONES DE LAS PARTES Y PERFIL DEL PERSONAL

8.1 Obligaciones del ISSPOL

- Cumplir de manera oportuna con los compromisos contractuales acordados.
- Designar formalmente al Administrador del Convenio y proveer los accesos técnicos controlados a los servidores y ambientes de pruebas necesarios.
- Ejecutar las transferencias mensuales de fondos recaudados previa conciliación técnica.

8.2 Obligaciones del Administrador del Convenio

- Coordinar y supervisar la correcta ejecución técnica y operativa del convenio. Se deberá registrar en actas de reunión los acuerdos realizados.
- Articular esfuerzos con el personal técnico de la Gestión de TI del ISSPOL para asegurar la compatibilidad arquitectónica.
- Emitir las instrucciones y aclaraciones complementarias que requiera el proveedor, garantizando que estas no alteren las bases del proyecto.
- Custodiar, organizar y archivar digitalmente toda la documentación del convenio como evidencia de control para auditorías del Estado.
- Aprobar la orden de pago mensual exclusivamente contra la recepción conforme del informe de trazabilidad y las facturas emitidas por la empresa.

8.3 Obligaciones de la Empresa Proveedora

- Asegurar la ejecución legal y técnica del objeto del convenio bajo estricto apego a la legislación ecuatoriana y las bases establecidas.
- Garantizar de forma permanente el cumplimiento de la Ley Orgánica de Protección de Datos Personales y reportar de manera inmediata cualquier anomalía de seguridad identificada.
- Proveer los respaldos de trazabilidad completos de todas las operaciones ejecutadas mensualmente al administrador del contrato.
- Mantener configurables las reglas de negocio de validación biométrica y flujos de firmado digital para adaptarlas dinámicamente al comportamiento de la cartera crediticia del ISSPOL.
- Garantizar el cumplimiento de la normativa legal vigente referente a Prevención de Lavado de Activos Financiamiento del Terrorismo y Financiación de Otros Delitos, para lo cual la empresa adjudicada, previo al inicio de la relación comercial deberá presentar el formulario de Información Básica y documentos requeridos para aplicación de debida diligencia y

conocimiento del socio de negocio , formularios que serán proporcionados por el ISSPOL; si la empresa adjudicada es sujeto obligado deberá adicionalmente entregar el certificado de cumplimiento de obligaciones con la UAFE.

- En observancia a los Sistemas de Gestión Antisoborno y Compliance instituidos en el ISSPOL, la empresa adjudicada deberá presentar los documentos "Acuerdo de Compromiso", "Cuestionario de Socio de Negocio" y "Declaración de Conflicto de Intereses" proporcionados por la ISSPOL.

8.4 Perfil profesional mínimo del equipo de ingenieros del proveedor

Para la fase de integración, estabilización y soporte del servicio, el contratista asignará de forma obligatoria un equipo técnico multidisciplinario mínimo con los siguientes perfiles:

- **1 Director / Gerente de Proyecto (PM):**
  - Formación: Tercer nivel en Ingeniería en Sistemas, Computación o afines.
  - Certificación: PMP (Project Management Professional) o Scrum Master vigente.
  - Experiencia: Mínimo 3 años liderando integraciones de software en el sector financiero o público.
- **1 Ingeniero de Integración y Desarrollo Senior (Backend/API):**
  - Formación: Tercer nivel en Ingeniería en Sistemas, Software o afines.
  - Experiencia: Mínimo 3 años en desarrollo de servicios web, seguridad en APIs y arquitecturas de microservicios.
- **1 Especialista en Ciberseguridad y Privacidad de Datos:**
  - Formación: Tercer nivel en TIC o cuarto nivel en Ciberseguridad o Seguridad de la Información.
  - Experiencia: Mínimo 3 años en ciberseguridad / seguridad de la información / seguridad informática / tratamiento legal de protección de datos.

9. ACUERDO DE NIVELES DE SERVICIO (SLA)

9.1 Niveles de Disponibilidad Técnica (SLA)

El servicio integral consumido por las APIs del ISSPOL deberá operar bajo un Acuerdo de Nivel de Servicio de Disponibilidad mensual mínimo del 99.7% (SLA >= 99.7%), calculado sobre una base de operación de 24 horas, los 7 días de la semana. Las ventanas de mantenimiento programado deberán notificarse por escrito al Administrador del Convenio con al menos 5 días hábiles de anticipación y ejecutarse exclusivamente en horarios no laborables (01h00 a 05h00).

9.2 Clasificación de incidentes y tiempos de solución

Severidad del Incidente	Definición Técnica	Tiempo Máximo de Respuesta	Tiempo Máximo de Solución
Crítica (Severidad 1)	Caída completa de la API biométrica o de firma. Ningún afiliado puede transaccionar.	Menor o igual a 15 minutos	Menor o igual a 1 hora
Alta (Severidad 2)	Degradación grave. El sistema opera, pero con lentitud extrema o intermitencia que afecta a más del 30% de los usuarios.	Menor o igual a 30 minutos	Menor o igual a 3 horas

Tabla 6: Clasificación de incidentes y tiempos de solución

10. REGLAS DE PARTICIPACIÓN, EVALUACIÓN Y CONFLICTOS

10.1 Presentación de propuestas

Las propuestas técnicas y económicas deberán remitirse de forma digital al correo electrónico institucional **jsilva@isspol.org.ec**, fijándose como fecha límite improrrogable las **13h00 del día 08 de junio de 2026**. El ISSPOL se reserva la potestad de declarar desierta la convocatoria pública en cualquier fase del proceso, sin que esto genere derecho a indemnización o responsabilidad económica alguna frente a los proponentes, cuyos costos de preparación corren por su propia cuenta.

10.2 Requisitos obligatorios de adjudicación (sobre único)

La oferta presentada deberá incorporar obligatoriamente la siguiente documentación técnica habilitante:

1. **Carta de presentación formal:** Detalle pormenorizado del alcance del servicio, tarifa unitaria por tipo de préstamo y desglose impositivo de ley.
2. **Título Habilitante Vigente:** Certificación oficial emitida por el Banco Central del Ecuador que acredite a la empresa como Entidad de Certificación registrada ante la **ARCOTEL**, o en su defecto, el convenio legal de Tercero Vinculado debidamente inscrito y ratificado por el Banco Central del Ecuador.
3. **Certificaciones de Calidad técnica:** Copia de los certificados vigentes de la empresa en las normas ISO/IEC 27001 (Seguridad) o ISO/IEC 27701 (Privacidad). **Alternativamente**, se aceptará la participación de empresas que se encuentren en proceso de certificación, para lo cual deberán presentar un certificado oficial emitido por un organismo de certificación acreditado.

4. **Hojas de vida del Personal Técnico:** Respaldos del cumplimiento estricto del perfil mínimo establecido en el numeral 8.4 (títulos profesionales y certificaciones internacionales solicitadas).

10.3 Estructura general de la evaluación técnica

La calificación de la propuesta técnica se realizará sobre un total de 100 puntos. Las ofertas técnicas que no alcancen un puntaje mínimo de 80 / 100 puntos serán rechazadas automáticamente, impidiendo su paso a la apertura de la oferta económica.

Componente Técnico Evaluado	Puntaje Máximo	Puntaje Mínimo
A. Experiencia y Capacidad del proveedor	25	15
B. Perfil profesional del equipo	20	15
C. Arquitectura y Calidad Algorítmica	35	20
D. Seguridad de la Información y Privacidad de Datos	20	30
TOTAL	**100**	**80**

Tabla 7: Matriz evaluación técnica

10.4 Desglose de criterios de ponderación (Matriz evaluación técnica)

A. Experiencia y Capacidad del Proveedor (Máximo 25 Puntos)

- A.1. Título Habilitante y Acreditación (10 Puntos)
    - 10 puntos: Entidad de Certificación de Información acreditada directamente ante ARCOTEL con vigencia actual.
    - 5 puntos: Tercer Vinculado legalmente registrado y autorizado por el Banco Central del Ecuador.
    - 0 puntos: No presenta acreditación válida o se encuentra vencida.
- **A.2. Experiencia Institucional en Servicios "One-Shot" (15 Puntos)**
    - 15 puntos: Haber ejecutado al menos 3 contratos similares de validación biométrica y firma electrónica en línea en entidades financieras o públicas en los últimos 3 años (demostrable con actas de entrega recepción definitivas).
    - 10 puntos: Haber ejecutado entre 1 y 2 contratos similares.
    - 0 puntos: Ninguna experiencia verificable en este tipo específico de servicio.

B. Perfil Profesional mínimo del equipo (Máximo 20 Puntos)

- **B.1. Calificación del Director / Gerente de Proyecto - PM (6 Puntos)**
    - 6 puntos: Título de Ingeniería en Sistemas/Computación + Certificación PMP o Scrum Master vigente 3 años de experiencia en integraciones técnicas.
    - 0 puntos: No cumple con el perfil, el título o la certificación requerida.

- **B.2. Calificación del Ingeniero de Integración y Desarrollo Senior (7 Puntos)**
    - 7 puntos: Título de Ingeniería en Sistemas, Software o afines + Experiencia verificable de 3 años en desarrollo de servicios web.
    - 0 puntos: No cumple con los años de experiencia o la formación requerida.
- **B.3. Calificación del Especialista en Ciberseguridad y Privacidad (7 Puntos)**
    - 7 puntos: Tercer nivel en TIC o cuarto nivel en Ciberseguridad o Seguridad de la Información.
    - 0 puntos: No cumple con tercer nivel en TIC o cuarto nivel o la experiencia requerida.

C. Arquitectura de software y calidad algorítmica (Máximo 35 Puntos)

- **C.1. Tasas de error del motor biométrico (25 Puntos)**
    - 25 puntos: Ficha técnica que demuestre una Tasa de Falso Rechazo (FRR) <= 0.2% y una Tasa de Falso Positivo (FAR) <= 0.01%.
    - 10 puntos: Tasas de error superiores a las exigidas contractualmente
- **C.2. Módulo de Contingencia y Reintentos Parametrizables (10 Puntos)**
    - 10 puntos: El sistema permite configurar alertas y reintentos automáticos de firma por correo sin costos extra y posee un flujo alterno validado hacia buzón institucional ante caídas del canal SFTP.
    - 0 puntos: No posee mecanismos de contingencia automatizados.

D. Seguridad de la Información y Privacidad de Datos (Máximo 20 Puntos)

- **D.1. Certificación ISO/IEC 27001:2022 (10 Puntos)**
    - 10 puntos: Presenta certificado internacional vigente bajo la norma ISO 27001
    - 5 puntos: Presenta certificado oficial de que la empresa se encuentra en proceso de certificación.
    - 0 puntos: No presenta certificación de seguridad de la información.
- **D.2. Cifrado de Datos en Reposo y Tránsito (10 Puntos)**
    - 10 puntos: Arquitectura técnica que garantice de forma nativa cifrado mediante TLS 1.3 en tránsito y AES-256 en reposo para todos los archivos PDF y plantillas biométricas temporales.
    - 0 puntos: Uso de protocolos de cifrado obsoletos o inferiores.

10.5 Causas de Rechazo y Descalificación Automática

Serán descalificadas de forma directa y sin derecho a réplica las ofertas que incurran en:

- Presentación extemporánea fuera del día y hora señalados.
- Falta o inconformidad en cualquiera de los documentos requeridos en el sobre único.
- Puntaje técnico ponderado inferior a **80 puntos**.
- Inclusión de información falsa, adulterada o inexacta. Los reclamos basados en desconocimiento o error documental posterior no serán admitidos bajo ningún concepto.

10.6 Mecanismos de contingencia y resolución de conflictos

- **Continuidad transaccional:** En caso de fallas imprevistas en los servicios web o el canal SFTP del ISSPOL, la plataforma de la empresa ejecutará colas automatizadas de reintentos e implementará un mecanismo de contingencia remitiendo los documentos firmados directamente a un buzón de correo institucional seguro para salvaguardar la información.
- **Resolución de disputas:** Cualquier controversia derivada de la ejecución o interpretación del convenio se someterá primeramente a un proceso de mediación formal ante el **Centro de Mediación de la Procuraduría General del Estado**. De no mediar acuerdo amistoso, las partes agotarán la vía judicial ante el **Tribunal Distrital de lo Contencioso Administrativo** competente.

11. ANEXOS (GUÍA VISUAL DE INTERFAZ DEL PROCESO EN SIISSPOLWEB)

NECESIDAD DE FIRMA ELECTRÓNICA EN LA CONCESIÓN DE CRÉDITOS QUIROGRAFARIOS ORDINARIOS

El ISSPOL tiene la necesidad de renovar convenio de la firma digital del afiliado, garante y funcionarios en los documentos que se generan en el proceso de concesión de créditos quirografarios ordinarios directamente del SIISSPOLWEB.

Secuencia de Actividades

- **Ingreso del Usuario al Sistema** (Usuario y Contraseña)

- **Ingresar a la opción de solicitud de PQ Ordinario**

- **Ingresar Información de solicitud de préstamo**

Aquí permite realizar el interfaz de comunicación con proveedor sobre la opción de firma electrónica con el sistema y donde se necesitaría integrar la firma electrónica (API) e incluirle el SIISSPOLWEB, en lo referente a la firma de deudor y garante.

- **Generar el préstamo luego de ingresar todos los campos requeridos.**