

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

**RENOVACIÓN CONVENIO SERVICIO DE FIRMAS  
ELECTRÓNICAS PARA EL PROCESO DE  
CONCESIÓN DE CRÉDITOS QUIROGRAFARIOS EN  
LÍNEA**


	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

Responsable	Nombre / Cargo	Firma	Fecha
<b>Elaboración:</b>	Ing. Nelson Santiago Sarzosa Carrillo <b>Jefe de Cobranzas</b>		04 de mayo de 2026
	Ing. Rosa Oderay Janeta López <b>Directora de Riesgos</b>		
	Ing. Jenny Beatriz Gómez Montesdeoca <b>Jefe de Gestión de Tecnologías de la Información</b>		
	Myr. Jorge Mosquera <b>Director de Servicios Sociales (E)</b>		
<b>Aprobado:</b>	Crnl. Patricio Simbaña <b>Director Administrativo</b>		


	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

**TABLA DE CONTENIDO**

1. ANTECEDENTES.....	5
2. BASE LEGAL .....	6
3. PROBLEMÁTICA.....	9
4. SITUACIÓN ACTUAL .....	10
5. OBJETIVOS .....	10
6. ALCANCE.....	11
7. METODOLOGÍA DE TRABAJO.....	12
7.1. Activación de los servicios.....	12
7.1.1. Levantamiento de requerimientos.....	12
7.1.2. Integración de los servicios técnicos .....	12
7.1.3. Pruebas integrales de los servicios técnicos .....	12
7.1.4. Puesta en producción de los servicios.....	13
7.1.5. Estabilización de los servicios .....	13
7.1.6. Resolución de incidentes.....	13
7.2. Servicio de validación de identidad de asegurados para la suscripción de documentos digitales .....	14
7.2.1. Envío de requerimiento de validación.....	14
7.2.1.1. Aplicación de algoritmo.....	14
7.3. Servicio de firma electrónica .....	15
7.3.1. Envío de requerimientos firma electrónica.....	15
7.3.1.1. Firma electrónica .....	16
7.3.1.2. Funcionalidad de reportes en línea.....	16
7.3.2. Respuesta del requerimiento de firma electrónica.....	17
8. INFORMACIÓN QUE DISPONE LA INSTITUCIÓN .....	18
9. PRODUCTOS O SERVICIOS ESPERADOS.....	18
10. COSTO POR INTEGRACIÓN DE FIRMA ELECTRONICA .....	18
11. PLAZO DE EJECUCIÓN Y TERMINACIÓN DEL CONVENIO .....	19
12. FORMA Y CONDICIONES DE PAGO.....	20
13. OBLIGACIONES .....	20
13.1. ISSPOL .....	20
13.2. ADMINISTRADOR CONVENIO.....	20
13.3. EMPRESA.....	20
14. RESOLUCIÓN DE CONFLICTOS.....	21

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

15.	PRESENTACIÓN DE LA PROPUESTA.....	21
16.	REGLAS DE PARTICIPACIÓN.....	22
17.	CAUSAS DE RECHAZO Y DESCALIFICACIÓN DE LA PROPUESTA.....	22
18.	ANEXOS.....	23

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

## 1. ANTECEDENTES

**1.1 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, con personería jurídica y domiciliada en Quito. Cuenta con coordinaciones provinciales en todo el país para gestionar las prestaciones y servicios sociales a sus asegurados. Como organismo ejecutor de la Ley de Seguridad Social de la Policía Nacional, el ISSPOL gestiona sus propios recursos para garantizar la protección social y el bienestar del policía y su familia. El Instituto ofrece servicios de salud, pensiones, préstamos y otros beneficios a sus afiliados.

El **Estatuto Orgánico de Gestión Organizacional por Procesos** del ISSPOL establece que la **Gestión de Servicios Sociales** tiene como **Misión**: *“Organizar y dirigir la gestión de servicios sociales del Instituto de Seguridad Social de la Policía Nacional, a través del control y evaluación del logro de resultados y satisfacción de las necesidades y demanda de los asegurados”*.

En cuanto a las atribuciones y responsabilidades están:

*“a) Innovar los tipos de productos crediticios en función del mercado financiero para cubrir las necesidades de los asegurados”*.

Así mismo cuenta con Gestiones Internas:


- Gestión de Afiliación e Información
- Gestión de Servicio y Trabajo Social
- Gestión de Crédito
- Gestión de Cobranzas Institucionales

### **Productos y Servicios de la Gestión de Crédito:**

1. *Préstamos Hipotecarios*
2. *Préstamos Quirografarios*
3. *Préstamos Prendarios*
4. *Certificados de Crédito*
5. *Campañas de promoción y divulgación de créditos*

### **1.2 Memorandos, oficios**

- Memorando No. ISSPOL-DG-2026-2092-I-ME, de fecha 09 de marzo del 2026, firmado electrónicamente por el señor Coronel de Policía de E.M. Juan Javier Silva, Director General del ISSPOL, mediante el cual remite la propuesta comercial para la renovación del contrato correspondiente al servicio de emisión y administración de certificados de firma electrónica utilizado en los procesos de formalización de créditos quirografarios.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

## **2. BASE LEGAL**

### **2.1 Constitución de la República del Ecuador**

- El artículo 227 de la Constitución de la República del Ecuador determina, señala: *“la administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.”*
- El artículo 226 de la Constitución de la República del Ecuador dispone que “Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley”.
- La Constitución de la República del Ecuador en el artículo 370, inciso segundo de la Constitución establece *“La policía nacional y las fuerzas armadas podrán contar con un régimen especial de seguridad social, de acuerdo con la ley; sus entidades de seguridad social formarán parte de la red pública integral de salud y del sistema de seguridad social”.*

### **2.2 Ley de Seguridad Social de la Policía Nacional**


- La Ley de Seguridad Social de la Policía Nacional en su artículo 3, reformada por la Ley de Fortalecimiento a los Regímenes Especiales de Seguridad Social de las FF. AA y de la Policía Nacional establece que El Instituto de Seguridad Social de la Policía Nacional (ISSPOL), forma parte del sistema de seguridad social, y es un organismo autónomo con finalidad social y sin ánimo de lucro, con personería jurídica, patrimonio propio domicilio en la ciudad de Quito.
- El artículo 6 de la Ley de Seguridad Social de la Policía Nacional, así mismo reformado, establece en el literal c) Dictar normas y resoluciones para asegurar la solvencia económica y la eficiencia administrativa del ISSPOL, la óptima utilización de sus recursos, la debida asignación de los fondos que administra, y para el control y evaluación de sus actividades.

### **2.3 Ley Orgánica de Transparencia y Acceso a la Información Pública**

- El artículo 10 de la Ley Orgánica de Transparencia y Acceso a la Información Pública, establece que es responsabilidad de las entidades públicas, personas jurídicas de derecho público y entidades públicas, crear, mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que en ningún caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.

### **2.4 Ley Orgánica de Protección de Datos Personales**

***“Capítulo VI  
SEGURIDAD DE DATOS PERSONALES***

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- **Art. 38.- Medidas de seguridad en el ámbito del sector público.** - *El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza., vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales”.*

- **Art. 41.- Determinación de medidas de seguridad aplicables.** - *Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:*

*Los resultados del análisis de riesgos, amenazas y vulnerabilidades; (...)*


*El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.*

- **Art. 43.- Notificación de vulneración de seguridad.** - *El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.*
- *El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.*

## **Capítulo VII**

### **DEL RESPONSABLE, ENCARGO Y DELEGADO DE PROTECCIÓN DE DATOS PERSONALES**

- **Art. 47.- Obligaciones del responsable y encargado del tratamiento de datos personales.** - *El responsable del tratamiento de datos personales está obligado a:*
  - **2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;**

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- **7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;**
- **Artículo 43 Notificación de vulneración de seguridad.-** *El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilatación.*

## 2.5 Ley de Comercio Electrónico

- La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos regula la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad de la persona.

## 2.6 Normas de Control Interno de la Contraloría General del Estado

- **Norma de Control Interno, 410-06 Administración de Proyectos Tecnológicos**

*“La Unidad de Tecnología de Información definirá mecanismos que faciliten la administración de todos los proyectos informáticos que ejecuten las diferentes áreas que conformen dicha unidad...”*


- **Norma de Control Interno, 410-17 Firmas electrónicas**

*“...las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su reglamento”.*

*Las servidoras y servidores autorizados por las instituciones del sector público podrán utilizar la firma electrónica contenida en un mensaje de datos para el ejercicio y cumplimiento de las funciones inherentes al cargo público que ocupan.*

*Los aplicativos que incluyan firma electrónica dispondrán de mecanismos y reportes que faciliten una auditoría de los mensajes de datos firmados electrónicamente.*

*a) Verificación de autenticidad de la firma electrónica Es responsabilidad de las servidoras y servidores de las entidades o dependencias del sector público verificar mediante procesos automatizados de validación, que el certificado de la firma electrónica recibida sea emitido por una entidad de certificación de información acreditada y que el mismo se encuentre vigente.*

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

*b) Coordinación interinstitucional de formatos para uso de la firma electrónica Con el propósito de que exista uniformidad y compatibilidad en el uso de la firma electrónica, las entidades del sector público sujetos a este ordenamiento coordinarán y definirán los formatos y tipos de archivo digitales que serán aplicables para facilitar su utilización. Las instituciones públicas adoptarán y aplicarán los estándares tecnológicos para firmas electrónicas que las entidades oficiales promulguen, conforme a sus competencias y ámbitos de acción.*

*c) Conservación de archivos electrónicos Los archivos electrónicos o mensajes de datos firmados electrónicamente se conservarán en su estado original en medios electrónicos seguros, bajo la responsabilidad del usuario y de la entidad que los generó. Para ello se establecerán políticas internas de manejo y archivo de información digital.*

*d) Actualización de datos de los certificados de firmas electrónicas Las servidoras y servidores de las entidades, organismos y dependencias del sector público titulares de un certificado notificarán a la entidad de certificación de información sobre cualquier cambio, modificación o variación de los datos que constan en la información proporcionada para la emisión del certificado. Cuando un servidor público deje de prestar sus servicios temporal o definitivamente y cuente con un certificado de firma electrónica en virtud de sus funciones, solicitará a la entidad de certificación de información, la revocación del mismo, además, el superior jerárquico ordenará su cancelación inmediata. El dispositivo portable seguro será considerado un bien de la entidad o dependencia pública y por tanto, a la cesación del servidor, será devuelto con la correspondiente acta de entrega recepción.*

*e) Seguridad de los certificados y dispositivos portables seguros Los titulares de certificados de firma electrónica y dispositivos portables seguros serán responsables de su buen uso y protección. Las respectivas claves de acceso no serán divulgadas ni compartidas en ningún momento. El servidor solicitará la revocación de su certificado de firma electrónica cuando se presentare cualquier circunstancia que pueda comprometer su utilización.*


### **3. PROBLEMÁTICA**

Este instituto dentro de su cartera de servicios, cuenta con préstamos quirografarios para sus afiliados cuyo trámite se lo realiza de forma virtual, siendo así con el proceso de la firma electrónica de un solo uso de los documentos habilitantes (pagares, tabla de amortización y autorización de débito), los cuales son generados con el uso de una firma electrónica acreditada.

Con la innovación de este proceso ejecutado desde el mes de abril 2024 y estar a la par con la tecnología, logrando con esto un nuevo y mejor servicio crediticio en línea que evite el traslado físico de sus afiliados hacia las oficinas del ISSPOL, que tiene a nivel nacional, teniendo de esta forma un mejoramiento en el proceso ya que se redujo tiempos, en la gestión de los créditos.

Es importante indicar que con la implementación de la firma electrónica en la cartera de servicios crediticios se ejecutó una solución a la problemática de la presencia masiva de afiliados en las diferentes coordinaciones del ISSPOL a Nivel Nacional.

Con este antecedente es menester que el ISSPOL, realice la invitación a las diferentes empresas proveedoras de firma electrónica ONE SHOT para la renovación del servicio de firma electrónica para los

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

productos crediticios con firma electrónica para el proceso de generación de préstamos en línea siendo aplicable de forma única para las personas naturales, manteniendo la autenticación de los afiliados y garantizar las personas que aplican al préstamo quirografario.

Proceso vigente implementado para el otorgamiento del préstamo digital en su totalidad el mismo establece de forma general la necesidad de solventar las siguientes etapas en el proyecto:

1. Plataforma de registro y atención a afiliados
2. Servicio de validación de datos en el registro civil.
3. Servicio de validación de identidad por biometría.
4. Emisión de firmas temporales
5. Firmado de documentos

Documentos a generarse en el proceso y se requiere firma de afiliados:

1. Pagaré a la orden
2. Solicitud del préstamo
3. Autorización de debito

#### **4. SITUACIÓN ACTUAL**

El Instituto de Seguridad Social de la Policía Nacional, dentro de sus servicios como entidad mantiene una cartera crediticia que el Instituto brinda a sus afiliados, al ser una de las inversiones privadas que tiene mucha dinámica en el proceso financiero que mantiene el ISSPOL, se estructuran los debidos procesos de los cuales existe el procedimiento de Préstamo Ordinario PSS-21, con fecha de actualización 06 de junio del 2025, el cual se encuentra implementado dentro del Sistema de Información del Instituto de Seguridad Social de la Policía Nacional (SISSPOLWEB).

Uno de las necesidades que el ISSPOL, siempre está tratando de mejorar es la atención a los afiliados que están dentro de los grupos prioritarios, entre ellos las personas de la tercera edad, personas con discapacidad y mujeres embarazadas entre otros, para que los afiliados que están dentro de estos grupos puedan acceder a los créditos con la mayor facilidad posible y logren de esta forma tener un servicio de calidad y sobre todo de manera ágil.


#### **5. OBJETIVOS**

##### **General:**

Mejorar la seguridad y legalidad de los servicios para los afiliados del ISSPOL mediante la implementación del servicio de validación biométrica de la identidad con firma electrónica transaccional, integrado en los canales digitales.

##### **Específicos:**

- Identificar los requisitos técnicos y de seguridad necesarios para la implementación del servicio de validación biométrica de la identidad con firma electrónica transaccional.


	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- Seleccionar y adquirir la tecnología necesaria para implementar el servicio de validación biométrica de la identidad con firma electrónica transaccional.
- Integrar el servicio de validación biométrica de la identidad con firma electrónica transaccional a través de canales digitales, como una aplicación móvil o una página web.
- Realizar pruebas y ajustes necesarios para garantizar el correcto funcionamiento del servicio de validación biométrica de la identidad con firma electrónica transaccional.
- Capacitar al personal encargado de utilizar y administrar el servicio de validación biométrica de la identidad con firma electrónica transaccional.
- Garantizar el cumplimiento de las normativas y regulaciones en materia de seguridad y privacidad de datos personales al implementar el servicio de validación biométrica de la identidad con firma electrónica transaccional, mismo que debe cumplir la Autoridad de Certificación y cumplirlos en todos y cada uno de los servicios (API) entregados.
- Promocionar el servicio de validación biométrica de la identidad con firma electrónica transaccional entre los afiliados, a través de campañas publicitarias y otros medios efectivos, para fomentar su uso y aumentar la seguridad y eficiencia en los servicios que lo requieran.

## **6. ALCANCE**

Implementar un sistema integral de validación biométrica 3D y firma electrónica de un solo uso para el ISSPOL, con el objetivo de mejorar la eficiencia, seguridad y legalidad en los procesos institucionales relacionados con la generación de créditos en línea y otros servicios que requieran la identificación y autenticación de los asegurados en servicio activo y pasivo a nivel nacional, que incluya:

- Poner a disposición de los asegurados en convenio con el ISSPOL un servicio adicional que podrán activar de forma opcional. Este servicio ofrecerá beneficios adicionales a los ya contemplados en el convenio, con el objetivo de mejorar la experiencia y la satisfacción de los asegurados con nuestro servicio.
- Ofrecer un servicio de validación de la identidad del asegurado a través del uso de tecnología biométrica. Este servicio permitirá generar documentos electrónicos para la firma electrónica, lo que agilizará los procesos y mejorará la seguridad en la gestión de documentos.
- Integrar la firma electrónica de un solo uso para los documentos generados a través del servicio de validación biométrica de identidad. Esto significa que cada vez que se requiera la firma de un documento, se generará una firma electrónica única que solo podrá ser utilizada una vez. De esta manera, se garantiza la autenticidad y la integridad de los documentos firmados electrónicamente, y se evita el riesgo de suplantación o fraude.
- Respecto al convenio este tiene como objetivo principal la autenticación de la identidad de los asegurados, con el fin de garantizar que los solicitantes de créditos tengan la identidad que afirman tener. Para lograr este objetivo, se requiere implementar una opción adicional para los afiliados que no puedan hacer uso de su firma electrónica a través de otros mecanismos. De esta manera, se busca mejorar la seguridad y la confiabilidad del proceso de solicitud de créditos en línea, lo que se traduce en una mayor satisfacción y confianza por parte de los usuarios del servicio.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

## 7. METODOLOGÍA DE TRABAJO

Para la ejecución del presente proyecto, es importante que la empresa tenga en cuenta las siguientes premisas:

### 7.1. Activación de los servicios

#### 7.1.1. Levantamiento de requerimientos

La empresa será responsable de realizar el levantamiento de las definiciones de las peticiones y respuestas para la activación de los servicios web entre el ISSPOL. Para ello, entregará los siguientes documentos:

- Requerimientos funcionales y técnicos.
- Requerimientos de integración.

En caso de que la empresa considere necesario entregar información adicional, esta podrá ser incluida en el proceso. La documentación será elaborada por la empresa y entregada al administrador del convenio para su revisión, validación y aprobación.

#### Entregables:

- Listado de requerimientos funcionales, técnicos y de integración

#### 7.1.2. Integración de los servicios técnicos

La empresa será responsable de llevar a cabo todas las tareas necesarias para activar los servicios web que permitirán el consumo de los servicios técnicos de acuerdo con los requerimientos del ISSPOL. Una vez activados los servicios, la empresa entregará un informe técnico detallando los servicios web a utilizar.

- Integrar de servicios web, contando con una plataforma para integrar el proceso la firma electrónica contando con una API programada para envío y recepción de la información desde el sistema SISSPOLWEB en el proceso de concesión de créditos quirografarios en línea.
- Definición y establecimiento del proceso de entrega de documentos firmados a través del canal de comunicación acordado entre la empresa y el ISSPOL.


#### Entregables:

- Informe técnico que detalle la integración de los servicios

#### 7.1.3. Pruebas integrales de los servicios técnicos

Para la elaboración, ejecución y aceptación de los casos de pruebas de usuarios finales, se deberá considerar lo siguiente:

- La empresa será responsable de elaborar los casos de pruebas de usuarios finales, los cuales contendrán la descripción de los casos de prueba basados en los documentos de requerimientos funcionales, técnicos y requerimientos de integración. La empresa validará y adicionará los casos de pruebas que considere necesarios, para su posterior aprobación por el administrador del convenio.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- Una vez aprobados los casos de prueba por el administrador del convenio, la empresa preparará el entorno de pruebas y ejecutará los casos de prueba de usuarios finales en conjunto con el equipo técnico y funcional del ISSPOL.
- Así mismo, concluidas las pruebas de aceptación de usuario, la empresa entregará un informe detallado de los resultados de las pruebas al administrador del convenio para su aprobación.

Es importante destacar que el ISSPOL a través de la Gestión de TI deberá proporcionar los ambientes controlados (ambientes de prueba, desarrollo) necesarios para la implementación de las diferentes fases del convenio.

**Entregables:**

- Informe detallado de los resultados de las pruebas

**7.1.4. Puesta en producción de los servicios**

La empresa será responsable de elaborar y entregar al administrador del convenio la documentación necesaria para el paso a producción. Dicha documentación será revisada, validada y aprobada por el administrador del convenio.

Una vez aprobada la documentación, el administrador del convenio entregará dicha documentación a la empresa y gestionará la autorización para la puesta en producción. La puesta en producción se llevará a cabo de manera conjunta entre la empresa y el personal técnico del ISSPOL, coordinando las actividades necesarias para garantizar que la funcionalidad se encuentre operativa.

**Entregables:**

- Informe de la puesta en producción del servicio

**7.1.5. Estabilización de los servicios**

Después de la aceptación de la puesta en producción del servicio, la empresa brindará un acompañamiento post-producción para garantizar que el servicio funcione de manera estable durante el plazo acordado con el administrador del convenio. Una vez finalizado el periodo de acompañamiento post-producción, se dará por concluido el servicio de puesta en producción.


La empresa entregará al administrador del convenio un informe técnico detallado de las actividades realizadas hasta la puesta en producción de los servicios técnicos, para su posterior validación y aceptación.

**Entregable:**

- Informe de la estabilización de los servicios

**7.1.6. Resolución de incidentes**

- La empresa del servicio de firma electrónica con validación biométrica (validación del rostro vivo con algoritmo que entregue al menos al 99% de fiabilidad), el cual debe garantizar la disponibilidad del servicio y puesta en producción las 24 horas del día, los 7 días de la semana, los 365 días del año, durante todo el convenio. Cualquier interrupción del servicio que dure más de cinco (5) minutos se

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

considerará un incidente. Además, la empresa brindará atención a los incidentes presentados en cualquier momento para resolver problemas, corregir errores y atender requerimientos de configuración y otros problemas que puedan surgir durante la prestación de los servicios técnicos.

- Los incidentes pueden ser notificados por el administrador del convenio o el personal técnico del ISSPOL en cualquier momento a través de vía telefónica, correo electrónico o en la herramienta que proporcione la empresa. De igual manera, entregará al administrador del convenio un informe correspondiente en un plazo máximo de 2 días calendario después de la resolución del incidente, para su aprobación. Si la empresa no cumple con la atención de los incidentes presentados, se aplicará la multa correspondiente por parte del administrador del convenio.

**Entregable:**

- Proceso para la resolución de incidentes
- Informes semanales que describa la resolución de los incidentes que se presenten durante la ejecución del convenio

**7.2. Servicio de validación de identidad de asegurados para la suscripción de documentos digitales**


**7.2.1. Envío de requerimiento de validación**

El ISSPOL utilizará la plataforma de la empresa para llevar a cabo la validación biométrica de identidad. Para ello, la empresa entregará al menos los siguientes campos.

Campos de Entrada	Campos de salida
<ul style="list-style-type: none"> <li>- Tipo de consulta ("Selfie" / Biométrico)</li> <li>- Número cédula del afiliado</li> <li>- Foto de cédula anverso y reverso</li> <li>- Método de comunicación (correo electrónico)</li> <li>- Correo electrónico del afiliado campos de salida</li> <li>- Código de proceso o trámite</li> </ul>	<ul style="list-style-type: none"> <li>- Código de proceso o trámite</li> </ul>

**7.2.1.1. Aplicación de algoritmo**

- **Identidad – fotografía**
  - o La solución debe comparar y reconocer la fotografía del asegurado con la fotografía de la Dirección Nacional de Registros Públicos (DINARP), Dirección General de Registro Civil, Identificación y Cedulación (DIGERCIC) u otros organismos autorizados, mediante una fotografía "selfie" y proporcionar una relación de correspondencia de las dos imágenes. Esto permitirá verificar la identidad del asegurado en una transacción. Además, esta funcionalidad deberá ser utilizada en medios virtuales para validar la identidad por dichos canales.
  - o La solución debe tener una tasa máxima de falso rechazo del 0,2% y una tasa máxima de falso positivo del 0,01%. En caso de que no se pueda realizar la validación automática de

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

fotografía, se generará una alerta y se enviará un código de error, y la transacción no será cobrada.

- La solución permitirá subir archivos manualmente con la autorización respectiva a través de perfiles establecidos para asegurados que tienen cédulas antiguas y no se puede hacer la validación con la fotografía. Estas funcionalidades podrán ser habilitadas o deshabilitadas según el proceso que se esté realizando.
  - La empresa deberá presentar una descripción detallada del proceso de validación, incluyendo material gráfico, audiovisual o digital.
- **Rostro vivo**
- Se integrará un servicio de validación biométrica de rostro vivo en los procesos crediticios que impliquen la firma de documentos de asegurados del ISSPOL, mediante algoritmos de reconocimiento facial. La activación del servicio permitirá confirmar que el asegurado que hace el requerimiento es efectivamente la dueña de la identidad que ostenta. Solo cuando el sistema valide dicha identidad permitirá continuar con el proceso de solicitud de créditos en línea.
  - Para la activación biométrica de rostro vivo, el servicio deberá realizar una validación con la DINARDAP, DIGERSIC u otros organismos autorizados, con el objetivo de comparar la fotografía del asegurado y así habilitar el proceso de solicitud de créditos en línea con firma electrónica.
  - La solución debe tener una tasa máxima de falso rechazo del 0,2% y una tasa máxima de falso positivo del 0,01%.
  - La empresa deberá presentar una descripción detallada del proceso de validación por rostro vivo, incluyendo material gráfico, audiovisual o digital.

**Entregable:**

- Informe del servicio de validación de identidad


**7.3. Servicio de firma electrónica**

Se usará la plataforma de la empresa y/o diseño de la firma electrónica de un solo uso para la suscripción de documentos digitales, en el cual se considerará:

**7.3.1. Envío de requerimientos firma electrónica**

Para que el servicio de firma electrónica se lo pueda consumir se lo hará a través de la plataforma de la empresa en el cual estarán definidos al menos los siguientes campos:

Campos de Entrada	Campos de salida
<ul style="list-style-type: none"> <li>- Documentos en formato PDF</li> <li>- Número de cédula del asegurado</li> <li>- Número de celular o correo electrónico</li> <li>- Descripción del servicio</li> <li>- Número de documentos a ser procesados</li> </ul>	<ul style="list-style-type: none"> <li>- Código de proceso o trámite</li> </ul>

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		


#### 7.3.1.1. Firma electrónica

- Se contará con una plataforma con una interfaz gráfica personalizada por parte de la empresa que permita administrar el proceso de firma electrónica para todos los documentos generados en la solicitud de créditos en línea, integrándose con los sistemas transaccionales Core del ISSPOL. Se empleará un servicio de firma electrónica certificada (de un solo uso) en los procesos crediticios que requieran la suscripción del asegurado.
- Se habilitarán interfaces para integrar los servicios y procesos necesarios para el firmado de documentos con firma certificada de un solo uso, los cuales generarán certificados digitales para la firma electrónica.
- Si el asegurado no responde para continuar con la firma electrónica de los documentos, se enviarán notificaciones de alerta y reintentos para la firma electrónica a través de los medios de comunicación establecidos (correo electrónico). Se establecerá un máximo de reintentos (parametrizable según la necesidad), siempre y cuando el asegurado no realice la firma de los documentos dentro del tiempo de validez de la firma, sin incurrir en costos adicionales para el ISSPOL.
- La empresa será responsable de garantizar que la firma electrónica utilizada para suscribir los documentos sea válida según la regulación del Ecuador, con el objetivo de que los documentos suscritos electrónicamente sean aceptados como válidos. Además, deberá cumplir con la "**Ley de Comercio Electrónico, Firmas y Mensajes de Datos**" para la emisión de firmas electrónicas que permitan realizar el proceso de suscripción electrónica de documentos. La empresa deberá ser certificado como entidad certificadora o su Tercer Vinculado que le permita emitir firmas electrónicas temporales a los asegurados que soliciten créditos en línea en el portal del ISSPOL.
- Los documentos digitalizados se firmarán durante la interacción con el crédito en línea. El documento firmado electrónicamente deberá ser almacenado tanto por el ISSPOL, convirtiéndose en un documento legal para su posterior respaldo y uso.
- Se identificará la documentación digital suscrita con firma electrónica por parte del asegurado y se asegurará que la documentación comercial suscrita sea enviada al servidor SFTP del ISSPOL mediante servicio web. La solución incluirá un reporte de documentos suscritos, no suscritos y otros definidos por el ISSPOL. Además, se contará con funcionalidad para firmar documentos bajo demanda en casos de excepción. La cantidad de documentos a suscribirse será configurable según el dinamismo del negocio.

#### 7.3.1.2. Funcionalidad de reportes en línea

La empresa deberá implementar una funcionalidad de consulta de reportes en línea que permita:

- Visualizar todos los estados de los documentos digitales, incluyendo aquellos generados, enviados, revisados, firmados y rechazados.
- Realizar búsquedas mediante filtros avanzados por criterios como número de cédula, nombres, apellidos, entre otros.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		


- Contar con un reporte que permita visualizar el estado de todos los documentos, incluyendo aquellos que están pendientes de firma electrónica, aquellos que se han firmado exitosamente y aquellos que se han rechazado por anulación, identificándolos mediante campos definidos para un control integral del proceso.
- Los campos requeridos para el reporte son:
  - o Número de cédula de identidad del asegurado, número de petición o solicitud, número de servicio, estado de servicio, tipo de producto, correo electrónico, fecha de activación y creación de servicio, fecha de suscripción o no de los documentos digitales, confirmación de envío por el ISSPOL y confirmación de envío al correo del asegurado. Además, se incluirán novedades en caso de rechazo de firma.

### 7.3.2. 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

- 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.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- 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.

**Entregable:**

- Informe del servicio de firma electrónica

**8. INFORMACIÓN QUE DISPONE LA INSTITUCIÓN**

El ISSPOL dispone de los siguientes recursos para el proyecto:

- Procedimiento No. PSS-21 "Préstamo Quirografario Ordinario", versión No. 4, aprobado por el Comité General de Desarrollo Institucional el 06 de junio de 2025.
- Normativa y procedimientos internos vigentes.
- Solicitud de Crédito (Tabla de amortización)
- Autorización de debito
- Pagará, podrán ser sujetos de actualización.

**9. PRODUCTOS O SERVICIOS ESPERADOS**


A continuación, se detalla los productos objeto del Convenio que deberá entregar la empresa

<b>Productos objeto del convenio</b>		
<b>No</b>	<b>Entregable</b>	<b>Observación</b>
1	Listado de requerimientos funcionales, técnicos y de integración	
2	Informe técnico que detalle la integración de los servicios	
3	Informe detallado de los resultados de las pruebas	
4	Informe de la puesta en producción del servicio	
5	Informe de la estabilización de los servicios	
6	Proceso para la resolución de incidentes	
7	Informes semanales que describa la resolución de los incidentes que se presenten durante la ejecución del convenio	
8	Informe del servicio de validación de identidad	
9	Informe del servicio de firma electrónica	

**10. COSTO POR INTEGRACIÓN DE FIRMA ELECTRONICA**

Se debe tomar en cuenta el número estimado de transacciones a utilizar para el proceso de firmas electrónicas en préstamos quirografarios.

<b>Año</b>	<b>Nro Oper</b>	<b>Nro Firmas</b>
2024	5119	8506
2025	8589	12873
2026	4157	5924
<b>Total general</b>	<b>17865</b>	<b>27303</b>

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

Los ofertantes tendrán que especificar los precios incluida **IVA**, ya sea por número de documentos para firmar o un solo valor independiente del número de firmas de acuerdo al siguiente cuadro:

Un préstamo				Total por Préstamo
	Solicitud de Crédito	Autorización de debito	Pagaré	
<b>1 Persona Deudor</b>	\$	\$	\$	
<b>2 Personas Deudor / Garante</b>	\$	\$	\$	


Indicar el porcentaje de fiabilidad de severidad de la firma empastada.

<b>Porcentaje de fiabilidad de la firma</b>	
---	--

## 11. PLAZO DE EJECUCIÓN Y TERMINACIÓN DEL CONVENIO

Dentro del plazo de ejecución del convenio, la empresa deberá contemplar lo siguiente:

- Dentro del plazo de ejecución del convenio, la empresa deberá garantizar que se cumpla el plazo para el inicio de la provisión del servicio, el cual es 720 días contados a partir de la notificación y aprobación por parte de la empresa y administrador del convenio, respectivamente, sobre la finalización de la implementación del servicio. Es importante que la empresa cumpla con este plazo para garantizar que el servicio sea entregado en tiempo y forma.
- Es importante destacar que la implementación del servicio deberá realizarse en un plazo máximo de 7 días contados a partir de la fecha de suscripción del convenio. Además, se contempla la posibilidad de renovar el servicio por un período adicional de un año, siempre y cuando se cuente con un informe favorable del administrador del convenio. Es necesario tener en cuenta estas condiciones para garantizar la continuidad del servicio en caso de que sea necesario.
- El Instituto de Seguridad Social de la Policía Nacional podrá dar por terminado el Convenio de manera unilateral en cualquier momento, para lo cual bastará con que la Máxima Autoridad remita a la empresa notificación respectiva con la fecha de finalización del servicio. En caso de que se dé por terminado el Convenio, los valores que correspondan cancelar a la empresa previo a la terminación serán liquidados según las operaciones realizadas hasta ese momento.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

## **12. FORMA Y CONDICIONES DE PAGO**

Los valores correspondientes a los servicios prestados, incluyendo los impuestos, será cubierto por el asegurado que accede al uso de la plataforma para la firma electrónica y será debitado del monto a ser desembolsado por el ISSPOL. Para llevar a cabo este proceso, la empresa deberá remitir un reporte del servicio prestado durante el mes y las facturas comerciales emitidas a nombre de los asegurados por la empresa.

Posteriormente, el administrador del convenio procederá a conciliar los valores que consten en los registros del ISSPOL con el valor de las facturas. Si es necesario, se realizará el trámite de pago correspondiente.

## **13. OBLIGACIONES**

### **13.1. ISSPOL**

- Todas las partes involucradas en el convenio deben cumplir con sus obligaciones de manera rápida y puntual, según lo establecido en el convenio.
- Designar a un administrador del convenio y proporcionar a la empresa los datos del servidor asignado para el cumplimiento del convenio.
- Realizar los pagos correspondientes a la empresa de manera oportuna, según lo establecido en el convenio, para garantizar el cumplimiento de las obligaciones.


### **13.2. ADMINISTRADOR CONVENIO**

- Coordinar todas las acciones necesarias para asegurar la correcta ejecución del Convenio.
- Garantizar el cumplimiento de todas las obligaciones establecidas en el convenio y sus documentos correspondientes.
- Trabajar en conjunto con otras entidades y profesionales técnicos del ISSPOL, cuya competencia, conocimientos y perfil sean necesarios para garantizar la correcta ejecución del convenio.
- Suministrar a la empresa todas las instrucciones necesarias para asegurar el adecuado cumplimiento del convenio.
- En caso de que falte algún dato o información necesaria para el cumplimiento del proyecto, o si la empresa no puede obtenerla directamente, se emitirán instrucciones adicionales. Cabe resaltar que dichas instrucciones no modificarán las bases del proyecto.
- Organizar y archivar correctamente toda la documentación relacionada con la administración del convenio, asegurando que exista suficiente evidencia documental para las auditorías que puedan llevar a cabo los órganos de control del Estado.
- Proceder a realizar la orden de pago únicamente después de haber recibido la liquidación mensual del servicio por parte de la empresa, la cual debe ser satisfactoria para el ISSPOL, y haber recibido las facturas comerciales emitidas por la empresa a nombre de los asegurados.

### **13.3. EMPRESA**

Asegurar una correcta y legal ejecución del Convenio en los términos establecidos.

- Asegurarse de cumplir con la legislación ecuatoriana aplicable a la ejecución del convenio, y verificar el cumplimiento total de lo establecido en las bases del proyecto, de acuerdo con los términos y condiciones del convenio correspondiente.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- Garantizar el cumplimiento de la normativa legal actual referente a la seguridad de la información y la protección de datos personales.
- Informar de manera oportuna acerca de los incidentes de seguridad de la información que se presenten durante la ejecución del convenio, y colaborar en la identificación, contención, investigación y solución de dichos incidentes. Además, tomar las medidas necesarias para prevenir su repetición.
- La empresa debe llevar a cabo todas las acciones necesarias para la adecuada integración, configuración, pruebas en todas sus etapas, puesta en servicio, soporte y mantenimiento de los servicios.
- Las validaciones de identidad biométrica y solicitudes de crédito en línea con firma electrónica deben ser configurables para su aplicación en función de los procesos crediticios.
- La empresa debe cumplir con la Ley de Comercio Electrónico para emitir firmas electrónicas que permitan realizar el proceso de suscripción electrónica de documentos.
- Asegurarse de cumplir con los procedimientos de resolución de incidentes establecidos en la metodología de trabajo.
- La empresa deberá entregar respaldos de la trazabilidad de todas las operaciones realizadas en el mes al administrador del convenio.

#### **14. RESOLUCIÓN DE CONFLICTOS**


En caso de incumplimiento de cualquiera de las partes durante la ejecución del convenio, la parte afectada puede exigir su cumplimiento a través de mediación ante el Centro de Mediación de la Procuraduría General del Estado. Si no se llega a un acuerdo, se puede acudir al Tribunal Distrital de lo Contencioso Administrativo correspondiente.

#### **15. PRESENTACIÓN DE LA PROPUESTA**

Las recepciones de propuestas se recibirán al correo electrónico de [jsilva@isspol.org.ec](mailto:jsilva@isspol.org.ec), hasta las 13h00 del día 14 de mayo de 2026. El ISSPOL se reserva el derecho de declarar desierta la convocatoria sin generar responsabilidad alguna.

Además, adjuntar:

- Carta de presentación que incluya la propuesta del servicio, con el precio unitario y sus componentes, discriminando entre costos por transacción y los impuestos correspondientes.
- Presentar el título habilitante del Banco Central del Ecuador como entidad de certificación registrada en la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) vigente, o convenio de tercero vinculado a la entidad de certificación de información del Banco Central del Ecuador vigente.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

- En caso de ser tercero vinculado, presentar la notificación de registro del convenio para la designación de tercero vinculado en calidad de tercero vinculado o distribuidor autorizado, celebrado entre el Banco Central del Ecuador y la empresa.


#### **16. REGLAS DE PARTICIPACIÓN**

- Es responsabilidad de la empresa revisar cuidadosamente estas bases y cumplir con todos los requisitos solicitados. El ISSPOL no aceptará reclamos posteriores de la empresa basados en el desconocimiento de los términos de las bases o en errores en la documentación presentada.
- Durante el proceso de revisión, el ISSPOL se reserva el derecho de rechazar la propuesta si se establece que la información proporcionada es falsa o ha sido adulterada. Los costos asociados a la preparación de la propuesta serán responsabilidad de cada interesado, por lo que el ISSPOL no reconocerá ni reembolsará ningún costo.

#### **17. CAUSAS DE RECHAZO Y DESCALIFICACIÓN DE LA PROPUESTA**

Las propuestas serán rechazadas y descalificadas por las siguientes razones:

- Si son presentadas después de la fecha límite.
- Si contienen información falsa.
- Si no cumplen con todos y cada uno de los requisitos exigidos en el sobre único.

	<b>INSTITUTO DE SEGURIDAD SOCIAL DE LA POLICÍA NACIONAL</b>	<b>REV. 1</b>
<b>RENOVACIÓN CONVENIO SERVICIO DE FIRMAS ELECTRÓNICAS</b>		

## 18. ANEXOS

### 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 SISSPOLWEB.

#### 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 SISSPOLWEB, en lo referente a la firma de deudor y garante.

Foto





Click para activar la cámara

Firma Electrónica
  Firma Manual

- USTED PUEDE PERSONALIZAR EL VALOR Y EL PLAZO DEL CRÉDITO
- REVISE TODAS LAS VALIDACIONES DEL CRÉDITO
- PARA CREAR LA SOLICITUD DE CRÉDITO DE CLICK EN CONTINUAR

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

### Solicitud de Crédito ?

✓ Continuar
⌛ Cancelar

- VALIDAR AÑOS SERVICIO DEUDOR MAXIMO
- VALIDAR EDAD MEDIA DEUDOR
- VALIDA LOS BANCOS ACEPTADOS PARA UN CREDITO
- VALIDA DEUDOR BLOQUEADO
- VALIDA SI EL DEUDOR SE ENCUENTRA EN MORA
- VALIDACION SUPERVIVENCIA DEUDOR