ANEXO N° 01-A

FORMATO DE CONTRATO MENOR DE SERVICIOS Y CONSULTORÍAS

DETALLE DEL REQUERIMIENTO	
Área usuaria / Área técnica estratégica	Departamento de Desarrollo de Sistemas
Número de Cuadro Multianual de Necesidades	54
Objetivo estratégico	**6.5**. Mantener una adecuada infraestructura física y tecnológica para el funcionamiento operativo de la SBS.
Denominación de la Contratación	Adquisición De Certificado Digital Para Firma De Código En Microsoft y Java
Persona de contacto del AU/ATE	Marco Antonio Chuquillanqui
Compatibilización	*No*

FINALIDAD PUBLICA

El producto tiene por finalidad contar con un (01) certificado digital para el firmado de código de software basado en Microsoft.NET y en Java, desarrollado y/o utilizado por la Superintendencia y es necesario para asegurar su correcta publicación, funcionamiento y operatividad, preservando así la inversión realizada.

OBJETIVO DE LA CONTRATACION

El requerimiento consiste en la adquisición de un certificado digital para el firmado de código desarrollado en Microsoft.NET y en Java, el cual es necesario para asegurar la correcta publicación, funcionamiento y operatividad de software, los cuales son utilizados actualmente en la Superintendencia para diversos servicios.

CARACTERISTICAS DEL SERVICIO

La Superintendencia, para el cumplimiento de sus funciones de regulación y supervisión de los Sistemas Financiero, de Seguros y del Sistema Privado de Pensiones, así como para prevenir y detectar el Lavado de Activos y Financiamiento del Terrorismo, desarrolla e implementa software para diversos propósitos, bajo las plataformas y lenguajes de programación en Microsoft.NET y Java, algunos de estos software utilizados requiere para su uso que sean firmados digitalmente por las siguientes razones:

a) Para que el software a ejecutar pueda ser reconocido como un software de confianza al momento de la instalación y ejecución en forma automática por parte del usuario final, el cual ofrece a éstos la confianza en los programas que descargan e instalan en sus equipos y dispositivos.

b) Para que el software desarrollado pueda ser verificado, cerrado y versionado en una determinada versión final al momento de la implementación y lanzamiento, a fin de evitar alteraciones de código fuente de forma externa bajo cualquier modalidad.

c) Para que determinado software, tales como el Sistema de Firmado Digital, pueda ser firmado como parte de los requerimientos de la evaluación de acreditación del software, conforme lo establecido por la IOFE e INDECOPI.

Algunos de estos softwares conocidos son el “Sistema de Firmado Digital de la Intranet” y el “Sistema de Transferencia de Archivos Web (SIX-TCL)” los cuales necesitan ser firmados mediante un certificado digital de firma de código proporcionado por una empresa reconocida a nivel internacional, cuyo producto sea reconocido en la mayoría de los sistemas operativos vigentes en la actualidad, en especial en las plataformas Microsoft Windows.

Asimismo, el uso de la característica de firmado digital de código permite que cualquier software sea utilizado de forma más segura desde cualquier computador o dispositivo, sin la necesidad de realizar configuraciones complejas, ya que desaparece o minimiza los mensajes de advertencia y/o de error del sistema operativo al momento de su descarga, instalación o uso, por temas de seguridad vigentes.

Actualmente, como parte de su infraestructura tecnológica, la Superintendencia cuenta con un (01) certificado digital de firma de código proporcionados por la empresa Entrust Code Signing (ver figuras abajo), los cuales proporcionan las características de fiabilidad y seguridad en la instalación y ejecución de las aplicaciones de software basados en las plataformas Microsoft.NET y Java.

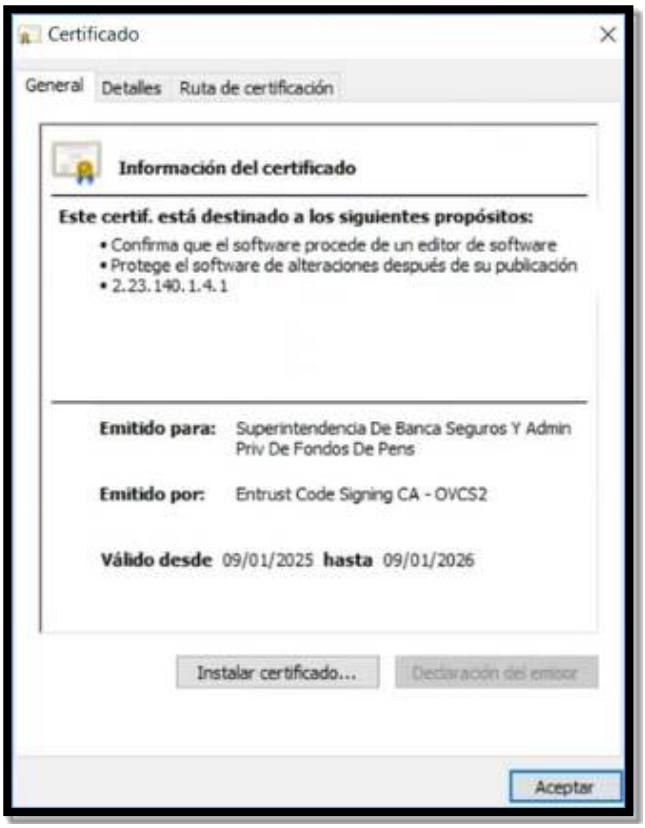

Figura N° 1: Certificado Digital de Firma de Código – Java y Microsoft.NET

El objetivo de la contratación es la adquisición de un (01) certificado digital de firmado de código para el software desarrollado y/o utilizado por la Superintendencia, basado en la plataforma Microsoft.NET y Java, por el período de 1 año, para sus diversos procesos y actividades relacionadas de forma interna y especialmente con las entidades estatales o privadas, en especial debido a que dicho certificado permitirá firmar el software de Firmado Digital, necesario como requerimiento solicitado por la IOFE como parte de la evaluación de seguimiento de la acreditación del software, según Oficio N° 101-2019/CFE-INDECOPI, la Comisión Transitoria para la Gestión de la Infraestructura Oficial de Firma Electrónica conforme al artículo 5° del reglamento General de Acreditación de los Prestadores de Servicios de Certificación Digital (PSC).

Asimismo, el certificado deberá contemplar lo siguiente:

- Permitir la entrega segura de contenido a través de Internet, esto es, permitir la descarga y la ejecución del software firmado, de modo que puedan estar seguros del origen del contenido y de su integridad.
- Permitir firmar digitalmente software de modo de usuario de 32 y 64 bits utilizando un certificado de tipo Java Object Signing, archivos Java como applets y/o empaquetados JAR, WAR, EAR, RAR, entre otros.
- Permitir firmar digitalmente software de modo de usuario de 32 y 64 bits utilizando un certificado de tipo Microsoft.NET, archivos como EXE, DLL, entre otros.
- Soporte para los siguientes navegadores: Internet Explorer 10.0 o superior
- Soporte para los siguientes navegadores (última versión disponible): Chrome, Firefox, Opera, Safari, Microsoft Edge
- Soporte a formatos de almacenes de certificados en PKCS#11.
- Soporte técnico gratuito local durante el horario laboral normal, mediante un número telefónico exclusivo y/o por correo electrónico.
- El certificado debe tener el KeyUsage como firma de código.

El proveedor, con motivo de la entrega del producto, podrá recibir de la Superintendencia información de carácter estrictamente confidencial, la cual deberá ser utilizada sólo para los fines de la entrega del producto, por ello, será obligación del proveedor mantener total secrecía y confidencialidad respecto a los datos e información de cualquier clase, que la Superintendencia le proporcione, o bien, a la que tenga acceso, con motivo de la entrega del producto.

Adicionalmente, el proveedor estará obligado a instruir a sus funcionarios o personal que será parte conformante del recurso humano que ejecutará el producto respecto a la obligación de mantener total secrecía y confidencialidad.

Finalmente, el proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del producto ofrecido por un plazo de un (01) año, contados a partir de la conformidad otorgada por la Gerencia de Tecnologías de Información.

REQUISITOS DEL PROVEEDOR / PERFIL DEL CONSULTOR

El proveedor debe ser fabricante, entidad certificadora o agente autorizado en el Perú para comercializar certificados de firma digital para código JAVA y NET, y ser reconocido a nivel internacional o debe encontrarse en el registro Oficial de Prestadores de Servicios de Certificación Oficial (ROPS[1]), cuyo producto sea reconocido en la mayoría de los sistemas operativos vigentes en la actualidad, en especial en las plataformas Microsoft Windows, esta acreditación debe presentarse al momento de iniciar el proceso de selección. Asimismo, una vez inicie el proceso de selección, el postor debe adjuntar la documentación necesaria que lo acredite como fabricante, entidad certificadora o agente autorizado en el Perú para comercializar certificados de firma digital para código JAVA y NET (carta del fabricante o del distribuidor oficial). Por otro lado, el fabricante, entidad certificadora o agente autorizado, debe brindar la asistencia y soporte para instalación y uso del certificado, en caso se requiera.

LUGAR Y PLAZO DE EJECUCIÓN

El certificado digital, cuya vigencia es de un año, deberá ser entregado, por medio electrónico o presencial, a la Superintendencia, directa o indirectamente, a un representante del Departamento de Desarrollo de Sistemas, en un plazo máximo de quince (15) días calendario contados a partir de la notificación formal emitida por la Gerencia de Tecnologías de la Información, en la que se solicita dicha entrega.

[1] Registro Oficial de Prestadores de Servicios de Certificación Digital (ROPS) - Informes y publicaciones - Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Plataforma del Estado Peruano

Asimismo, luego de formalizado el contrato, el proveedor podrá solicitar una ampliación del plazo de entrega únicamente en caso de existir causas justificadas que impidan cumplir con el plazo originalmente establecido. La solicitud deberá presentarse por escrito y/o correo electrónico, dirigida a la Gerencia de Tecnologías de la Información, dentro de los cinco (5) días hábiles siguientes a la identificación de la causa que motiva el retraso, adjuntando la documentación sustentadora correspondiente.

La Gerencia evaluará la solicitud y emitirá su pronunciamiento en un plazo no mayor a cinco (5) días hábiles. La ampliación de plazo será válida únicamente si cuenta con la aprobación expresa de dicha Gerencia. En ningún caso se aceptarán solicitudes de ampliación presentadas fuera del plazo establecido o sin la debida sustentación técnica o documental

Los medios válidos de comunicación para el inicio y finalización del producto, será de manera formal mediante cartas, correo electrónico o actas entre ambas entidades.

ENTREGABLES

Para realizar la entrega del certificado, el fabricante, entidad certificadora o el postor como representante de algunas de éstas, deberá generar un nuevo certificado en el token que tiene actualmente la Superintendencia. Para ello, el postor debe asistir con dicha generación a un representante del Departamento de Desarrollo de Sistemas de la Superintendencia. De esta manera, se asegura la integridad y seguridad del proceso en todo momento. En ese sentido, el postor se comprometerá a coordinar activamente con la Superintendencia para asegurar que el proceso de generación se realice de manera eficiente y sin contratiempos. Asimismo, el fabricante, entidad certificadora o el postor deben entregar guías y/o manuales con la información pertinente sobre cómo se debe realizar el proceso de firmado digital utilizando tokens, contemplando los siguientes puntos:

- IDEs de programación en .NET: Visual Studio .NET 2019 o superior (requerido)
- IDEs de programación en Java: Eclipse (opcional), IntelliJ IDEA (opcional), NetBeans (opcional)
- Power Builder (opcional)
- Por líneas de comando (requerido)

CONFORMIDAD

La Superintendencia realizará el pago contra la entrega del certificado digital emitidos por el proveedor, luego de la conformidad otorgada por la Gerencia de Tecnologías de Información.

FORMAS Y CONDICIONES DE PAGO

El pago se efectuará contra prestación del servicio o contra entrega de los bienes, luego de la conformidad de la Gerencia de Tecnologías de Información.

El contratista será responsable por la calidad ofrecida y por los vicios ocultos del servicio, conforme a lo indicado en el Artículo 69° de la Ley de Contrataciones del Estado vigente, por un plazo de un (01) año a partir de la conformidad otorgada por parte de la Superintendencia

CLÁUSULAS ESPECIALES

a) RESOLUCIÓN CONTRACTUAL

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas, y numeral 229.3 del artículo 229 de su Reglamento.

b) ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción del contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de LA SUPERINTENDENCIA en relación con el contrato.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de LA SUPERINTENDENCIA, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA SUPERINTENDENCIA.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA SUPERINTENDENCIA el derecho de resolver total o parcialmente el contrato. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

c) SOLUCIÓN DE CONTROVERSIAS:

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante conciliación.

d) GESTION DE RIESGOS:

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación. Los riesgos identificados se encuentran descritos en el Anexo A del presente requerimiento.

NOMBRE COMPLETO DEL RESPONSABLE DEL AREA USUARIA / AREA TÉCNICA ESTRATEGICA
MARCO ANTONIO ROJAS AGUEDO JEFE DE DESARROLLO DE SISTEMAS
FECHA: 24 de Noviembre de 2025

ANEXO N° 02

<table>
<tr><th colspan="7">Formato para identificar, evaluar y asignar riesgos</th></tr>
<tr><td rowspan="3">1</td><td colspan="6">IDENTIFICACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="2">RIESGOS EN EL PROCESO DE CONTRATACIÓN (*)</td><td colspan="4">• Falta de proveedores en la interacción con el mercado</td></tr>
<tr><td colspan="2">RIESGOS EN LA EJECUCIÓN DE LA PRESTACIÓN (**)</td><td colspan="4">• Incumplimiento, retrasos en los plazos de ejecución</td></tr>
<tr><td rowspan="8">2</td><td colspan="6">EVALUACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="2">RIESGO IDENTIFICADO</td><td colspan="2">PROBABILIDAD DE OCURRENCIA</td><td colspan="2">IMPACTO EN LA EJECUCIÓN DE LA PRESTACIÓN</td></tr>
<tr><td rowspan="3" colspan="2">Falta de proveedores en la interacción con el mercado</td><td>Baja</td><td></td><td>Baja</td><td></td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td>X</td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td rowspan="3" colspan="2">Incumplimiento, retrasos en los plazos de ejecución</td><td>Baja</td><td></td><td>Baja</td><td></td></tr>
<tr><td>Media</td><td>X</td><td>Media</td><td>X</td></tr>
<tr><td>Alta</td><td></td><td>Alta</td><td></td></tr>
<tr><td rowspan="3">3</td><td colspan="6">ASIGNACIÓN DE LOS RIESGOS</td></tr>
<tr><td colspan="3">Falta de proveedores en la interacción con el mercado</td><td colspan="3">Subgerencia de Logística</td></tr>
<tr><td colspan="3">Incumplimiento, retrasos en los plazos de ejecución</td><td colspan="3">Contratista</td></tr>
</table>

(*) A identificar por parte de la SL

(**) A identificar por parte del Área usuaria