PROGRAMA DE DESARROLLO DE SANIDAD AGROPECUARIA - PRODESA: MEJORAMIENTO DEL SERVICIO DE INOCUIDAD AGROALIMENTARIA DEL SENASA

CONTRATO DE PRESTAMO N° 5941/OC-PE

ESPECIFICACIONES TÉCNICAS

"ADQUISICIÓN DE LA PLATAFORMA DE FIRMA ELECTRÓNICA (APPLIANCE HSM)"

UNIDAD EJECUTORA	Programa de Desarrollo de Sanidad Agropecuaria - PRODESA: Mejoramiento del Servicio de Inocuidad Agroalimentaria del SENASA
COMPONENTE	Componente 2. Mejora del Control de la inocuidad agroalimentaria
PRODUCTO	Sistemas de información del SENASA mejorados e interoperando
ACCIÓN	Sistema de información de alertas rápidas de inocuidad agroalimentarias diseñado e implementado
RESPONSABLE	Josue Alfonso Carrasco Valiente
DIRECCIÓN	Dirección de Insumos Agropecuarios e Inocuidad Agroalimentaria
SOLICITANTE	Ivan Pavel Angeles Nuñez
UNIDAD / SUB DIRECCION	Unidad de Informática y Estadística

1. ANTECEDENTES

Mediante Resolución DE-137/24 el Banco Interamericano de Desarrollo – BID aprueba el Préstamo No 5941/OC-PE a la República del Perú para financiar parcialmente el proyecto de inversión con CUI No 2593747 "Mejoramiento del servicio de inocuidad agroalimentaria del SENASA", tercera operación individual bajo la Línea de Crédito Condicional para Proyectos de Inversión – CCPLIP de Largo Plazo del Servicio Nacional de Sanidad Agraria – SENASA.

El 10 de junio del 2025 se suscribió con el Banco Interamericano de Desarrollo - BID el Contrato de Préstamo N° 5941/OC-PE para la ejecución del Proyecto "Mejoramiento del servicio de inocuidad agroalimentaria del SENASA" PE-L1280.

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO – Dirección de Insumos Agropecuarios e Inocuidad Agroalimentaria – V°B° – DIRECTOR GENERAL – SENASA

2. FINALIDAD PÚBLICA:

El SENASA a través del PRODESA ejecuta el "Programa de Desarrollo de Sanidad Agropecuaria", cuyo objetivo es la "Adecuada prestación del servicio de vigilancia y control de la inocuidad agroalimentaria del SENASA". El logro de dicho objetivo contribuirá al "incremento de la competitividad de los productores agropecuarios por cumplimiento de estándares de inocuidad". El resultado de las actividades implementadas en el proyecto Mejoramiento del servicio de inocuidad agroalimentaria del SENASA, es "contribuir a elevar el desempeño del sistema nacional de inocuidad alimentaria del Perú a través de un abordaje sistémico, preventivo, basado en riesgo y armonizado internacionalmente de las políticas, planes y programas de gestión de inocuidad del SENASA; cuyo propósito es que los productores agropecuarios accedan a la prestación del servicio de vigilancia y control de la inocuidad agroalimentaria del SENASA.

En ese sentido la firma de documentos mediante certificados digitales nos permite agilizar la emisión de documentos con los respectivos estándares de seguridad y la posibilidad de intercambio electrónico.

3. OBJETIVO DE LA CONTRATACIÓN:

Adquisición de la Plataforma de Firma Electrónica (Appliance HSM) para garantizar la veracidad y legalidad de los documentos emitidos por el Servicio Nacional de Sanidad Agraria mediante el uso de certificados digitales.

4. DESCRIPCIÓN DE LOS BIENES

ITEM	UNIDAD DE MEDIDA	DESCRIPCIÓN	CANTIDAD
1	Unidad	Adquisición de la Plataforma de Firma Electrónica (Appliance HSM)	1

5. CARACTERISTICAS Y CONDICIONES DE LOS BIENES:

5.1 ADQUISICION DE INFRAESTRUCTURA DE FIRMA DIGITALIZADA REMOTA

EL CONTRATISTA proveerá todos los componentes del Sistema de Firma Digital Remota (SFDR) que resulten necesarios para el cumplimiento del objetivo general y requisitos señalados en el presente documento, quedando estos en propiedad de SENASA al finalizar la implementación

- **Hardware e Infraestructura:**

a) El equipamiento permitirá la generación y almacenamiento de los pares de claves requeridos para los usuarios finales bajo los algoritmos RSA o de curva elíptica en sus variantes vigentes internacionalmente y con los parámetros exigidos bajo la IOFE o equivalentes.

b) El equipamiento permitirá su utilización como Dispositivo Cualificado de Creación de Firma (QSCD)[1] en un entorno operativo seguro y remoto. El QSCD (SAM) deberá contar con certificación bajo el estándar CEN-EN 419.241-2 (perfil de protección Common Criteria EAL4+). El postor presentará la documentación sustentatoría acompañando a su propuesta.

c) Las funciones de firma del SFDR deberán basarse en dispositivos criptográficos seguros centralizados (Hardware Security Modules-HSMs) que cuenten con certificación bajo el estándar CEN-EN 419.221-5 (perfil de protección Common Criteria EAL4+), bajo los algoritmos RSA o de curva elíptica en sus variantes vigentes internacionalmente y con los parámetros exigidos bajo la IOFE o equivalentes. El postor presentará la documentación sustentatoría acompañando a su propuesta.

[1] El uso de Dispositivos Cualificados de Creación de Firma es requerido en la Unión Europea para que una firma electrónica pueda considerarse como cualificada, modalidad de firma de alto nivel de seguridad con prerrogativas de equivalencia funcional y jurídica con la firma manuscrita, de manera equivalente a la firma digital emitida bajo la IOFE en el Perú.

d) Permitirá firmar digitalmente cualquier documento desde cualquier plataforma (escritorio y móvil) explotando un elemento seguro remoto.

e) EL CONTRATISTA deberá implementar el SFDR en los centros de datos principal y de contingencia de SENASA, bajo las políticas de seguridad de la Información.

f) La implementación deberá garantizar que el SFDR cuente con una disponibilidad mínima del 99% anual.

g) El equipamiento a ser provisto deberá ser raqueable en lo que resulte aplicable, incluyendo los servidores de aplicaciones, los dispositivos criptográficos HSM o *appliances* que incorporen ambas funcionalidades. Las características técnicas mínimas exigidas para los mismos se especifican en el **Anexo N° 1** de estas especificaciones técnicas. La infraestructura a implementarse deberá soportar una demanda concurrente o simultánea estimada de generación de 19 pares de claves RSA de 2048 bits (o de curva elíptica con un nivel de fortaleza equivalente) y de 36 firmas digitales por segundo basadas en los referidos tipos de claves.

h) Las características técnicas de cualquier otro equipamiento a proveerse serán determinadas por EL CONTRATISTA, debiendo todos los componentes del SFDR a ser provistos garantizar en su conjunto la total funcionalidad, prestaciones y requisitos establecidos para el SFDR.

i) El equipamiento debe ser nuevo para garantizar la calidad del servicio a implementarse. EL CONTRATISTA deberá presentar antes de la entrega del equipamiento documentación como copia de las Guías de Compra o Facturas de Compra con fechas iguales o posteriores a la fecha de la firma del Contrato que así lo acrediten.

j) SENASA proveerá el control de acceso físico, condiciones ambientales apropiadas y monitoreo permanente por cámaras de videograbación para el equipamiento a instalarse.

k) SENASA proveerá el acceso a redes con seguridad perimetral para el SFDR.

l) SENASA proveerá el servicio de banda ancha de acceso a Internet que se requiera para la prestación del servicio de firma digital remota.

- **Software para la infraestructura:**

a) El software permitirá la generación y almacenamiento de los pares de claves requeridos para los usuarios finales bajo los algoritmos RSA o de curva elíptica en sus variantes vigentes internacionalmente y con los parámetros exigidos bajo la IOFE.

b) El *SFDR* debe contener los módulos SIC, SSA y QSCD. Las características técnicas mínimas exigidas para los mismos se especifican en el **Anexo N° 2** de estas especificaciones técnicas

c) El software permitirá que el SFDR ofrezca un servicio de Dispositivo Cualificado de Creación de Firma (QSCD) en un entorno operativo seguro y remoto. El QSCD (SAM) deberá contar con certificación bajo el estándar CEN-EN 419.241-2 (perfil de protección Common Criteria EAL4+). El postor presentará la documentación sustentatoria acompañando a su propuesta.

d) El SFDR debe integrarse con la Infraestructura de SENASA y el almacenamiento de los Certificados Digitales dentro del SFDR. El proceso de integración a efectuarse por EL CONTRATISTA se describe a continuación:

- El SFDR genera el par de llaves de tipo RSA o curva elíptica según corresponda.
- El SFDR vincula el par de llaves generado a la identidad del individuo cuyos datos se proporcionó, generando las solicitudes de certificados *(Certificate Signing Requests, CSRs).*
- Las solicitudes (archivos CSRs) en formato. PEM codificado en base64 son devueltas al software que ha iniciado la comunicación.
- A través del SFDR, se emite el certificado digital en base al CSR correspondiente y lo envía al SFDR por intermedio de la interface web REST para su almacenamiento correspondiente.
- El SFDR no almacena datos biográficos de las personas fuera de lo contenido en sus certificados. Sí almacena las llaves privadas asociadas.

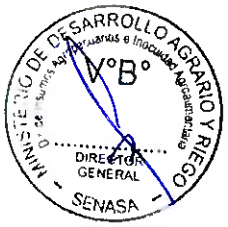
e) Deberá soportar certificados digitales emitidos bajo el estándar RFC 5280.

f) El SFDR debe disponer de un componente de software o herramienta para monitorear el estado de salud de sus componentes y la disponibilidad de los servicios o funcionalidades del SFDR. El componente de software o herramienta de monitoreo permitirá como mínimo:

- Monitorear en tiempo real las transacciones y estado de los recursos de la infraestructura de red del sistema de firma remota, el nivel de servicio, la carga y las caídas (down-times), informando instantáneamente 24 horas al día, 365 días al año, en los casos en los que se produzca un fallo en alguno de los elementos monitorizados.
- Generar alarmas de notificación. Cuando se produzca un cambio de estado se disparará una alerta que produce una notificación en tiempo real al responsable del servidor, servicio o elemento de red.

g) El SFDR dispondrá de un componente de software estadístico y de monitoreo de la producción que presentará en forma gráfica, numérica y en tiempo real a través de un dashboard como mínimo las cifras de generación de pares de claves, emisión de solicitudes de certificados (CSRs), generación de firmas digitales, entre otras en línea y en periodos de tiempo configurables. El componente estadístico generará asimismo reportes estadísticos con posibilidad de exportación a formato Excel.

h) El SFDR deberá guardar el registro de un log donde se detalle lo requerido bajo el estándar EN 419.241-1, incluyendo las firmas realizadas por los certificados almacenados, el instante de realización y el usuario que lo utilizó. Igualmente, se registrarán en un log todas las operaciones de administración del sistema y de los certificados almacenados. Se dispondrá de logs diferenciados para la plataforma de administración del SFDR y para el servicio de creación de firma digital remota. Los logs generados deberán poder ser exportados a través del protocolo y/o



interfaces correspondientes de manera programada y configurable.

i) Todos los procedimientos de administración del SFDR, la gestión de los usuarios, sus claves, etc. deberán poder realizarse de forma remota y en tiempo real. El software de administración del SFDR deberá brindar protección de la consola de administración mediante el protocolo HTTPS. Los certificados SSL necesarios serán provistos por el contratista como parte de la implementación del software, para lo cual coordinará con el RENIEC para los nombres de dominio correspondientes.

- ***Software* cliente *y middleware para computadoras de escritorio (PCs o laptops):***

a) EL CONTRATISTA deberá proporcionar un software de tipo cliente y middleware que permita a los softwares de firma digital acreditados frente a la IOFE interactuar con el SFDR de forma transparente al usuario final, para lo cual no se requerirá que los softwares de firma digital tengan que ser modificados o integrados con el SFDR.

b) Este software debe estar disponible para entornos Windows, versión 10 en adelante, debe interactuar entre el software de firma digital remota que menciona el punto precedente, en el momento de requerir el acceso a la llave privada del usuario final, redireccionando la petición al SFDR en donde se encuentra dicha llave privada.

c) Para los fines de identificación y autenticación a efectos de la matrícula de afiliación del usuario frente al SFDR y para el inicio de sesión frente al SFDR el software cliente deberá interoperar con los servicios de identificación/autenticación, debiendo cumplirse con los requisitos del estándar CEN-EN 419.241-1 para el nivel de certeza en el control exclusivo de la clave 2 (SCAL2), incluyendo identificación con doble factor y autenticación con factor de tipo dinámico. La integración que resultase necesaria será efectuada por EL CONTRATISTA,

d) Se contemplará el caso de uso en el que el usuario acceda a una plataforma web desde la cual a través de un software de firma integrado a la misma deba firmar digitalmente documentos electrónicos, cumpliendo en este caso la funcionalidad de middleware; como también el caso de uso en el que se dispone de documentos electrónicos en formato PDF remitidos, por ejemplo, adjuntos a un mensaje de correo electrónico, los cuales deberán ser firmados por los softwares de firma digital existentes.

e) El software deberá cumplir con los requisitos de la norma CEN-EN 419.241-1 para el nivel de certeza en el control exclusivo de la clave 2 (SCAL2) en todos los aspectos de su diseño y desarrollo.

f) El software será proporcionado a SENASA con licenciamiento perpetuo y para una cantidad ilimitada de usuarios.

g) El software dispondrá de un instalador que verificará los prerrequisitos de instalación señalando cualquier incumplimiento y que, de manera automática para el caso de softwares requeridos como prerrequisito, los incorporará o descargará instalándolos previamente a la instalación del software. De presentarse un error al momento de la instalación, generará un log que podrá ser exportado para su análisis.

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
V°B°
DIRECTOR GENERAL
SENASA

h) Deberá poderse acceder a los instaladores y los instructivos correspondientes, manual de usuario, video instructivo, etc., como recursos que forman parte del software requerido en una parte pública accesible del SFDR, a fin de que el usuario final pueda instalarlos y revisarlos en su computadora de escritorio.

5.2 INTEGRACION DE FIRMA DIGITALIZADA EN 2 APLICACIONES DE SENASA

a) Integración total del servicio con 2 sistemas institucionales de SENASA (Reporte de Inspección y Verificación- RIV Digital y Sistema de Gestion Documental-SGD), mediante el desarrollo de las adecuaciones técnicas necesarias para garantizar la interoperabilidad y el intercambio seguro de información entre plataformas.

b) El servicio web de integración de los procesos de firma requerido, deberá utilizar los componentes de firma digital y validación de firmas digitales asociados a los sistemas de SENASA

c) El servicio web de integración de los procesos de firma digital requerido, será utilizado para proveer procesos de firma digital y validación de firma digital, a otros sistemas institucionales de SENASA, cuyos flujos de procesos incluyan requerimientos de firma digital y validación de firmas digitales. La integración de los sistemas de información institucionales con el servicio web de firma digital y validación de firmas digitales, se realizará mediante la invocación al mencionado servicio y el intercambio de parámetros de información correspondientes.

d) El servicio web de integración de los procesos de firma digital y validación de firmas digitales requerido debe permitir operaciones de firma digital en lote.

e) El proveedor ejecutará los procesos de adecuación e integración necesarios para conectar el servicio de firma digital con los sistemas core institucionales de SENASA, respetando las políticas de acceso, seguridad y control definidas por la entidad.

f) Los procesos de integración y adecuación de las soluciones core, se realizarán de manera externa a la solución de firmas digitales.

g) El proveedor accederá a las soluciones de SENASA para ejecutar los procesos de adecuación e integración de los servicios requeridos para la integración de los sistemas de firma digital.

h) Acompañamiento técnico durante las pruebas de integración y validación, garantizando la correcta adopción del servicio por parte de los sistemas de información institucionales.

i) Toda integración se realizará sin alterar la lógica funcional principal de los sistemas institucionales, preservando su operatividad y garantizando compatibilidad con futuras actualizaciones

6. DE LA IMPLEMENTACION

El contratista, deberá realizar La instalación y configuración en un plazo máximo de diez (10) días calendarios contados a partir del día siguiente de la entrega del total de los bienes en las instalaciones del SENASA, ubicado en la avenida la Molina 1915 – La Molina, lo cual deberá incluir la instalación física, configuración y puesta en marcha de los equipos.

La integración de la firma digitalizada en las aplicaciones del SENASA deberá realizarse en un plazo máximo de veinte (20) días calendarios contados a partir

del día siguiente de la instalación y configuración de los bienes en las instalaciones del SENASA.

La información y accesos serán otorgados al contratista a solicitud, así como se desocupará los espacios, oficinas y/o pasillos donde vayan a ser ejecutados los respectivos trabajos de instalación y se realizará en coordinación con el área de infraestructura de la Unidad de Informática y Estadística.

El contratista deberá entregar un informe al finalizar la implementación con diagramas y configuraciones realizadas.

7. SOPORTE

a) El CONTRATISTA, al igual que el fabricante, deberán brindar el servicio de soporte el periodo de Treinta y seis (36) meses en la modalidad 24x7x365, contabilizados a partir del día siguiente de haberse otorgado la conformidad.
b) El SENASA podrá abrir casos directamente con el fabricante, de requerirlo, por lo que el CONTRATISTA deberá brindarle los accesos correspondientes.
c) El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio del SENASA, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".
d) El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".
e) El servicio de soporte técnico comprenderá la instalación de parches, actualizaciones, hotfixes, nuevas versiones, mejoras en la arquitectura, reglas, políticas, releases, etc. de la solución ofertada.
f) El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.
g) El servicio de soporte técnico se efectuará a través de un servicio en la nube, línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, el Centro de Atención al Cliente o SOC del CONTRATISTA, registrará el requerimiento y/o falla del servicio y proporcionará al SENASA un número de ticket.
h) Tiempo de solución: Es el tiempo que toma el personal técnico designado por el contratista para brindar el soporte, atender el requerimiento o fallas reportadas, contabilizado desde que se emite el ticket de atención. El CONTRATISTA deberá enviar el ticket de atención vía correo electrónico, en un tiempo máximo de 15 minutos de reportado el problema y deberá enviar un mail a la culminación del soporte, resolución del requerimiento o falla reportada, en el cual deberá indicar las acciones que se tomaron y el tiempo de solución.
i) Niveles de atención del servicio acordado (SLA) de soporte debe ser el siguiente:

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
V°B°
DIRECTOR GENERAL
SENASA

Tipo	Descripción de la Falla	Tiempo máximo de respuesta en la atención
Falla Grave	Se deberá cumplir cualquiera de los siguientes puntos: ✓ Interrupción total del servicio o degradación del servicio brindado por la solución ofertada.	04 horas
Falla Leve	Se deberá cumplir cualquiera de los siguientes puntos: ✓ Falla en alguna funcionalidad que no afecta ni pone en riesgo el servicio brindado por la solución ofertada.	08 horas
Requerimiento	Consultas y/o solicitudes de informes o de cambio de configuración.	24 horas

8. PERFIL DEL PROFESIONAL REQUERIDO:

8.1 Formación Académica

- **Gerente de Proyectos:**
  Profesional titulado en Ingeniería de Sistemas y/o Informática y/o Telecomunicaciones y/o Electrónica y/o Telecomunicaciones
- **Especialista en Ciberseguridad**:
  Profesional titulado en Ingeniería o Bachiller en Ingeniería de Sistemas y/o Redes y Comunicaciones y/o Informática o Telecomunicaciones

8.2 Experiencia Profesional

- **Gerente de Proyecto:** Será el responsable de planificar, coordinar, supervisar y garantizar la correcta implementación de los equipos de seguridad perimetral.
  - **Experiencia General:** Experiencia de trabajo de tres (03) años como Gerente y/o Jefe y/o Gestor, de Proyecto en Tecnologías de la Información.
  - **Experiencia Especifica:** (03) años en la especialidad de Tecnología de la información y/o seguridad de la información

- **Especialista en Ciberseguridad:** Será el responsable de la implementación y soporte Postventa.
  - **Experiencia General:** cinco (05) años en el ejercicio de su profesión en el sector público y/o privado.
  - **Experiencia Especifica:** Experiencia de trabajo Mínimo tres (03) años de experiencia en instalación de Sistemas de Firma Digital

9. TRANSFERENCIA DE CONOCIMIENTO

El contratista deberá brindar una transferencia de conocimiento de doce (12) horas para cinco (05) personas, sobre la arquitectura y administración de la solución, debiendo entregar constancias de participación a los asistentes

10. GARANTÍA

El proveedor deberá entregar una carta de garantía del fabricante o equivalente en la modalidad 24x7, el cual asegure que los equipos ofrecidos contarán con una garantía de funcionamiento y soporte técnico por un periodo no menor de tres (3) años; además de consignar un canal de comunicaciones en el cual se entregue el soporte técnico del producto ofrecido.

Adquisición de la Plataforma de Firma Electrónica (Appliance HSM), deberán contar con garantía y soporte del fabricante en la modalidad de 24x7 por los 36 meses del contrato y que incluya el reemplazo de componentes en caso de fallas. Este soporte debe permitir que la entidad pueda crear sus propios casos directamente con la marca.

11. REPOSICIÓN DEL BIEN DEFECTUOSO

La reposición de componentes y/o equipo en caso de fallas, deberá efectuarse en un plazo no mayor a tres (03) días calendarios, a partir de la notificación del hecho.

12. LUGAR Y PLAZO DE EJECUCIÓN DE LA PRESTACIÓN

LUGAR:

Sede Central del SENASA, ubicada en la Av. La Molina N°1915 (REF: Puerta N°01 de la Universidad Agraria), de lunes a viernes en el horario de 9:00 a.m. a 13:00 p.m. y desde las 14:00 p.m. a 17:00 p.m.

PLAZO:

Los bienes serán entregados en un plazo máximo de treinta (30) días calendario, contados a partir del día siguiente de notificado la orden de compra.

- La instalación y configuración deberá realizarse en un plazo máximo de diez (10) días calendario contados a partir del día siguiente de la entrega del total de los bienes en las instalaciones del SENASA, lo cual deberá incluir la instalación física, configuración y puesta en marcha de los equipos.
- La integración de la firma digitalizada en las aplicaciones del SENASA deberá realizarse en un plazo máximo de veinte (20) días calendario contados a partir del día siguiente de la instalación y configuración de los bienes en las instalaciones del SENASA.

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO – SENASA – DIRECTOR GENERAL – V°B°

13. REQUISITOS DE CALIFICACION

El postor debe acreditar un monto facturado acumulado equivalente al valor de su oferta total en la venta de bienes iguales o similares al objeto de la convocatoria, durante los cinco (5) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes: Implementación de Servicios de Firma Digital, Servicios de Valor añadido acreditado en Indecopi, Servicios con Servidores HSM para uso de Firma Digital

Acreditación:
La experiencia del postor en la especialidad se acreditará con copia simple de (i)

contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes.

Otros Requisitos

- El Postor Deberá tener Certificaciones de Seguridad y Calidad que garanticen la idoneidad del Sistema de Firma Digital Remota, de manera específica:
  - ISO 27001: 2022 Sistema de Gestión de Seguridad de la información, Ciberseguridad y Protección de Datos
  - ISO 9001: 2015 Sistema de Gestión de la Calidad
- El Postor deberá, tener acreditada Firma Digital Remota ante el INDECOPI, que garantice el cumplimiento de lo establecido en la normatividad vigente

14. FORMA DE PAGO:

La Entidad paga las contraprestaciones pactadas a favor del proveedor, dentro de los quince (15) días calendarios siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato u orden de compra para ello, bajo responsabilidad del funcionario competente.

El pago se efectuará en soles, PAGO UNICO; para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Comprobante de pago.
- Carta de garantía.
- Acta de conformidad/Memorándum o equivalente emitida por el área usuaria.

15. CONFORMIDAD

La conformidad estará a cargo de la Dirección General de Insumos Agropecuarios e Inocuidad Agroalimentaria y la Unidad de Informática y Estadística de la Dirección General de Planificación y Desarrollo Institucional del SENASA, en un plazo que no exceda de siete (07) días calendario para el trámite de pago; de existir observaciones, la Entidad las comunica al proveedor, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (08) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar.

Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la Entidad puede otorgar al contratista periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo.

16. PENALIDAD

Penalidades por mora:

Se aplicará al proveedor la penalidad establecida en el artículo 120° numeral 120.1. del Reglamento de la Ley de Contrataciones del Estado. En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F} \times \text{Plazo}$$

Donde F tendrá los siguientes valores:

Para bienes y servicios: F = 0.40

En caso de cubrir el monto máximo de la penalidad, se podrá resolver el contrato por incumplimiento

17. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del bien ofertado por un plazo de un (03) años, contado a partir de la conformidad otorgada por la Entidad

18. CONFIDENCIALIDAD

El proveedor, guardará, bajo responsabilidad a que hubiere lugar, estricta confidencialidad respecto de la información que recabe con ocasión de las visitas a las instalaciones de la institución, así como de la información que genere, no pudiendo emplear dicha información para un fin distinto al contratado.

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
SERVICIO NACIONAL DE SANIDAD AGRARIA
OFICINA DE PLANIFICACIÓN Y DESARROLLO INSTITUCIONAL
UNIDAD DE INFORMÁTICA Y ESTADÍSTICA

Ing. IVAN PAVEL ANGELES NUÑEZ
Director
Firma

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
SERVICIO NACIONAL DE SANIDAD AGRARIA
DIRECCIÓN DE INSUMOS AGROPECUARIOS E INOCUIDAD AGROALIMENTARIA

Ing. Josue A. Carrasco Valiente
Director General
Firma

ANEXO N°1 – ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL DISPOSITIVO CRIPTOGRÁFICO HSM*

Descripción	Característica
Cumplimiento de estándares	EN 419 221-5, cumple como servidor de firma remota según EN 419 241-2
Certificación	eIDAS y Common Criteria EAL4 + AVA_VAN.5 y ALC_FLR.2 según el perfil de protección EN 419 221-5
Formatos de firma admitidos:	RSA, PAdES, CAdES, XAdES
Algoritmos de firma soportados	RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
Longitudes de claves admitidas	RSA 2048, 3072, 4096, 8192
Algoritmos de hash admitidos	SHA-2, SHA-3
Algoritmos de cifrado	AES, AES-GCM, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES
Rendimiento de firma	Al menos 3000 tps para claves RSA de 2048 bit
Formato	Rackeable
Alimentación	220V, 60Hz o auto voltaje y auto frecuencia que comprenda los mismos

Nota: el dispositivo criptográfico HSM podrá encontrarse integrado con el servidor en un *appliance.*

ANEXO N°2 – ESPECIFICACIONES TÉCNICAS MÍNIMAS DEL SERVIDOR DE APLICACIONES

Descripción	Característica
Procesador	Al menos dos unidades con 24 núcleos y 48 subprocesos con frecuencia base de 3,00GHz
Memoria	Al menos 256GB de ECC RDIMM, 4800 MT/s
Almacenamiento	Al menos 6 unidades de 2,0 TB unidades de estado sólido NVMe en configuración RAID 10
Fuente de poder	Dual con hot swap
Red	Al menos dos puertos 10GbE o superiores
Sistema operativo	Linux sin licenciamiento comercial
Virtualización	Docker
Formato	Rackeable
Alimentación	220V, 60Hz o auto voltaje y auto frecuencia que comprenda los mismos
Controladora de almacenamiento RAID	RAID de hardware
Administración server	Puerto de administración por red

Nota: el servidor de aplicaciones criptográfico podrá encontrarse integrado con el HSM en un *appliance.*

MINISTERIO DE DESARROLLO AGRARIO Y RIEGO
V°B°
DIRECTOR GENERAL
SENASA