I. OBJETIVO

Contratar un servicio de validación de identidad de personas que permita a Caja Maynas verificar de forma automatizada la identidad de las personas desde sus canales digitales.

II. PLAZO

- ✓ **Plazo de la integración**: 30 días calendarios.
- ✓ **Plazo del servicio**: debe ser de 12 meses, renovables de forma automática por periodo similares; contados desde el día siguiente de culminado la integración.

III. CARACTERÍSTICAS DEL PROVEEDOR

El proveedor debe cumplir con las siguientes características mínimas:

- ✓ Debe ser una empresa perteneciente al sector de las tecnologías de la información y comunicaciones o FinTech con servicios de firma digital, validación de identidad de personas y afines.
- ✓ Debe contar con experiencia mínima de 5 años brindando servicios de firma digital, firma electrónica, OnBoarding o verificación de identidad de personas. Asimismo, debe brindar o haber brindado dichos servicios a por lo menos 1 entidad perteneciente al sistema financiero peruano.
- ✓ Debe tener la capacidad de emitir certificados digitales seguros ya sea directa o indirectamente a través de un prestador de servicios de confianza y/o entidad emisora de certificados (AC) debidamente registrado ante el Registro Oficial de Prestadores de Servicios de Certificación Digital (ROPS) de INDECOPI.
- ✓ Debe tener la capacidad de emitir certificados digitales seguros para la entidad ya sea directa o indirectamente a través de un prestador de servicios de confianza que esté debidamente reconocido por Adobe y que sea miembro activo y vigente del programa Adobe Approved Trust List (AATL).
- ✓ Debe contar con canales de atención que permita a Caja Maynas reportar los incidentes del servicio y puedan ser atendidos por el proveedor.
- ✓ Debe estar integrado con los servicios asociados a la validación de identidad de personas de la RENIEC, cumpliendo con las normativas y estándares establecidos por la entidad.

Los cumplimientos del proveedor podrán ser sustentadas por medio de contratos, certificados, cartas, órdenes de servicio, u otros documentos que haga referencia a lo requerido.

Gerente de Operaciones y Canales
VºBº
Danny Dan Ordoñez Torres
CMAC MAYNAS S.A.

CAJA MUNICIPAL DE MAYNAS S.A
DEPARTAMENTO DE LOGÍSTICA
28 SEP. 2024
RECIBIDO
LA RECEPCION DEL PRESENTE NO SIGNIFICA LA CONFORMIDAD DEL MISMO
HORA: 11:07 AM

IV. CARACTERÍSTICAS DEL SERVICIO

El servicio de validación de identidad de personas debe contar con las siguientes características mínimas:

- ✓ Debe poder integrarse a los diversos canales digitales de Caja Maynas: sitio web, Banca por Internet y Banca Móvil (App en Android e iOS).
- ✓ Debe contar con una interfaz de programación (API) que realice la validación de identidad de la persona, con lo siguiente:
  - La captura, mediante la cámara de los dispositivos, del anverso y reverso del DNI, y verificar que sea un DNI válido. Mediante técnicas de reconocimiento óptico de caracteres (OCR) deberá obtener y proporcionar los siguientes datos del anverso del DNI: nombres, apellidos, país, sexo, fecha de nacimiento, estado civil, fecha de expiración y ubigeo. Además, del reverso deberá obtener y proporcionar el número del DNI.
  - La captura, mediante la cámara de los dispositivos, del rostro de la persona y realizar la validación biométrica facial con la RENIEC. Durante la validación con la RENIEC deberá obtener y proporcionar, por lo menos, los siguientes datos: resultado de validación, número de DNI, nombres, apellidos y fecha de expiración.
  - Debe poder realizar el reconocimiento de la presencia física y viva de la persona (prueba de vida) en el momento que esté realizando el proceso de validación de identidad, con el fin de evitar ataques de presentación; debiendo utilizar un enfoque pasivo de una sola imagen del tipo selfie (captura del rostro) que pueda ser utilizada simultáneamente para la comparación biométrica facial con RENIEC y la detección de prueba de vida a través de Inteligencia Artificial (IA).
  - La validación de identidad de una persona consiste en el uso en conjunto de: la captura del rostro y validación biométrica con RENIEC, la captura del anverso y reverso del DNI y determinar si corresponde a un DNI válido, y la prueba de vida de la persona. Asimismo, proporcionar los datos según lo descrito en los ítems anteriores.

- ✓ Utilizar tecnologías de prueba de vida pasiva que implemente la Detección de Ataques de Presentación (PAD) que cumplan con el estándar ISO/IEC 30107-3 y en conformidad con el marco ISO/IEC 30107-1, certificadas por una entidad acreditado por el Instituto Nacional de Estándares y Tecnología (NIST) bajo el Programa Nacional de Acreditación Voluntaria de Laboratorio (NVLAP).
- ✓ Deberá emplear métodos y/o tecnologías e almacenamiento seguras e inalterables, tales como blockchain, que aseguren salvaguardar el registro de la información del proceso de validación de identidad.
- ✓ Debe contar con una plataforma o sistema en entorno web, que permita lo siguiente:
  - La gestión de accesos a la plataforma web a través de diferentes usuarios (multi-usuarios), permitiendo asignar privilegios para la habilitación o bloqueo de características del sistema, mediante listas de control de accesos, en función al perfil de usuario.

Gerente de Operaciones y Canales
VºBº
Danny Dan Ordoñez Torres
CMAC MAYNAS S.A.

- La verificación de todos los pasos realizados con el API en el proceso de validación de identidad de las personas, que incluye las capturas del DNI y captura del rostro realizados.
- Contar con un historial o registro (log) que muestre todo el proceso o actividad al momento de realizar el proceso de verificación de identidad, almacenando las evidencias colectadas durante el proceso.
- Contar con reportes que permita obtener información relevante y detallada de los procesos de validación de identidad realizados.

✓ El servicio debe contar con alta disponibilidad, debiendo estar operativo las 24 horas del día y los 365 días del año. En caso de mantenimiento de los sistemas que forman parte del servicio, el proveedor deberá comunicar con una anticipación mínima de 7 días calendarios. Asimismo, los mantenimientos deberán realizarse en horas de la noche, a partir de las 22 horas.

V. CARACTERÍSTICAS DE LA INTEGRACIÓN

✓ La solución deberá contar con una interfaz de programación (API) y acceso a la documentación, que permita la integración con las aplicaciones y/o sistemas de Caja Maynas.

✓ Deberá contar con ambientes de pruebas disponibles para la certificación del correcto funcionamiento sobre funcionalidades o cambios requeridos por Caja Maynas.

✓ El proveedor deberá brindar orientación técnica para la correcta integración con los sistemas de Caja Maynas y brindar acompañamiento durante todo el tiempo que tome la integración.

✓ Culminado la integración, se deberá suscribir un acta entre ambas partes.

VI. CARACTERÍSTICAS DE SEGURIDAD

✓ Debe contar con auditorías externas para la revisión de la seguridad de la información gestionadas en la solución de firma electrónica y validación de identidad de personas.

✓ El proveedor deberá tomar conocimiento de las obligaciones establecidas en la ley de protección de datos personales (Ley 29733), con el propósito de que el servicio ofrecido cumpla con lo establecido en dicha Ley.

Gerente de Operaciones y Canales VºBº Danny Dan Ordoñez Torres CMAC MAYNAS S.A.

✓ El Proveedor deberá tener conocimiento de las obligaciones establecidas en la Resolución SBS 504-2021 Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, con el propósito de que el servicio ofrecido cumpla con lo establecido en dicha norma.

✓ Deberá contar con mecanismos de doble factor de autenticación (2FA) para confirmar la identidad de los usuarios de la organización al portal web de la herramienta de manera segura.

✓ La solución debe contar con archivos de log de eventos, tanto del tipo FrontEnd; como Backend.

Los cumplimientos del proveedor podrán ser sustentadas por medio de contratos, certificados, cartas, órdenes de servicio, u otros documentos que haga referencia a lo requerido.

VII. CAPACITACIÓN

El postor deberá cumplir con las siguientes condiciones de capacitación:

- ✓ Debe brindar sesiones de transferencia de conocimiento, de manera remota, que incluyan, como mínimo, la explicación detallada de cada una de las funcionalidades disponibles, configuraciones, administración de la solución, generación de estadísticas entre otras relevantes al mejor uso de esta.
- ✓ Debe entregar manuales que incluyan, como mínimo, el diagrama de la arquitectura de la solución y una breve explicación de cada uno de los componentes que conformen la misma.
- ✓ Debe entregar manuales del tipo "usuario", que incluyan, como mínimo, la documentación de todas las funcionales de la solución y los pasos a seguir para su debido uso.
- ✓ Debe contar con información/documentación de los procedimientos a seguir en caso de registro de reporte de incidencias y/o consultas.

VIII. CAUSALES DE AMPLIACIÓN DE PLAZOS

Se podrá ampliar excepcionalmente los plazos para la ejecución de la prestación cuando se presente alguno de los siguientes supuestos:

- Causas no atribuibles al contratista.
- Caso fortuito o fuerza mayor debidamente comprobado.

Toda solicitud de ampliación de plazo deberá efectuarse dentro del plazo de vigencia del contrato u orden de servicio, debidamente sustentada. La ampliación del plazo será aprobada por el área usuaria, informando al departamento de Gestión de Logística dicha ampliación adjuntando el sustento de aprobación.

IX. PENALIDADES

De la Integración:

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA CAJA aplicará al contratista una penalidad por cada día calendario de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto la ODS vigente. - En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

Gerente de Operaciones y Canales
VºBº
Danny Dan Ordoñez Torres
CMAC MAYNAS S.A.

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde:
Para plazos menores o iguales a sesenta (60) días, para bienes y servicios F = 0.40
Para plazos mayores a sesenta (60) días, para bienes y servicios F = 0.25

Cuando se llegue a cubrir el monto máximo de la penalidad, LA CAJA podrá resolver la Orden de Servicio por incumplimiento.

Del servicio de validación de la identidad de la persona:

Si al momento de acceder al API del servicio de validación de identidad de la persona, éste no se encuentre disponible por parte del postor, LA CAJA aplicará una penalidad de acuerdo al monto por transacción de la tarifa, hasta por un monto máximo equivalente al diez por ciento (10%) de la tarifa mensual acerca del servicio de validación de identidad.

X. FORMA DE PAGO

El postor deberá establecer un modelo de cobro de los servicios mediante una tarifa por cada validación de identidad de persona que se realice. Asimismo, deberá establecer tarifas según rango de transacciones de validación. El postor también podrá establecer un consumo mínimo mensual de transacciones de validación de identidad. Los pagos se realizarán de forma mensual, y el monto total a pagar será acorde al número de transacciones de validación de identidad realizados o utilizados por Caja Maynas. El postor deberá incluir el rango mínimo de 1 a 1,000 transacciones mensuales de validación de identidad de personas.

La tarifa de validación de identidad del proveedor y los pagos mensuales que realice Caja Maynas por uso de las transacciones de validación de identidad incluye a todo costo los aspectos detallados en el presente documento.

A modo de ejemplo se muestra una forma de tarifas por rango de transacciones de validación de identidad:

Rango Inicial	Rango Final	Tarifa
De 1	A 1,000	Monto de tarifa
De 1,001	A 2,000	Monto de tarifa
De 2,001	A 5,000	Monto de tarifa
De 5,001	A más	Monto de tarifa

Gerente de Operaciones y Canales
VºBº
Danny Dan Ordoñez Torres
CMAC MAYNAS S.A.

El postor podrá establecer un costo inicial por concepto de setup e integración al sistema de Caja Maynas, y en caso la propuesta del postor incorpore conceptos de costos adicionales deberá precisarlo con el detalle correspondiente.

XI. CONFIDENCIALIDAD

El proveedor guardará reserva respecto de las actividades y acciones encomendadas, así como de la información privilegiada que le concierne en el ejercicio de su actividad, no revelando en forma oral o escrita, hechos, datos, procedimientos y documentación no autorizada o confidencial de acuerdo a Ley.

XII. ACCESO A LA INFORMACIÓN

El proveedor debe facilitar la entrega de cualquier información requerida por la UAI, OCI, SAE, CGR, SBS o cualquier ente de control, relacionado con el ejercicio del presente servicio.