

# **BASES**

## **Concurso de Méritos N° 0004-2026-BN**

### **Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente**

**2026**

## DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios generales del derecho público que resulten aplicables al presente proceso de contratación.

En este contexto, se encuentran obligados a prestar su colaboración a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento de la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.



## CAPÍTULO I

### 1. DISPOSICIONES GENERALES Y SERVICIO A CONTRATAR

#### 1.1 OBJETO DEL PROCESO DE CONCURSO DE MERITOS

El Banco de la Nación convoca a un concurso de méritos para contratar una empresa especializada, para que preste el Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente, con la finalidad de reforzar la seguridad durante la realización de operaciones con tarjeta NO presente en las redes de pago Visa y Mastercard, cumpliendo así con las disposiciones dadas por la SBS (Superintendencia de Banca, Seguros y AFP) respecto a estos temas.

Asimismo, es objeto implementar el CVV2 Dinámico como segundo factor de autenticación durante la realización de operaciones con tarjeta NO presente, dando cumplimiento a lo establecido por la SBS en su Resolución N° 2286-2024; así como, reducir el riesgo de pérdidas para el Banco a causa de reclamos de clientes por el no reconocimiento de operaciones con tarjeta NO presente en comercios que no participan de 3DS.

#### 1.2 ALCANCE DEL REQUERIMIENTO

El alcance de la prestación del servicio está definido en el numeral 7 del Anexo N° 1 - Términos de Referencia, de la presente bases.

#### 1.3 CONDICIONES DEL SERVICIO

##### 1.3.1 VALOR REFERENCIAL

El valor referencial del presente Concurso de Méritos es de **US\$. 1,097,800.00 (Un Millón Noventa y Siete Mil Ochocientos con 00/100 Dólares Americanos)**, el cual incluye todos los tributos, los costos laborales conforme a la legislación vigente; así como, cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar.

##### 1.3.2 MODALIDAD DE PAGO

La contratación se regula por el Sistema Esquema Mixto de Suma Alzada y Precios Unitarios: A suma alzada el servicio de implementación/configuración del del servicio generación y validación de CVV2 dinámico y el soporte técnico y, a precios unitarios los servicios transaccionales, descrito en el numeral 6 del Anexo N° 1 - Términos de Referencia de la presente bases.

##### 1.3.3 LUGAR Y PLAZO DE PRESTACION DEL SERVICIO

###### 1.3.3.1 Lugar

La prestación del servicio se prestará de forma remota.

### 1.3.3.2 Plazo

El plazo de prestación del servicio queda establecido en:

- a) Dos semanas (15 días calendarios) para el Kick off y la planificación del proyecto.
- b) Ocho (08) meses calendarios por la Implementación del servicio de generación y validación del CVV2 dinámico para tarjetas de débito del BN (lo que se evidenciará con la emisión del acta de conformidad correspondiente por parte del Banco)
- c) Ocho (08) meses calendarios por la Implementación del servicio de generación y validación del CVC2 dinámico para tarjetas de crédito del BN (lo que se evidenciará con la emisión del acta de conformidad correspondiente por parte del Banco)
- d) Servicio Transaccional (generación y validación de CVV2/CVC2 dinámico): Treinta y seis (36) meses. Se empieza a ejecutar una vez culminada la implementación del primer componente transaccional (independientemente de cuál de los 2 sea) en el ambiente de producción.
- e) Soporte Técnico: Treinta y seis (36) meses, paralelo a la prestación del servicio transaccional en producción.

Las implementaciones descritas en los literales b) y c) se deben ejecutar en paralelo.

El plazo de EL CONTRATO será por un periodo de cuarenta y cuatro (44) meses y dos (2) semanas, el cual rige desde la fecha de su firma, conforme se establece en el numeral 14.2 de los Términos de Referencia del Anexo N° 1 de la presente bases. Por la prestación del servicio transaccional y de soporte técnico (que ambos tienen un plazo de 36 meses), éstos podrán ser renovados antes de su vencimiento y por el mismo periodo de 36 meses; lo cual se materializara mediante suscripción de una adenda.

Sin perjuicio de ello, cualquiera de LAS PARTES podrá resolver EL CONTRATO de forma unilateral sin expresión de causa, comunicándolo por escrito a su contraparte con al menos un (1) año de anticipación antes del vencimiento del plazo contractual en curso.

El Plan de Implementación Base se presenta en el numeral 14.2 Plazo del Anexo N° 1 - Términos de Referencia de la presente bases.

Los plazos de Implementación de Componentes Transaccionales del Servicio y el Plan de Implementación Bases, se presenta en el numeral 14.2 del Anexo N° 1 - Términos de Referencia, de la presente bases.

### 1.3.4 ADMINISTRADOR DEL CONTRATO Y MEDIDAS DE CONTROL

#### a) Administrador del Contrato

La Subgerencia Canales Alternos de la Gerencia Banca Digital, a través de la Sección Canales Virtuales se encargará de la administración del contrato, siendo responsable de la supervisión y coordinación de la prestación contratada.

#### b) Medidas de Control

La Subgerencia Canales Alternos, de la Gerencia Banca Digital, a través de la Sección Canales Virtuales, durante la ejecución contractual desarrollará las siguientes actividades de control:

- Verificar el cumplimiento de las características y condiciones técnicas establecidas en el Anexo N° 1 - Términos de Referencia de la presente bases.
- El personal designado por la Sección Canales Virtuales al detectar observaciones durante la prestación del servicio, las mismas serán puestas de conocimiento al contratista, otorgándosele un plazo de dos (02) a ocho (08) días calendario para sus subsanaciones. La subsanación de las observaciones no exime al contratista de ser penalizado.

### 1.3.5 FORMA DE PAGO

El pago se realizará en la moneda nacional (soles) por la prestación efectiva del servicio instalado. En el caso de propuestas presentadas en moneda extranjera, el pago se ajustará al tipo de cambio Venta Promedio Ponderado, publicado por la Superintendencia de Banca y Seguros (SBS) en la fecha del registro contable de los pagos. Este proceso se llevará a cabo luego de recibir de manera formal y completa toda la documentación correspondiente.

Este proceso se llevará a cabo luego de recibir de manera formal y completa toda la documentación correspondiente.

#### a) Por Implementación del Servicio

Se efectuará en pago único por cada servicio de implementación de los siguientes componentes transaccionales:

- Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para Tarjetas de Débito Visa.
- Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para Tarjetas de Crédito Mastercard.

Para que este pago único por cada componente transaccional implementado se pueda efectivizar, el proveedor debe cumplir con presentar la siguiente documentación:

- Remitir todos los documentos que se indican en el numeral 10. Entregables del Anexo N° 1 - Términos de Referencia de la presente bases, en lo que corresponda al componente del servicio por cuya implementación se va a realizar el pago.
- Comprobante de pago emitido por el proveedor.
- Presentar Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- Presentar Informe Técnico emitido por la Subgerencia de Producción de la Gerencia de Tecnologías de Información confirmando el despliegue del servicio en ambiente productivo, tanto de los componentes del proveedor como de los componentes que el Banco haya tenido que implementar como parte de la integración.
- Presentar Acta de conformidad, emitida por la Subgerencia Innovación Digital, Sección Canales Virtuales y Subgerencia Canales Alternos de la Gerencia de Banca Digital. En caso el componente del servicio implementado esté relacionado a la tarjeta de crédito, el acta de conformidad será también firmada por la subgerencia Banca Personal. Una vez el proveedor haya remitido todos los entregables descritos en el numeral 10 del Anexo N° 1 - Términos de Referencia de la presente bases, el Banco tendrá 20 días hábiles (laborables) para emitir el acta de conformidad respectiva.

**b) Por Servicios Transaccionales**

**- Costo por tarjeta activa en la plataforma del proveedor:**

El Banco efectuará un pago mensual dependiente del número de PAN activos en la plataforma del proveedor en el periodo facturado, bajo las siguientes consideraciones:

- El enrolamiento de las tarjetas del Banco de la Nación en la plataforma del proveedor no las convierte en activas por defecto.
- Un PAN enrolado se convierte activo cuando se genera con éxito el primer CVV2/CVC2 dinámico para esta tarjeta, independientemente de si se llega luego a utilizar o no como parte de un requerimiento de autorización de una operación con tarjeta no presente.
- Se cobra por el PAN activo en el periodo, independientemente del número de CVV2 dinámicos generados o validados para el PAN.
- Un PAN permanece con la condición de activo en la plataforma del proveedor (independientemente si transacciona o no) hasta el mes en el que el Banco solicita su baja o eliminación mediante el API/SDK correspondiente.

El costo mensual para pagar por el Banco se define por rango de número de tarjetas (PAN) activas en la plataforma del proveedor y se aplica el modelo de precios escalonados. Es decir, el precio total a pagar es igual a la suma del número de PAN activos multiplicado por el respectivo costo unitario (CU) por la ejecución del servicio en

cada rango.

A continuación, los rangos para los que los postores deberán presentar sus propuestas de costos unitarios:

N° de PAN Activos	Costo Unitario por PAN Activo (US\$. inc. IGV)	Demanda Mensual Estimada de PAN Activos Año 01	Demanda Mensual Estimada de PAN Activos Año 02	Demanda Mensual Estimada de PAN Activos Año 03	Requerimiento Total Estimado del Servicio
De 1 hasta 200,000		200,000			2,400,000
De 200,001 hasta 1,000,000			350,000	500,000	10,200,000
De 1,000,001 hasta 3,000,000					
Más de 3,000,000					

Así, si en un mes determinado hubiese 800.000 tarjetas del BN enroladas y activas en la plataforma de CVV2 dinámico del proveedor, el Banco debería pagar:

**Total a pagar = (200.000 \* CU Rango 1) + (600.000 \* CU Rango 2)**

(CU = Costo Unitario)

Para que el pago por los servicios transaccionales pueda efectivizarse, todos los meses el proveedor debe presentar la siguiente documentación:

- o Comprobante de pago emitido por el proveedor.
- o Los documentos que se indican en el numeral 10. Entregables del Anexo N° 1 - Términos de Referencia de la presente bases, en lo que respecta a los informes por las atenciones brindadas por los componentes transaccionales.
- o Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- o Acta de conformidad, emitida por la Sección Canales Virtuales y firmada además por la Subgerencia Canales Alternos de la Gerencia de Banca Digital y la Subgerencia Banca Personal de la Gerencia de Productos e Inclusión Financiera. Una vez el proveedor haya remitido todos los entregables descritos en el numeral 10. Entregables del Anexo N° 1 - Términos de Referencia de la presente bases, el Banco tendrá 10 días hábiles(laborables) para emitir el acta de conformidad respectiva.
- o Documentación que evidencie certificación vigente del proveedor como PCI DSS.

**c) Por Servicio de Soporte Técnico**

Pago fijo mensual, para que el pago pueda efectivizarse el proveedor todos los meses debe presentarse la siguiente documentación:

- Comprobante de pago emitido por el proveedor.
- Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- Acta de conformidad, emitida por la Sección Canales Virtuales y Subgerencia Canales Alternos de la Gerencia de Banca Digital. Una vez el proveedor haya remitido todos los entregables descritos en el numeral 10 del Anexo N° 1 - Términos de Referencia de la presente bases, el Banco tendrá 10 días hábiles(laborables) para emitir el acta de conformidad respectiva.
- Si se trata del primer pago: un informe de la Subgerencia de Producción, de la Gerencia de Tecnologías de Información, confirmando el despliegue/entrega en el ambiente productivo de todas los entregables que se indican en el numeral 10. Entregables del Anexo N° 1 - Términos de Referencia de la presente bases, en lo que corresponda este componente del servicio.

### 1.3.6 CONFORMIDAD DEL SERVICIO

La conformidad por la implementación del servicio será dada de la siguiente manera:

- La conformidad por la "Implementación/Configuración del servicio de Generación y Validación de CVV2 Dinámico para Tarjetas de Débito Visa" la darán la Subgerencia Innovación Digital, la Sección Canales Virtuales y la Subgerencia Canales Alternos de la Gerencia de Banca Digital.
- La conformidad por la "Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para Tarjetas de Crédito Mastercard" la darán la Subgerencia Innovación Digital, la Sección Canales Virtuales y la Subgerencia Canales Alternos de la Gerencia de Banca Digital; así como la Subgerencia Banca Personal de la Gerencia de Productos e Inclusión Financiera.

Respeto a la conformidad del servicio luego de su puesta en operación, esta será dada por la Sección Canales Virtuales y la Subgerencia Canales Alternos de la Gerencia Banca Digital del Banco de la Nación.

Respecto al servicio de generación y validación del CVV2 Dinámico para las tarjetas de crédito Mastercard, la Subgerencia Banca Personal (Gerencia Productos e Inclusión Financiera) remitirá a la Sección Canales Virtuales un informe dando conformidad del servicio recibido en el periodo facturado por el proveedor.

Recibidos los entregables descritos en el numeral 10. Entregables del Anexo N° 1 - Términos de Referencia de la presente bases, el Banco tendrá el plazo de veinte (20) días calendarios para emitir el acta de conformidad por la implementación de los componentes del servicio y diez (10) días calendarios por la prestación del servicio transaccional mensual y el de soporte técnico.

### 1.3.7 GARANTÍA COMERCIAL

- **Alcance de la Garantía:**

Contra defectos de diseño y/o desarrollo del software, disponibilidad o fallas de funcionamiento de los componentes alojados en la nube, entre otros supuestos ajenos al uso normal o habitual de los servicios y no detectables al momento que se otorgó la conformidad, sin perjuicio a la entidad.

Para el periodo de garantía, los recursos asignados por el proveedor deben ser totalmente independientes a los recursos asignados a los servicios de soporte y mejoras continuas.

Se considerarán como garantía todos los errores detectados durante la operación en producción, los cuales hayan sido originados por fallas en la etapa de construcción respecto de las definiciones realizadas, aun cuando estos procesos hayan sido aprobados por el Banco de la Nación en etapa de pruebas integrales.

Las mejoras por garantía consideran los mismos SLA's declarados en el numeral 9. Nivel de Servicio (SLA) y Responsabilidades del Proveedor del Anexo N° 1 - Términos de Referencia de la presente bases.

- **Periodo de la Garantía:**

La garantía debe incluir la corrección de cualquier error o diferencia con lo definido hasta 12 meses después de poner en producción el último componente transaccional del servicio.

- **Inicio del Cómputo de la Garantía:**

La garantía entrará en vigor después de poner en producción el último componente transaccional del servicio.

### 1.3.8 GARANTÍA FINANCIERA

El postor adjudicado con la buena pro del concurso de méritos entregará para el perfeccionamiento del contrato la garantía (carta fianza) de fiel cumplimiento de contrato.

La garantía que se presente debe ser incondicional, solidaria, irrevocable y de realización automática en el país, al solo requerimiento del Banco de la Nación. Asimismo, debe ser emitida por empresa que se encuentre bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuente con clasificación de riesgo B o superior. Asimismo, debe estar autorizada para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

La garantía (carta fianza) deberá ser emitida a favor del Banco de la Nación, por el concepto, monto y vigencia siguiente:

- Garantía de fiel cumplimiento del contrato: por una suma equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la última conformidad de la recepción de la prestación.

### 1.3.9 SUBCONTRATACIÓN

Se permitirá que el proveedor pueda como máximo subcontratar actividades complementarias (No la principal o principales, que en este caso serían los componentes para generar y validar el CVV2 Dinámico) hasta por el 40% del monto del contrato inicial.

Es importante precisar que la subcontratación no enerva la responsabilidad del proveedor, pues este mantiene la responsabilidad por la ejecución total de su contrato frente al BN.

### 1.3.10 DEL CODIGO DE ETICA DEL BANCO DE LA NACION

El proveedor del servicio declara bajo juramento conocer que el Banco cuenta con un código de Ética, cuyo objetivo está orientado a establecer valores instituciones, principios, derechos, deberes y prohibiciones éticas. Por lo tanto, el proveedor del servicio se compromete a tomar conocimiento del contenido de este, a través del enlace: [www.bn.com.pe/nosotros/archivos/CodigoEticaBN.pdf](http://www.bn.com.pe/nosotros/archivos/CodigoEticaBN.pdf).

### 1.3.11 ANTICORRUPCION

EL CONTRATISTA promete desde la suscripción de EL CONTRATO, que EL SERVICIO se brindarán con sujeción a las normas legales aplicables a este tipo de servicios en el Perú, absteniéndose de realizar cualquier práctica o acción que no se ajuste o no esté contemplada en las referidas normas o que pueda poner en tela de juicio su calidad profesional y/o moral, ante cualquier autoridad pública o privada, medios de comunicación o cualquier tercero.

EL CONTRATISTA declara que, durante el proceso de negociación y formalización de EL CONTRATO, no se ha generado ningún evento, situación o hecho que involucre algún indicio de corrupción que pueda comprometer el servicio, que se ofrece a EL BANCO ni a las obligaciones que se adquieren a la suscripción de EL CONTRATO.

En caso EL CONTRATISTA o sus representantes o personas vinculadas sean condenadas, en el país o el extranjero, mediante sentencia consentida o ejecutoriada por delitos de concusión, peculado, corrupción de funcionarios, enriquecimiento ilícito, tráfico de influencias, delitos cometidos en remates o procedimientos de selección, o delitos equivalentes en caso estos hayan sido cometidos en otros países; asimismo, en caso EL CONTRATISTA directamente o a través de sus representantes, hubiesen admitido y/o reconocido la comisión de

cualquiera de los delitos antes descritos ante alguna autoridad nacional o extranjera competente; EL BANCO tendrá la facultad de resolver EL CONTRATO de pleno derecho y de forma automática en aplicación al artículo 1430 del Código Civil, sin perjuicio de la obligación de EL CONTRATISTA de pagar a EL BANCO la indemnización correspondiente.

### **1.3.12 RESPONSABILIDAD DEL CONTRATISTA POR VICIOS OCULTOS**

La recepción conforme de la prestación por parte del BN no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos. El plazo máximo de responsabilidad del proveedor por la calidad ofrecida y por los vicios ocultos de los servicios ofertados es de un (01) año contado a partir de la última conformidad otorgada.

### **1.3.13 PREVENCIÓN DEL LAVADO DE ACTIVOS Y FINANCIAMIENTO DEL TERRORISMO**

El proveedor declara conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015 - Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, que tiene implementado un sistema de prevención de LA/FT con componentes de cumplimiento y de gestión de riesgos de LA/FT. Por tanto, el proveedor se obliga a respetar la mencionada norma, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia.

Como parte de la gestión del Riesgo de Lavado de Activos y Financiamiento del Terrorismo, EL BANCO no se vincula con personas (ya sea con personas naturales como tal o estas en calidad de representantes de personas jurídicas privadas o de Entidades con personería jurídica de derecho público), respecto de las cuales se les haya atribuido, en sede judicial, responsabilidad por delitos precedentes de lavado de activos y financiamiento del terrorismo. Para tales efectos, EL BANCO, conforme a la Resolución SBS N° 2660-2015, aplica procedimientos de debida diligencia en el conocimiento de sus proveedores.

El proveedor para la suscripción del contrato deberá presentar una Declaración Jurada de conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015 - Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, para tal efecto deberá presentar el (Formato N° 10) registrando la información requerida.

El proveedor se compromete a actualizar la información en forma periódica, cada 02 años, y en caso no haya modificación de la información, deberá dejarse constancia de ello. Sin perjuicio de lo anterior debe comunicar a EL BANCO cualquier modificación de la información declarada.

La información a la que tiene acceso el proveedor sólo podrá ser utilizada, para los fines señalados en el presente contrato, de modo tal, que se obliga a guardar estricta y severa reserva de la información a la que tiene acceso.

#### **1.3.14 PENALIDADES**

Las Penalidades por Mora y Otras Penalidades se presentan en el numeral 18, sub numerales 18.1 y 18.2 del Anexo N° 1 - Términos de Referencia de la presente bases.

#### **1.4 EL COMITÉ DE CONCURSO DE MERITOS**

El presente Concurso de Méritos, se desarrollará de acuerdo con lo establecido en las presentes Bases, y será conducido por el Comité de Concurso de Méritos designado, quienes actúan en forma colegiada cuentan con autonomía para interpretar y adoptar las decisiones que sean pertinentes, las cuales no requieren ratificación de algún funcionario del Banco de la Nación.

Ante la ausencia de un miembro titular en el Comité, este será reemplazado por el suplente designado, siempre y cuando se respete la conformación aprobada por la Gerencia de Administración y Logística del Banco de la Nación. El suplente solo reemplazará al titular en las sesiones del Comité en las que este último se encuentre ausente.

En caso de ausencia de un titular y su suplente, la Gerencia que los designó, deberá designar con carácter de urgente a un miembro adicional, en reemplazo de ambos por las sesiones que cualquiera de ellos no pueda asistir.

Para sesionar y adoptar acuerdos válidos, el Comité del Concurso de Méritos deberán tener un quórum igual a la totalidad de sus miembros titulares o suplentes y los acuerdos serán adoptados por mayoría y consignados en Actas.


## CAPÍTULO II

### BASE NORMATIVA

- Constitución Política del Perú.
- Código Civil.
- Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 30096, Ley de Delitos Informáticos.
- Ley N° 30171, que modifica la Ley 30096 Ley de Delitos Informáticos.
- Acuerdo de Promoción Comercial Perú - Estados Unidos aprobado por el Congreso de la República mediante Resolución Legislativa N° 28766 y ratificado mediante Decreto Supremo N° 030-2006 - RE.
- Decreto Legislativo N° 1412 - Ley de Gobierno Digital, y sus modificatorias.
- Decreto Supremo N° 016-2024-JUS, Reglamento de la Ley N° 29733 - Ley de Protección de Datos Personales, y sus modificatorias.
- Decreto Supremo N° 029-2021-PCM, Reglamento del Decreto Legislativo N° 1412, Ley de Gobierno Digital, y sus modificatorias.
- Resolución S.B.S. N° 6523 -2013, Reglamento de Tarjetas de Crédito y Débito.
- Resolución SBS N° 504-2021, Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad.
- Resolución S.B.S N° 877-2020 Reglamento para la gestión de la continuidad del negocio.
- Resolución SBS N° 272-2017, Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos
- Resolución SBS N° 2660-2015, Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento de Terrorismo
- Resolución SBS N° 2116-2009, Reglamento para la Gestión del Riesgo Operacional
- Artículo 7, numeral 7.1 literal a) de la Ley N° 32069, Ley General de Contrataciones Públicas.
- Pronunciamientos emitidos por la Superintendencia de Banca, Seguros y AFP (SBS) a solicitud del Banco.
- NTP-ISO/IEC 27001-2022 2023 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.
- Manual de Organización y Funciones del Banco de la Nación - BN-MOF-7700-030-01.
- Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento al Terrorismo, aprobado por Resolución SBS N° 2660 - 2015 y modificatorias.
- Manual BN-MAN-1200-001-08, "Manual de Prevención y Gestión de los Riesgos de Lavado de Activos y del Financiamiento del Terrorismo del Banco de la Nación".
- Manual BN-MAN-2100-010-06, "Manual para el Tratamiento de Contrataciones / Subcontrataciones Significativas en el Banco de la Nación".
- Directiva BN-DIR-5500-152-01 Rev. 12 Contratación de Servicios Financieros en el Banco de la Nación.
- Las demás disposiciones legales que resulten aplicables.

### CAPÍTULO III

#### PROCESO DE CONCURSO DE MERITOS

##### 3.1 ETAPAS DEL CONCURSO DE MERITOS

El Concurso de Méritos se desarrolla conforme a las disposiciones del Cronograma establecido en las presentes Bases que se detalla:

##### Cronograma del Concurso de Méritos

N°	Etapa	Periodo
1	Convocatoria	09/07/2026
2	Formulación de Consultas	10/07/2026 al 16/07/2026
3	Absolución de Consultas	22/07/2026
4	Integración de Bases	22/07/2026
5	Presentación de Propuestas (Acto Público) A las 09:00 horas en el piso 8 de la Sede Central del BN (Av. Javier Prado Este N° 2499 - San Borja)	04/08/2026
6	Evaluación de Propuestas	12/08/2026
7	Otorgamiento de la Buena Pro	12/08/2026
8	Comunicación de Resultados	12/08/2026

Las etapas del Concurso de Méritos son las siguientes:

##### 3.1.1 Convocatoria

Se efectuará a través de invitaciones a través de correo electrónico, a las empresas que ofrecen el servicio requerido, adjuntando el archivo con las Bases aprobadas.

##### 3.1.2 Formulación de Consultas

Las consultas que formulen los participantes deben estar referidas al alcance o contenido de cualquier aspecto de las Bases, deberán ser enviadas a los correos electrónicos: [cquevedo@bn.com.pe](mailto:cquevedo@bn.com.pe), [hzevallos@bn.com.pe](mailto:hzevallos@bn.com.pe), [ediazg@bn.com.pe](mailto:ediazg@bn.com.pe), [rburgos@bn.com.pe](mailto:rburgos@bn.com.pe), respetando el plazo de presentación establecido en el Cronograma, las consultas que presenten fuera del plazo establecido o enviadas por algún otro medio, se considerarán como no presentadas y no serán tomados en cuenta por el Comité que conduce el proceso de concurso de méritos.

##### 3.1.3 Absolución de Consultas

El Comité del Concurso de Méritos absolverá las consultas presentadas por los participantes, la Absolución de Consultas será comunicada a todos los participantes a través de los correos electrónicos que hayan designado, dentro de los plazos establecidos en el Cronograma del proceso de concurso de méritos.

### 3.1.4 Integración de Bases

Las Bases Integradas constituyen las reglas definitivas del Concurso de Méritos, las que contendrán las correcciones, precisiones y/o modificaciones producidas como consecuencia de la Absolución de las Consultas.

### 3.1.5 Presentación de Propuestas

La presentación de propuestas se realizará en acto público, en el lugar, fecha y hora señaladas en el cronograma del Concurso de Méritos, con la participación de Notario Público.

El acto se inicia cuando el Comité empieza a llamar a los participantes para que entreguen sus propuestas. Si al momento de ser llamado el participante no se encuentra presente, se le tendrá por desistido.

Las propuestas se presentarán en dos (2) sobres cerrados, que contendrán la propuesta técnica y económica respectivamente, la que debe estar foliada correlativamente empezando por el número uno y deben llevar el sello y la rúbrica del postor o de su representante legal o mandatario designado para dicho fin.

Después de recibidas las propuestas, el Comité procederá a abrir los sobres que contienen la propuesta técnica y económica de cada postor, a fin de verificar que se encuentren los documentos presentados por cada postor sean los solicitados en las Bases.

Todos los documentos que contengan información referida a los requisitos para la admisión de propuestas, factores de evaluación y requisitos de calificación se presentarán en idioma castellano o, en su defecto, acompañados de la respectiva traducción por traductor público juramentado o traductor colegiado certificado, salvo el caso de la información técnica complementaria contenida en folletos, instructivos, catálogos o similares, que podrá ser presentada en el idioma original. El postor será responsable de la exactitud y veracidad de dichos documentos.

En el caso que de la revisión de la propuesta se adviertan defectos de forma, tales como errores u omisiones subsanables en los documentos presentados que no modifiquen el alcance de la propuesta técnica y económica, se puede otorgar plazo para subsanar la propuesta técnica.

Después de abierto cada sobre que contiene la propuesta técnica y económica verificado que contengan los requeridos como documentación de presentación obligatoria, el Notario procederá a sellar y firmar cada hoja de los documentos de la propuesta técnica y económica.

Al terminar el acto público, se levantará un acta, la cual será suscrita por el Notario, todos los miembros del Comité del concurso de méritos y facultativamente los representantes de las empresas postoras.

✓ **Sobre: Propuesta Técnica**

Se presentará en un original con el siguiente rotulado:

<p>Señores Banco de la Nación Av. Javier Prado Este N° 2499 - San Borja Att.: Comité del Concurso de Méritos</p> <p><b>CONCURSO DE MERITOS N° 0004-2026-BN</b></p> <p>"Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente"</p> <p>SOBRE: PROPUESTA TÉCNICA [NOMBRE / RAZÓN SOCIAL DEL POSTOR]</p>
--

El Sobre de la propuesta técnica contendrá, además de un índice de documentos, la siguiente documentación:

**Documentación de Presentación Obligatoria**

- a) Declaración Jurada de Datos del Postor. (**Formato N° 1**).
- b) Documento que acredite la representación de quien suscribe la propuesta.  
  
Copia del Certificado de Vigencia de Poder del representante legal, apoderado o mandatario designado para tal efecto.  
  
En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.
- c) Declaración Jurada de cumplir con los requisitos para ser postor en el presente proceso de concurso de méritos. (**Formato N° 2**).
- d) Declaración Jurada de Cumplimiento de los Términos de Referencia contenidos en el Anexo N° 1 de la presente Bases. (**Formato N° 3**).
- e) Declaración Jurada de Plazo de Prestación del Servicio. (**Formato N° 4**).
- f) Promesa de Consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. (**Formato N° 5**).
- g) Detalle de la Experiencia del Postor en la Especialidad (**Formato N° 6**).

- h) De ser el caso, Declaración Jurada de Reorganización Societaria (Formato N° 7).

El Comité de Selección responsable de la conducción de Concurso de Méritos N° 0004-2026-BN, verificará la presentación de los documentos requeridos con carácter de presentación obligatoria. De no cumplir con lo requerido, la propuesta se considera no admitida.

**Documentos para Acreditar los Requisitos de Calificación**

Incorporar en la propuesta los documentos que acreditarán el cumplimiento de los "Requisitos de Calificación" que se detallan en el numeral 24 del Anexo N° 1 - Términos de Referencia del Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente, de la presente bases, en caso de no cumplir con alguno de los requisitos de calificación la propuesta quedará descalificada.

✓ **Sobre: Propuesta Económica**

Se presentará en un original con el siguiente rotulado:

<p><b>Señores</b> Banco de la Nación Av. Javier Prado Este N° 2499 - San Borja Att.: Comité del Concurso de Méritos</p> <p><b>CONCURSO DE MERITOS N° 0004-2026-BN</b></p> <p>"Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente"</p> <p>SOBRE: PROPUESTA ECONOMICA [NOMBRE / RAZÓN SOCIAL DEL POSTOR]</p>
---

La Propuesta Económica, deberá incluir obligatoriamente su propuesta en Dólares Americanos (US\$.), y el detalle de precios conforme a los establecido en las Bases (Formato N° 8) incluidos todos los tributos, los costos laborales conforme a la legislación vigente; así como, cualquier otro concepto que pueda tener incidencia sobre el costo del servicio a contratar.

El monto total de la propuesta económica y los subtotales que lo componen deberán ser expresados con dos decimales. Los precios unitarios podrán ser expresados con más de dos decimales.

En el documento que contiene el precio ofertado u propuesta económica puede subsanarse la rúbrica y la foliación.

En caso de divergencia entre el precio cotizado en números y letras, prevalece este último. Cuando se advierta errores aritméticos, corresponde su corrección al Comité, debiendo constar dicha rectificación en el acta respectiva; en este último caso, dicha corrección no implica la variación de los precios unitarios ofertados.

### 3.1.6 Evaluación de Propuestas

La evaluación de propuestas se realizará en tres (3) etapas: Admisión de Propuestas, Evaluación Económica y Evaluación Técnica.

La información contenida en la propuesta debe ser objetiva, clara, precisa y congruente entre sí y debe encontrarse conforme con lo requerido en las bases, a fin de que el Comité del Concurso de Méritos encargado de la Contratación, puedan apreciar el real alcance de la misma y su idoneidad para satisfacer el requerimiento de la Entidad, lo contrario, por los riesgos que implica, determinará que la propuesta sea desestimada.

No es función del Comité del Concurso de Méritos, interpretar el alcance de una propuesta, esclarecer ambigüedades o precisar contradicciones o imprecisiones, sino evaluar las propuestas en virtud de las bases, realizando un análisis integral que permita generar convicción de lo realmente ofertado, sin posibilidad de inferir o interpretar hecho alguno.

Excepcionalmente el Comité del Concurso de Méritos podrá solicitar aclaración y/o precisión sobre algún documento que forme parte de las Propuestas Técnicas recepcionadas, otorgando un plazo máximo de hasta tres (3) días hábiles para la atención, contados a partir del día siguiente de la solicitud.

#### 3.1.6.1 Admisión de Propuestas

Se procederá a la verificación de los documentos de Presentación Obligatoria, según lo establecido en la presente bases del Concurso de Méritos N° 0004-2026-BN, Capítulo III Proceso de Concurso de Méritos, numeral 3.1 Etapas del Concurso de Méritos, subnumeral 3.1.5 Presentación de Propuestas, cuyas propuestas que cumplan con los documentos de presentación obligatoria serán declarados Admitidas y las propuestas que no cumplan con los documentos de presentación obligatoria serán declarados No Admitidas, solo pasan a la etapa de Evaluación Económica las propuestas declaradas Admitidas.

#### 3.1.6.2 Evaluación Económica

Solo se evaluarán las propuestas declaradas Admitidas.

Para determinar la propuesta con el mejor puntaje y el orden de prelación de las propuestas, se aplicará el siguiente procedimiento:

1. **Puntaje Total:** 100 puntos
2. **Evaluación del Costo del Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente:** se asignará 100 puntos.

Para determinar la propuesta con el mejor puntaje, consistirá en asignar el puntaje máximo establecido a la propuesta económica de menor monto. Al resto de propuestas se les asignará un puntaje inversamente proporcional, según la siguiente fórmula:

$$P_i = \frac{O_m \times PMPE}{O_i}$$

Donde:

i = Propuesta  
P<sub>i</sub> = Puntaje de la propuesta económica i  
O<sub>i</sub> = Propuesta Económica i  
O<sub>m</sub> = Propuesta Económica de monto o precio más bajo  
PMPE = Puntaje Máximo de la Propuesta Económica

### 3.1.6.3 Evaluación Técnica

Se verificarán las propuestas técnicas de los postores que en la evaluación económica han obtenido el primer y segundo puesto en el orden de prelación, en caso alguna no cumpla con los requisitos de calificación se continuará con la evaluación técnica siguiendo el orden de prelación.

La evaluación técnica consistirá en la verificación de los requisitos de calificación. Se verificará que la propuesta técnica cumpla con los requerimientos técnicos mínimos contenidos en las presentes Bases. Las propuestas que no cumplan dichos requerimientos quedarán como descalificadas.

En aquellos casos en los que se hubiese otorgado plazo para la subsanación de la propuesta, el Comité de Selección deberá determinar si se cumplió o no con la subsanación solicitada. Si luego de vencido el plazo otorgado, no se cumple con la subsanación, el Comité tendrá la propuesta por no admitida.

Una vez cumplida la subsanación de la propuesta o vencido el plazo otorgado para dicho efecto, se continuará con la evaluación de las propuestas técnicas admitidas, verificando que cumplan con los requisitos de calificación. La propuesta que no cumpla con los requisitos de calificación es descalificada.

### 3.1.7 Otorgamiento de la Buena Pro

Una vez evaluadas las propuestas el Comité de Selección procederá a otorgar la Buena Pro a la propuesta ganadora, de acuerdo con el cuadro comparativo en el que se consignará el orden de prelación en que han quedado calificados.

En el supuesto que dos (2) o más propuestas empaten, la determinación

del orden de prelación de las propuestas empatadas se realiza a través de sorteo efectuado por un Notario Público.

En los casos de haberse presentado una sola propuesta al Concurso de Méritos, el Comité, a su sola decisión, podrá otorgar la Buena Pro al único postor, siempre que cumpla con los requisitos de las Bases.

### 3.1.8 Comunicación de Resultados

El presidente del Comité comunicará los resultados del Concurso de Méritos, mediante correo electrónico dirigido a todos los postores.

### 3.2 Procedimiento para la Atención de Solicitudes o Reclamos Presentados por Postores

En el supuesto que algún postor presente una solicitud, o presente un reclamo, respecto a cualquier acto que haya realizado el Comité del Concurso de Méritos en el ejercicio de sus funciones, se deberá seguir el procedimiento que se detalla a continuación (no se incluyen en este procedimiento, las consultas y/o observaciones que se efectúen dentro del Concurso de Méritos, cuando correspondan estos a la etapa del Concurso):

- a) El Postor deberá presentar su reclamo o solicitud, en el plazo máximo de tres (3) días hábiles, contados a partir del día siguiente de la comunicación de los resultados del proceso efectuado por el Banco, en la Sección Trámite Documentario sito en la Calle Arqueología N° 120 - San Borja en el horario de 08:30 a 16:30 Horas, quien deberá remitirlo a la Gerencia de Administración y Logística. Dicha Gerencia, de manera inmediata, enviará el documento a los miembros del Comité de Concurso de Méritos para su revisión, quienes emitirán de manera colegiada, el informe técnico respectivo, dando respuesta a cada una de las solicitudes, reclamos y/o pedidos formulados por el postor. El citado documento también es remitido a la Subgerencia Compras para el seguimiento respectivo. Dicho informe sirve como sustento para brindar respuesta a la solicitud o reclamo presentado por el postor.
- b) El informe deberá ser emitido dentro de los tres (03) días hábiles siguientes desde la fecha de recepción del documento, por parte del comité, bajo responsabilidad. En caso se requiere de mayor tiempo para emitir el informe, por complejidad del asunto a contestar o por necesitar información y/o documentación de otras áreas del Banco, se puede ampliar el plazo por tres (03) días hábiles adicionales por una sola vez.
- c) Dicho informe será remitido a la Subgerencia Compras de la Gerencia de Administración y Logística juntamente con el Expediente de Contratación para su revisión, análisis, opinión y elaboración del proyecto de carta de respuesta, previa consulta con la Gerencia Legal, de corresponder (en caso exista un aspecto jurídico para su evaluación).
- d) La Gerencia de Administración y Logística, en un plazo máximo de tres (03) días hábiles, formalizará la carta de respuesta y solamente en caso existan

aspectos de carácter jurídico en la respuesta a brindar, procederá la visación de la Gerencia Legal.

### 3.3 Del Perfeccionamiento del Contrato

Dentro del plazo de ocho (08) días hábiles siguientes al otorgamiento de la Buena Pro, el postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

- a) Garantía Financiera (carta fianza) de fiel cumplimiento de contrato, acorde a lo establecido en el numeral 1.3.8 de la presente bases.
- b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- d) Póliza Tech E&O que deberá cumplir con las características y condiciones establecidas en el numeral 21. Seguros del Anexo N° 1 - Términos de Referencia, de la presente bases.
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato.
- f) Domicilio para efectos de la notificación durante la ejecución del contrato.
- g) Autorización de notificaciones por el Banco de la Nación, durante la ejecución contractual mediante medios electrónicos de comunicación (**Formato N° 9**).
- h) El ganador de la Buena Pro a la suscripción del contrato deberá presentar obligatoriamente una Declaración Jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo y su Reglamento; así como, el cumplimiento de la Resolución Ministerial N° 022-2024/MINSA, Directiva Administrativa N° 349-MINSA/DGIESP-2024, que establece las disposiciones para la Vigilancia, Prevención y Control de la Salud de los Trabajadores con Riesgo de Exposición a SARS-CoV-2, o aquella que la reemplace.
- i) El ganador de la Buena Pro a la suscripción del contrato deberá presentar obligatoriamente una Declaración Jurada que declare conocer que el Banco de la Nación es una Entidad Financiera sujeta al cumplimiento del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS N° 2660-2015, y que por tanto se obliga a proporcionar toda aquella información necesaria a fin de dar cumplimiento a lo dispuesto en los artículos 36° y 37° del referido Reglamento, para tal efecto, deberá presentar el (**Formato N° 10**) registrando la información requerida.
- j) Declaración Jurada de no encontrarse inscrito en el Registro de Deudores de Reparaciones Civiles (REDERECI). (**Formato N° 11**).
- k) Declaración Jurada de no estar Inhabilitado para contratar con el Estado Peruano. (**Formato N° 12**).

En un plazo que no podrá exceder de los dos (02) días hábiles siguientes de presentados los documentos, de existir observaciones el BN solicitará la subsanación de los requisitos, en un plazo adicional de cuatro (04) días contados desde el día siguiente de la notificación al postor. De no existir observaciones, el BN solicitará al postor que en un plazo no mayor de (02) días hábiles comunique sobre sus observaciones al Proyecto de Contrato contenido en las Bases, luego

de lo cual, las partes tendrán un plazo de cuatro (04) días hábiles para realizar los ajustes que resulten necesarios dentro de los alcances del servicio contratado y suscribir el contrato. Dicho plazo podrá ser ampliado por acuerdo de las partes.

Cuando no se perfeccione el contrato, por causa imputable al postor, éste pierde automáticamente la buena pro; en tal supuesto, la Subgerencia de Compras como dependencia encargada de las contrataciones (DEC) del BN, en un plazo máximo de tres (03) días hábiles, requiere al postor que ocupó el segundo lugar que presente los documentos para perfeccionar el contrato en los mismos plazos previstos en el párrafo anterior. Si el postor no perfecciona el contrato, el órgano encargado de las contrataciones del BN declara desierto el proceso de concurso de méritos.

Se deja constancia que el proyecto de Contrato contenido en estas bases es referencial, por lo que, previo al perfeccionamiento del Contrato, el Banco tiene la facultad de poder establecer otras estipulaciones en el Contrato, que será la versión final a ser suscrita por el Proveedor y el Banco.

#### 3.4 DISPOSICIONES FINALES

- a) Los servicios financieros que contrata el Banco, no se enmarcan dentro de los procedimientos administrativos regulados por el TUO de la Ley del Procedimiento Administrativo General, aprobado por Decreto Supremo N° 004-2019-JUS, por lo que no constituye el Concurso de Méritos llevado a cabo bajo los alcances de la Directiva BN-DIR-5500-152-01 Rev.12, un procedimiento o acto administrativo que pueda ser sujeto de recurso impugnatorio alguno.
- b) El Comité del Concurso de Méritos culminará sus funciones con la entrega del informe correspondiente a la Gerencia de Administración y Logística, lo que se producirá luego de la notificación en acto público del otorgamiento de la buena pro del Concurso de Méritos.

# Anexos

## Anexo N° 1

### SERVICIO DE IMPLEMENTACION DE MECANISMOS DE SEGURIDAD EN TRANSACCIONES CON TARJETA BN (DE CRÉDITO Y DÉBITO) NO PRESENTE

#### TÉRMINOS DE REFERENCIA

#### 1. DENOMINACION DE LA CONTRATACIÓN

Servicio de implementación de mecanismos de seguridad en transacciones con tarjeta BN (de crédito y débito) NO presente.

#### 2. FINALIDAD PÚBLICA

El presente servicio tiene como finalidad brindar a nuestros tarjetahabientes seguridad durante la realización de sus operaciones en las redes de pago Visa y Mastercard con sus tarjetas de débito y crédito del Banco de la Nación respectivamente, específicamente sobre las transacciones con tarjeta NO presente.

#### 3. VINCULACIÓN CON EL OBJETIVO META DEL POI

El servicio materia de la contratación se encuentra vinculado a los Objetivos Estratégicos Institucionales: Masificar el Acceso y Uso de los Canales Alternos y Incrementar las Operaciones y los clientes Digitales del Plan Estratégico Institucional 2022-2026.

#### 4. ANTECEDENTES

El 26 de junio del 2024 la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) publicó la Resolución N° 2286-2024, mediante la cual precisa la responsabilidad de las empresas en los procedimientos de validación de identidad de los usuarios y la obtención su consentimiento al momento de realizar operaciones.

#### 5. OBJETIVOS DE LA CONTRATACIÓN

##### Objetivo General

Reforzar la seguridad durante la realización de operaciones con tarjeta NO presente en las redes de pago Visa y Mastercard, cumpliendo así con las disposiciones dadas por la SBS (Superintendencia de Banca, Seguros y AFP) respecto a estos temas.

##### Objetivos Específicos

- a) Implementar el CVV2 Dinámico como segundo factor de autenticación durante la realización de operaciones con tarjeta NO presente, dando cumplimiento a lo establecido por la SBS en su Resolución N° 2286-2024.
- b) Reducir el riesgo de pérdidas para el Banco a causa de reclamos de clientes por el no reconocimiento de operaciones con tarjeta NO presente en comercios que no participan de 3DS.

#### 6. MODALIDAD DE PAGO

La contratación se regula por el Sistema Esquema Mixto de Suma Alzada y Precios Unitarios: A suma alzada el servicio de Implementación/configuración del del servicio generación y validación de CVV2 dinámico y el soporte técnico descrito en el numeral 7.2 de los presentes términos de referencia, y a precios unitarios los servicios transaccionales.

## 7. ALCANCE Y DESCRIPCION DEL SERVICIO

El Servicio objeto de la contratación debe comprender la implementación / Configuración de los servicios que se detallan:

Servicio	Componentes
Generación y Validación de CVV2 Dinámico	Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de débito Visa
	Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para tarjetas de crédito Mastercard
	Servicio de generación y validación de CVV2/CVC2 Dinámico
Soporte Técnico	Soporte Técnico descrito en el numeral 7.2 de los presentes términos de referencia

El proveedor al implementar los componentes transaccionales de su servicio deberá tener en cuenta que el Banco de la Nación autoriza y procesa por sí mismo las operaciones de su tarjeta de débito Visa y se vale de un tercero (la empresa Izipay) para autorizar y procesar las operaciones de su tarjeta de crédito Mastercard.

El proveedor debe cumplir con los estándares de seguridad de las marcas para la generación y validación del CVV2 Dinámico.

### 7.1. GENERACION Y VALIDACION DE CVV2 DINAMICO

El servicio de CVV2 Dinámico a ser proporcionado por el proveedor debe ser implementado/configurado para que se ejecute bajo las siguientes condiciones:

- El CVV2 dinámico que genere la plataforma del proveedor tendrá un periodo de vigencia establecido, que se renovará cada cierto periodo de tiempo, producto de 2 situaciones:
  - o La caducidad del CVV2 dinámico, que fue solicitado pero que no fue usado por el tarjetahabiente como parte de una operación con tarjeta NO presente. El periodo de caducidad se definirá en un parámetro de la plataforma del proveedor, el que podrá ser ajustado a solicitud del Banco cuando lo considere conveniente.
  - o Una solicitud de autorización de operación sin tarjeta presente denegada o aprobada.
- Durante el periodo de vigencia de un CVV2, este solo debe poder ser usado en una transacción de la tarjeta (de crédito o débito) para la cual fue generado, independientemente de si la transacción fue autorizada o denegada por el Banco; sin embargo, el proveedor debe garantizar la flexibilidad de su solución, de tal forma que, para casos de uso excepcionales, pueda configurarla para que sea posible autenticar más de una transacción con el mismo CVV2 dinámico.
- El proveedor proporcionará al Banco de la Nación una API que permita enrolar en línea una tarjeta BN (de débito Visa o de crédito Mastercard) en la plataforma de generación del CVV2 dinámico.
- El proveedor proporcionará al Banco de la Nación una API que permita dar de baja en línea a una tarjeta BN (de débito Visa o de crédito Mastercard) en la plataforma de generación del CVV2 dinámico.
- El proveedor deberá proporcionar funcionalidad que sea ejecutada a demanda y permita el alta (enrolamiento) o baja masiva de tarjetas en la plataforma de

generación de CVV2 dinámico.

- El proveedor proporcionará un SDK, compatible con los sistemas operativos Android e iOS, de tal forma que el Banco lo integre en su Banca Móvil para:
  - o Solicitar a demanda y en línea a la plataforma del proveedor la generación de un CVV2 dinámico para la tarjeta del cliente del Banco de la Nación. Para que esto sea posible, el smartphone del cliente deberá tener acceso a internet, de lo contrario no podrá acceder a la banca móvil del Banco (App BN) y por ende tampoco podrá solicitar la visualización del CVV2 dinámico de su tarjeta.
  - o Recibir el CVV2 dinámico generado por la plataforma del proveedor y mostrarlo al tarjetahabiente en la pantalla de la aplicación móvil.
- El proveedor proporcionará una API o una interfaz ISO8583 (en función a lo que el Banco defina), o ambos, a través de la cual el componente (propio o tercerizado) del Banco, que resuelve los requerimientos de autorización de transacciones provenientes de las redes de pago (Visa y Mastercard), solicite a la plataforma del proveedor validar el CVV2 dinámico que el tarjetahabiente ingresó junto a los otros datos de la tarjeta durante su compra en un comercio electrónico. Esta API/ISO8583 entregará como respuesta la confirmación de si el CVV2 dinámico que llegó en la trama de requerimiento de autorización al Banco es válida o no.  
De optarse por usar la interfaz ISO8583, para validar el CVV2 dinámico de la tarjeta de débito la integración deberá efectuarse usando el formato ISO de Visa, y para validar el CVV2 dinámico de la tarjeta de crédito la integración deberá efectuarse usando el formato ISO de Mastercard.
- El proveedor debe proporcionar acceso a un portal web, a ser usado por el personal de las áreas del back office del Banco, que disponga de:
  - o Control de acceso a través de validación de código de usuario, contraseña (podrá ser cambiada por el trabajador a demanda) y un segundo factor de autenticación.
  - o La solución deberá cumplir con las políticas de seguridad de información del Banco referente a los estándares para la administración de cuentas de usuario y contraseñas establecidas en la Normativa Interna (ver Anexo 1), cuyos parámetros deberán ser configurables.
  - o Maneje perfiles de usuario de tal forma que se gestionen y asignen los accesos correspondientes dependiendo el rol de cada trabajador del Banco.
  - o Consultar logs de la fecha de enrolamiento y de baja de una tarjeta en la plataforma de generación de CVV2 dinámico y su estado actual.
  - o Enrolar en línea una tarjeta del BN (de débito Visa o de crédito Mastercard) en la plataforma de generación de CVV2 dinámico del proveedor.
  - o Dar de baja en línea una tarjeta del BN (de débito Visa o de crédito Mastercard) en la plataforma de generación de CVV2 dinámico del proveedor.
- El proveedor debe asegurar la grabación de los registros o logs para auditoría de las actividades relacionadas al consumo (procesamiento, almacenamiento, transmisión) de los componentes de software de su solución (APIs, SDK), registros que como mínimo deberán contener los siguientes datos:
  - o Fecha (DD/MM/YYYY) y hora de consumo (HH:MM:SS:MMM) del componente de software del proveedor.
  - o Componente de software consumido.
  - o PAN de la tarjeta (enmascarada).
  - o IP de la ubicación desde donde se hizo el requerimiento y el procesamiento.
  - o Id de la Transacción Único
  - o Resultado: operación exitosa / operación fallida / autenticación fallida

- ID del Usuario
- Todo dato que reciba el componente y devuelva
- Detalle error

Respecto al portal web para el back office, debe registrarse la actividad de los usuarios finales y de las cuentas principales, de integración y privilegiadas, como parte del uso de la solución, como por ejemplo información de los login (hayan sido estos exitosos o fallidos) o de las acciones realizadas a través de este portal. En cada registro debe al menos registrarse la información indicada en el acápite previo.

En todos los casos, los logs o registros guardados por el proveedor deben contar con un código de identificación o similar y ser inmutables (no modificables). El almacenamiento de estos logs o registros en las instalaciones del proveedor deberá estar disponible durante toda la vigencia del servicio de manera inalterable.

El proveedor deberá poner a disposición del Banco de la Nación, de forma diaria, los logs o registros generados en la fecha, mediante alguna de las siguientes alternativas:

- a) Depositar los archivos en una carpeta SFTP proporcionada por el Banco, en formatos estructurados como TXT o XLS; o
- b) Proveer API(s) seguras, disponibles y documentadas que permitan la consulta y/o extracción de los logs o registros.

En ambos casos, el proveedor deberá garantizar la integridad y disponibilidad de la información entregada.

- El proveedor deberá garantizar el soporte y acompañamiento técnico al Banco de la Nación durante las fases de implementación y pruebas del servicio, incluso durante la primera semana de operación del servicio en el ambiente productivo.
- El proveedor debe garantizar que los SDK que entregue al Banco sean compatibles con todas las versiones vigentes de los sistemas operativos Android e iOS; así como asegurar (sin costo para el Banco) las respectivas actualizaciones de estos SDK para garantizar su compatibilidad con las versiones nuevas (de estos S.O.) que liberen Google y Apple.
- El proveedor deberá brindar todas las facilidades y el acompañamiento técnico necesario al equipo del Banco de la Nación, a fin de que pueda implementarse el mecanismo que permita a sus componentes de software sensar automática y periódicamente las APIs del proveedor.

## 7.2. SOPORTE TECNICO

El proveedor debe proporcionar el siguiente soporte antes y después de la puesta en producción de los componentes del servicio contratado:

- El proveedor debe proporcionar al Banco los siguientes ambientes de trabajo, los que deberán estar disponible 24X7, los 365 días del año, durante el tiempo de vigencia del contrato:
  - Un ambiente Pre-Productivo: conectado con los ambientes pre-productivos del Banco de la Nación, donde única y exclusivamente se puedan efectuar las pruebas de los desarrollos e integraciones entre ambas partes (proveedor y Banco de la Nación) antes de su despliegue en producción.
  - Un ambiente Productivo: entorno donde se encuentran desplegados y operan los componentes de la plataforma tecnológica que soporta el servicio prestado por el proveedor, el mismo que está conectado al ambiente de producción del Banco de la Nación.
- **Una Mesa de Ayuda:**  
Disponible 24X7 los 365 días del año durante el tiempo de vigencia del contrato, donde el equipo del Banco de la Nación pueda reportar caídas o problemas con el

servicio (en cualquiera de ambientes de trabajo proporcionados por el proveedor) a través de llamadas telefónicas o emails, de tal forma que el proveedor pueda tomar las acciones correspondientes. Este servicio debe ser prestado por el proveedor en idioma español (oral y escrito).

- **Un Sistema de Tickets:**

Portal web que permite enviar, gestionar y realizar el seguimiento de incidentes (comunicados por el Banco o identificados internamente por el proveedor), requerimientos de información y solicitudes de cambio; para gestionar el flujo de trabajo interno y realizar el seguimiento de la respuesta, la resolución y la restauración del servicio, así como para entregar los informes correspondientes.

Los tickets podrán ser registrados por el proveedor (ante el reporte de caídas del servicio efectuadas a su Mesa de Ayuda por parte del Banco, por ejemplo) o por el personal autorizado del Banco. Este sistema permitirá a ambas partes registrar contenido y compartir archivos dentro del ticket como parte del seguimiento de su atención. El contenido de las comunicaciones que se efectúen a través de esta plataforma debe ser en idioma español.

- **Actualizaciones obligatorias:**

El proveedor implementará todos los cambios o actualizaciones necesarios en el hardware y software en la plataforma informática que soporta la operatividad de los componentes del servicio prestado al Banco de la Nación (debido entre otras cosas a obsolescencia, falta de soporte de los fabricantes, por conveniencia para garantizar el óptimo desempeño de la solución de acuerdo a los SLA, entre otros) con la finalidad de garantizar la disponibilidad y continuidad de este servicio, debiendo asumir íntegramente los costos de estos cambios y/o actualizaciones.

El proveedor deberá monitorear los mandatos de redes de pago (Visa, Mastercard) relacionados directamente con el servicio de CVV dinámico, y notificarlos al Banco mediante carta simple u otro medio electrónico acordado entre las partes. La comunicación al Banco deberá realizarse dentro de los 30 días calendarios posteriores a la publicación del mandato, debiendo el proveedor asumir los costos de estas implementaciones, las que deberá ser efectuadas dentro de los plazos establecidos por las redes de pago. Respecto a los cambios regulatorios establecidos por la SBS (Superintendencia de Banca, Seguros y AFP), Banco Central de Reserva del Perú o alguna otra entidad gubernamental, el Banco informará al proveedor sobre el alcance e implicancias de estas adecuaciones, debiendo este último presentar una propuesta de plan de implementación, con los respectivos costos asociados si fuera el caso, los cuales el Banco evaluará para su aceptación e implementación.

- **Soporte AD HOC post pase a Producción:**

El proveedor debe asegurar el soporte dedicado al Banco de la Nación de un equipo técnico que esté disponible 24X7 durante 07 días calendarios, contados a partir de la puesta en producción de cada uno los componentes transaccionales del servicio. El objetivo es tener el enfoque y asistencia prioritaria para la gestión de incidencias durante estos periódicos críticos.

## 8. CARACTERÍSTICAS TÉCNICAS DE LA SOLUCIÓN TECNOLÓGICA REQUERIDA

- Los componentes transaccionales que forman parte del servicio prestado por el proveedor deben soportar mínimo 10 TPS, pudiendo escalar de acuerdo con la demanda.
- Debe garantizar una alta disponibilidad, de tal forma que no se requiera reconfigurar el servicio en caso de caída para continuar con la operación.
- Los componentes de la solución deben operar en al menos 3 zonas de disponibilidad geográficamente distantes.
- Debe realizarse pruebas funcionales de los componentes transaccionales del servicio, así como las pruebas de rendimiento, estrés y de alta disponibilidad de estos componentes.

- Capacidad de escalar su operación en la medida que aumente la demanda de los componentes transaccionales del servicio. El servicio debe estar desplegado en una arquitectura basada en kubernetes y/u otra tecnología que permita la escalabilidad descrita.
- Capacidad para ser invocado desde canales/aplicaciones on premise del Banco de la Nación, como la Banca Móvil, Banca por Internet (Multired Virtual) y/u otro canal de atención, servicio o producto, a través de una VPN.
- La plataforma del proveedor debe disponer de un WAF (Web application firewall) que mitigue el riesgo y proteja de múltiples ataques.
- EL PROVEEDOR deberá considerar para el establecimiento de las comunicaciones entre terceros, enlaces VPN Site to Site (S2S) o VPC (private link).
- El proveedor debe usar HSM (Módulo de Seguridad de Hardware) con certificación FIPS 140-2, nivel 3 o superior, y para uso exclusivo del servicio prestado al Banco
- Toda la información en tránsito (punto a punto) (considerar protocolo TLS 1.3 como mínimo) y en reposo (base de datos) deberá estar cifrada y firmada digitalmente (integridad de datos).
- Para la información de datos en reposo el proveedor deberá de indicar el método de cifrado robusto utilizado.
- Todo servicio WEB (llámese API/RESTFull, SOAP, entre otros) deberá ser accedido a través de una plataforma de seguridad WAF.
- EL PROVEEDOR deberá considerar tecnología para mitigar ataques de denegación de servicio distribuida (DDoS) y ataques de Bots Automatizados (AntiBot) (Los actuales y los futuros).
- La solución deberá garantizar la seguridad de los datos en tránsito, utilizando el protocolo HTTPS al llamar a los recursos web, API de Rest o al acceder a objetos en el almacenamiento.
- Para el despliegue de la solución se deberá considerar el principio de mínimo privilegio, es decir que solo se deberá otorgar los privilegios necesarios a las cuentas o servicios que forman parte de la solución.
- La solución deberá ser capaz de mitigar los ataques de presentación (PAD/PADER).
- La prestación del servicio y la solución deberán asegurar la adopción y manejo de los requisitos de seguridad de la información y ciberseguridad del Sistema de Gestión de Seguridad de la Información del Banco, aplicables al servicio a contratar, acorde con las exigencias del negocio y al estricto cumplimiento de los requerimientos de seguridad de la información establecida en la normativa externa que se menciona en este acápite. Los componentes de la solución deberán contar con los controles de seguridad de la información requeridos de tal modo que permitan su cumplimiento en lo que aplique a dichos componentes de acuerdo a:
  - o Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad (Resolución SBS N°504-2021).
  - o Certificación ISO/IEC 27001.
  - o Ley de Protección de Datos Personales (Ley N° 29733).
  - o Reglamento de Tarjetas (Resolución SBS N° 6523-2013).
  - o Estándar PCI DSS V4.0.
- Las aplicaciones Web y componentes SDK deberán considerar en su construcción los estándares ASVS y MASVS de OWASP
- Se requiere que el proveedor entregue pruebas de seguridad en todos los Componentes entregados al Banco (Ejemplo: SDK, API) que deberán ser ejecutadas por una entidad tercera independiente. El proveedor coordinará con el Banco de la Nación el tipo de pruebas.
- Las interfaces de programación de aplicaciones (API) de EL PROVEEDOR, deberán implementar mínimamente las siguientes medidas: autenticación mutua de los sistemas

y la de los usuarios, cifrado de datos en almacenamiento o transmisión, realizar y evidenciar análisis de vulnerabilidades y pruebas de penetración, se cuente con mecanismos de tolerancia ante fallos, control de accesos en el entorno de datos, sistemas e infraestructura, desarrollo seguro de API, revisión de prácticas de codificación segura y Monitoreo de eventos de seguridad de la información y gestión de estos cuando se constituyan en incidentes.

## 9. NIVEL DE SERVICIO (SLA) Y RESPONSABILIDADES DEL PROVEEDOR

El proveedor debe asegurar la disponibilidad de los componentes del servicio en los siguientes términos:

### 9.1. SLA de Componentes Transaccionales

El proveedor debe garantizar que durante la fase de ejecución/operación los componentes transaccionales del servicio tengan una Alta Disponibilidad igual o mayor al 99.99%, las 24 horas del día, los 365 días del año, durante el periodo de vigencia del contrato:

El tiempo objetivo de recuperación (RTO) del servicio prestado debe ser de 1 hora.

El SLA de los componentes transaccionales es aplicable solo a su desempeño en el ambiente productivo.

#### Tiempos de no Disponibilidad Excluidos

El proveedor no será responsable en ningún caso del incumplimiento del SLA en periodos de tiempo durante los cuales los componentes del servicio no estén disponibles o se vean afectados, debido a las siguientes causas, eventos o circunstancias que se describen a continuación, quedando dichos periodos excluidos del SLA de Disponibilidad:

- El mal comportamiento de las aplicaciones, errores de programación o scripts personalizados del propio Banco;
- Configuraciones del Banco fuera de la infraestructura del proveedor que afecten a los componentes del Servicios;
- Fallo o uso inadecuado de los Servicios por parte del Banco, sus empleados, agentes o terceros;
- Servicios prestados por un tercero fuera del control del proveedor.
- Mantenimiento programado o mantenimiento correctivo según se detalla en el numeral 9.3.

### 9.2. SLA de Componentes de Soporte

Servicio	Disponibilidad Requerida
Portal web de acceso a documentación técnica del proveedor	24x7, todos los días del año durante periodo de vigencia del contrato
Ambiente Pre-Productivo	24x7, todos los días del año durante periodo de vigencia del contrato
Mesa de Ayuda	24x7, todos los días del año durante periodo de vigencia del contrato.

Sistema de Tickets	24x7, todos los días del año durante periodo de vigencia del contrato El SLA respecto a la gestión de incidencias se detalla en el numeral 9.4 ("Gestión de Incidencias")
Actualizaciones obligatorias	Durante el periodo de vigencia del contrato. El proveedor debe asegurarse de entregar los cambios/actualizaciones previamente probados y dentro de los plazos correspondientes, de tal forma que no se comprometa la disponibilidad, ni la calidad del servicio prestado al Banco.
Soporte AD HOC post pase a producción	24x7, durante 07 días calendarios contados a partir de la fecha de pase a producción de cada componente transaccional del servicio.
Reportes	Durante el periodo de vigencia del contrato. A más tardar el quinto día calendario de cada mes, el proveedor debe entregar al Banco todos los reportes e informes relacionados al desempeño y consumo del servicio en el mes anterior y que son descritos en el numeral 10.2. ("ENTREGABLES MENSUALES UNA VEZ IMPLEMENTADOS LOS SERVICIOS") de los términos de referencia.

### 9.3. Mantenimientos Preventivos Programados, de Urgencia o Correctivos

El proveedor podrá suspender ocasionalmente la disponibilidad de los componentes del servicio para realizar tareas de mantenimiento de los siguientes tipos:

- **Preventivos Programados:** relacionadas a tareas que tienen por objeto el garantizar el rendimiento de los componentes del servicio prestado por el proveedor, actualizar el software y/o el hardware, reconfigurar un sistema, implementar mejoras identificadas por el propio proveedor o a solicitud del Banco, o para desplegar funcionalidades mejoradas o nuevas para cumplir mandatos impuestos por las redes de pago (Visa, Mastercard), autoridades gubernamentales o entidades reguladoras.
- **De Urgencia:** cuando el proveedor identifica una amenaza inmediata y material para los servidores u otros componentes tecnológicos críticos que afectan la disponibilidad del servicio prestado al Banco. En ocasiones implica la implementación de una solución temporal, en tanto se trabaja en la solución definitiva.
- **Correctivos:** aquellos que tienen por objeto implementar una solución definitiva a incidentes/defectos observados en el ambiente productivo.

El tiempo que duren estas interrupciones programadas, urgentes o correctivas deben ser excluidas del SLA de Disponibilidad.

Todo mantenimiento a los componentes del servicio debe ser comunicado con anticipación a la Subgerencia de Producción del Banco (a los teléfonos/direcciones de correo electrónico que a la firma del contrato este defina), en los siguientes términos:

Tipo	Notificación al Banco
Mantenimiento Preventivo Programado	7 días calendarios antes
Mantenimiento de Urgencia	4 horas antes
Mantenimiento Correctivo	5 días calendarios antes

Los mantenimientos preventivos o correctivos deben ser programados para ejecutarse en el día y la franja horaria de más baja transaccionalidad en el canal o canales de atención del Banco que podrían afectarse con los cambios, información que deberá ser proporcionada por el Banco al proveedor. En el caso de los mantenimientos de urgencia, ambas partes (el Banco y el proveedor) deberán evaluar y determinar la factibilidad de esperar hasta la franja horaria para la ejecución del mantenimiento.

Respecto a los mantenimientos en el ambiente Pre-Productivo, si el periodo de no disponibilidad del servicio será menor o igual a 8 horas, no será necesario que el proveedor notifique al Banco. En caso contrario, si la inactividad superase este periodo de tiempo, el proveedor deberá notificar a la Subgerencia Construcción de Aplicaciones del Banco (a los teléfonos/direcciones de correo electrónico que a la firma del contrato este defina) sobre el mantenimiento 24 horas antes como mínimo.

#### 9.4. Gestión de Incidencias

El SLA para la gestión de incidentes se limita a las incidencias identificadas en el ambiente Productivo por el propio proveedor o reportadas por el Banco a la Mesa de Ayuda.

Una vez identificado o reportado el incidente por el Banco (por teléfono o email), el personal de la mesa de ayuda del proveedor procederá a abrir un caso en el sistema de tickets, precisando su nivel de gravedad, a través del cual se gestionará y monitoreará el incidente hasta su resolución.

En caso el incidente sea identificado por el propio proveedor, este deberá informar sobre el evento inmediatamente a la Subgerencia de Producción del Banco, dentro de los 5 minutos siguientes (a los teléfonos/direcciones de correo electrónico que a la firma del contrato este defina), indicando el número del ticket abierto y las acciones inmediatas aplicadas o en proceso de aplicación.

En el caso de los incidentes reportados por el Banco, el primer contacto por parte del proveedor (a través de un email a los contactos que indique el Banco a la firma del contrato), confirmando el haber tomado conocimiento del evento, debe ser efectuado dentro de los 5 minutos posteriores al reporte antes mencionado.

Los incidentes serán clasificados de acuerdo con el nivel de gravedad o afectación al servicio de la siguiente manera:

Nivel de Gravedad	Descripción
Crítico	<ul style="list-style-type: none"> <li>• Cualquier componente del servicio no está disponible, o</li> <li>• cualquier Incidente que afecte al menos al treinta por ciento (30%) o más del número total de usuarios finales del componente del servicio, o</li> <li>• cualquier Incidente que afecte al menos al cinco por ciento (5%) o más del número total de operaciones donde interviene el componente del servicio durante un periodo de una hora, o</li> <li>• cualquier Incidente de seguridad que afecte a los sistemas, la información o los activos del proveedor o del Banco con un impacto potencial significativo en los ingresos o la reputación de ambas partes</li> </ul>

Moderado	<ul style="list-style-type: none"> <li>• Un incidente que afecte al menos al diez por ciento (10%) y no supere el treinta por ciento (30%) del número total de usuarios finales del componente del servicio, o bien</li> <li>• un incidente que afecte al menos al uno por ciento (1%) y no supere el cinco por ciento (5%) del número total de operaciones donde interviene el componente del servicio durante un periodo de una hora, o</li> <li>• cualquier Incidente de seguridad que afecte a los sistemas, información o los activos del proveedor o del Banco con impacto potencial en los ingresos o la reputación de ambas partes.</li> </ul>
Bajo	<ul style="list-style-type: none"> <li>• Cualquier Incidente que afecte a menos del diez por ciento (10%) del número total de Usuarios Finales del componente del servicio, o</li> <li>• cualquier Incidente que afecte a menos del uno por ciento (1%) del número total de operaciones donde interviene el componente del servicio durante un periodo de una hora, o</li> <li>• cualquier posible Incidente de seguridad que afecte a los sistemas, información o activos del proveedor o del Banco que no tenga un impacto inmediato en los ingresos o la reputación de ambas partes y que por ende no requiera de una acción sensible al tiempo</li> </ul>

Las métricas establecidas para determinar el nivel de gravedad deben aplicarse sobre los usuarios y operaciones donde interviene el componente del servicio afectado por el incidente.

Todos los incidentes serán evaluados y gestionados por el proveedor hasta su solución, y considerando su nivel de gravedad, deberán resueltos como máximo en los siguientes plazos:

Acción	Nivel de Gravedad del Incidente		
	Crítico	Moderado	Bajo
Primera respuesta	30 minutos	60 minutos	2 horas
Solución del incidente	60 minutos	4 horas	24 horas

Otras consideraciones importantes respecto a la gestión de los incidentes son:

- El tiempo de resolución se empieza a contar desde el momento del registro del incidente (como nuevo caso) en el sistema de tickets del proveedor.
- A través de la primera respuesta el proveedor informará a la Subgerencia de Producción del Banco (a los teléfonos/direcciones de correo electrónico que a la firma del contrato este defina), de forma breve pero concreta, sobre los componentes del servicio afectados por la incidencia, la forma y el nivel de afectación a los clientes del BN, así como el tiempo estimado de solución, el que no debe exceder a los máximos establecidos de acuerdo a la criticidad del incidente.
- Consideran tanto horas laborables como no laborables.
- El proveedor deberá alcanzar una matriz de escalamiento al Banco, con los nombres y datos de contacto a donde recurrir en segunda o tercera instancia en caso de demoras en la gestión del incidente.
- Para el caso de los incidentes críticos y moderados, una vez resueltos y como parte del cierre del ticket, el proveedor deberá entregar a la Subgerencia de Producción del Banco, **en un tiempo no mayor a 3 días hábiles**, un informe que contenga principalmente:
  - ✓ La causa raíz del incidente.
  - ✓ Detalle de acciones de mitigación y recuperación efectuadas. Debería precisarse si la solución aplicada fue temporal o definitiva.
  - ✓ Cronología de los acontecimientos desde el reporte hasta la resolución del incidente.

- ✓ Plan de acciones posteriores a la resolución del incidente, de corresponder. Generalmente esto se debería dar cuando el incidente se atendió con una solución temporal y se requerirá de un mantenimiento correctivo para aplicar una solución definitiva. Si se trata de un incidente crítico, el mantenimiento correctivo deberá ejecutarse e implementarse en el ambiente productivo en un plazo no mayor de 20 días laborables.
- El proveedor debe registrar periódicamente en el sistema de tickets un reporte resumido y a muy alto nivel, pero claro, del estatus del avance en la resolución del incidente. Así:
  - ✓ Si el incidente es crítico: se reportará estatus cada 30 minutos.
  - ✓ Si el incidente es moderado: se reportará estatus cada 1 hora.
  - ✓ Si el incidente es bajo: se reportará estatus cada 6 horas.

Quedan exceptuados de este SLA los siguientes casos:

- Las incidencias en los servicios/aplicaciones de las redes de pago (Visa, MasterCard), Banco de la Nación o de terceros fuera del control del proveedor.
- Las incidencias producto de un fallo o uso inadecuado de los Servicios por parte del Banco.

#### 9.5. Gestión de Problemas

Si se identifican dos o más incidentes iguales se creará un problema el cual se debe identificar y eliminar la causa raíz.

El problema será registrado en la Mesa de Ayuda del Banco, tendrá una revisión semanal. Si la causa raíz es atribuible al proveedor la eliminación debe ser máximo a los 30 días calendarios luego de haber sido registrado, luego de lo cual el proveedor deberá entregar a la Subgerencia de Producción del Banco (en un plazo no mayor de 3 días hábiles) un informe detallando la causa raíz del problema, así como las acciones y cambios efectuados para solucionarlo. Cuando el problema no sea atribuible al proveedor, este último deberá proporcionar al Banco toda la evidencia de la revisión de sus componentes tecnológicos.

#### 10. ENTREGABLES

Como parte del servicio el proveedor deberá proporcionar al Banco de la Nación los siguientes entregables:

##### 10.1. POR SERVICIOS DE IMPLEMENTACION:

###### 10.1.1. Por la Implementación/Configuración del servicio de Generación y Validación de CVV2 Dinámico para Tarjetas de Débito Visa:

- Acta firmada por la Subgerencia Construcción de Aplicaciones, dando conformidad de la recepción de la URL y credenciales de acceso a portal web donde el personal del Banco pueda acceder a documentación técnica y funcional de los componentes de software del proveedor (APIs, SDK, entre otros), así como especificaciones de los componentes de software que debe implementar el Banco y que son requeridos para la implementación del componente del servicio del proveedor.
- El esquema/diagrama de arquitectura y comunicaciones implementado para poner el componente de servicio en producción, el que debe haber sido revisado y aceptado formalmente por el Banco de la Nación (por la Subgerencia Arquitectura de TIC).
- Acta firmada por la Oficina de Seguridad Informática, dando conformidad de la recepción de la documentación del tipo de algoritmos criptográficos utilizados para el cifrado de la información confidencial de los clientes del Banco.
- El proveedor deberá presentar acta de conformidad firmada por la

Subgerencia Innovación Digital, la Subgerencia Canales Alternos (Gerencia Banca Digital) y la Subgerencia de Producción (Gerencia Tecnologías de Información) del Banco de la Nación, dando conformidad de la implementación en el ambiente productivo de las siguientes funcionalidades/parametrizaciones:

- Caducidad automática de cada CVV2 dinámico generado por tiempo de vigencia definido por el Banco y parametrizado en la plataforma del proveedor.
- Caducidad automática del CVV2 dinámico por solicitud de validación procesada.
- CVV2 dinámico solo puede ser usado durante su periodo de vigencia y en una sola transacción de la tarjeta de débito para la cual fue generado, independientemente de si la transacción fue autorizada o denegada por el Banco.
- Proceso batch para enrolamiento o baja masiva de tarjetas de débito de la plataforma del proveedor.
- SDK del proveedor integrado a versiones Android e iOS de la App Banca Móvil del Banco, de tal forma que el tarjetahabiente pueda por si mismo:
  - ✓ Solicitar en línea a la plataforma del proveedor la generación de un CVV2 dinámico para su tarjeta de débito.
  - ✓ Visualizar el CVV2 dinámico generado por la plataforma del proveedor en la pantalla de la aplicación móvil
- API del proveedor integrado a las siguientes aplicaciones del Banco de la Nación, de tal forma que se proceda a enrolar la tarjeta de débito Visa del Banco en la plataforma de CVV2 Dinámico del proveedor:
  - ✓ Transacciones 4556, 4554, 4510 y 4520 del aplicativo SARAWEB, que se usan en la red de agencias del Banco de la Nación para registrar la entrega de una tarjeta de débito Visa al cliente. Esta integración debe permitir el enrolamiento en línea de la tarjeta en la plataforma del proveedor.
  - ✓ Componente de software del Banco que se ejecutará automáticamente todos los días y que se encargará de regularizar masivamente el enrolamiento de las tarjetas de débito Visa entregadas en la fecha y cuyo enrolamiento en línea no se pudo efectivizar en la plataforma del proveedor.
- API del proveedor integrado a las siguientes aplicaciones del Banco de la Nación, de tal forma que se proceda a dar de baja la tarjeta de débito Visa del Banco en la plataforma de CVV2 Dinámico del proveedor:
  - ✓ Transacción 4540 del aplicativo Saraweb, que permite realizar el bloqueo de la tarjeta de débito VISA en la red de agencias del Banco. Esta integración debe permitir la baja en línea de la tarjeta en la plataforma del proveedor.
  - ✓ Componente de software del Banco que es invocado por el IVR (del Call Center) para realizar el bloqueo de la tarjeta de débito VISA. Esta integración debe permitir la baja en línea de la tarjeta en la plataforma del proveedor.
  - ✓ Componente de software del Banco que invocan los canales Banca Móvil y Banca por Internet para efectuar el bloqueo de la tarjeta de débito VISA. Esta integración debe permitir la baja en línea de la tarjeta en la plataforma del proveedor.
  - ✓ Componente de software del Banco que se ejecutará automáticamente todos los días y que se encargará de regularizar masivamente la baja, en la plataforma de CVV2 dinámico del proveedor, de las tarjetas de débito Visa vencidas (caducadas) y las bloqueadas/anuladas en la fecha, cuya baja en línea no se pudo efectivizar.

- o API o interfaz ISO8583 del proveedor (en función a lo que el Banco defina) integrado al componente Host del Banco de la Nación que procesa las solicitudes de autorización de transacciones provenientes de Visa, de tal forma que este API/interfaz ISO8583 atienda los requerimientos de validación de CVV2 dinámico, cuyo resultado (positivo o negativo) es requisito indispensable para continuar con el proceso de autorización. Si se optó por la interfaz ISO8583, la integración debió efectuarse usando el formato ISO de VISA.
- El proveedor proporcionará URL y credenciales de acceso a portal web que usarán las áreas del back office del Banco de la Nación para atender consultas, requerimientos y reclamos de clientes, así como de entidades externas, relacionados al uso del CVV2 dinámico durante la realización de operaciones con tarjeta NO presente. El proveedor deberá presentar un acta de conformidad firmada por la Subgerencia Canales Alternos (Gerencia Banca Digital), dando conformidad de la correcta operatividad de las funcionalidades requeridas en este portal y que se detallan en el numeral 7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO.
- Acta firmada por la Subgerencia Producción y la Subgerencia Construcción de Aplicaciones, ambas pertenecientes a la Gerencia de Tecnologías de Información, dando conformidad del mecanismo implementado para la entrega por parte del proveedor de los logs para auditoría de las actividades relacionadas al consumo de los componentes de software de su solución, considerando para tal efecto una de las 2 alternativas posibles descritas en el numeral 7.1 de este documento.

**10.1.2. Por la Implementación/Configuración del servicio de Generación y Validación de CVC2 Dinámico para Tarjetas de Crédito Mastercard:**

- Acta firmada por la Subgerencia Construcción de Aplicaciones, dando conformidad de la recepción de la URL y credenciales de acceso a portal web donde el personal del Banco pueda acceder a documentación técnica y funcional de los componentes de software del proveedor (APIs, SDK, entre otros), así como especificaciones de los componentes de software que debe implementar el Banco y que son requeridos para la implementación del componente del servicio.
- El esquema/diagrama de arquitectura y comunicaciones implementado para poner el componente de servicio en producción, el que debe haber sido revisado y aceptado formalmente por el Banco de la Nación (por la Subgerencia Arquitectura de TIC).
- Acta firmada por la Oficina de Seguridad Informática, dando conformidad de la recepción de la documentación del tipo de algoritmos criptográficos utilizados para el cifrado de la información confidencial de los clientes del Banco (especificación del algoritmo, datos y tipo de llaves de cifrado).
- El proveedor deberá presentar acta de conformidad firmada por la Subgerencia Innovación Digital, la Subgerencia Banca Personal (Gerencia Productos e Inclusión Financiera) y la Subgerencia de Producción (Gerencia Tecnologías de Información) del Banco de la Nación, dando conformidad de la implementación en el ambiente productivo de las siguientes funcionalidades/parametrizaciones:
  - o Caducidad automática de cada CVC2 dinámico generado por tiempo de vigencia definido por el Banco y parametrizado en la plataforma del proveedor.
  - o Caducidad automática del CVC2 dinámico por solicitud de validación procesada.
  - o CVC2 dinámico solo puede ser usado durante su periodo de vigencia y en una sola transacción de la tarjeta de crédito para la cual fue generado, independientemente de si la transacción fue autorizada o

- denegada por el Banco.
- Proceso batch para enrolamiento o baja masiva de tarjetas de crédito de la plataforma del proveedor.
- SDK del proveedor integrado a versiones Android e iOS de la App Banca Móvil del Banco, de tal forma que el tarjetahabiente pueda por si mismo:
  - ✓ Solicitar en línea a la plataforma del proveedor la generación de un CVC2 dinámico para su tarjeta de crédito.
  - ✓ Visualizar el CVC2 dinámico generado por la plataforma del proveedor en la pantalla de la aplicación móvil.
- API del proveedor integrado a las siguientes aplicaciones del Banco de la Nación, de tal forma que se proceda a enrolar la tarjeta de crédito Mastercard del Banco en la plataforma de CVV2 Dinámico del proveedor:
  - ✓ Transacción 4004 del aplicativo SARAWEB que se usa en la red de agencias del Banco de la Nación para activar la tarjeta de crédito Mastercard que está siendo entregada al cliente. Esta integración debe permitir el enrolamiento en línea de la tarjeta en la plataforma del proveedor.
  - ✓ Componente de software del Banco que se ejecutará automáticamente todos los días y que se encargará de regularizar masivamente el enrolamiento de las tarjetas de crédito Mastercard entregadas en la fecha y cuyo enrolamiento en línea no se pudo efectivizar en la plataforma del proveedor.
- API del proveedor integrado a las siguientes aplicaciones, de tal forma que se proceda a dar de baja la tarjeta de crédito Mastercard del Banco en la plataforma de CVV2 Dinámico del proveedor:
  - ✓ Funcionalidad de bloqueo de tarjeta de crédito del aplicativo MIG de empresa Izipay. Esta integración debe permitir la baja en línea de la tarjeta en la plataforma del proveedor.
  - ✓ Componente de software del Banco que se ejecutará automáticamente todos los días y que se encargará de regularizar masivamente la baja, en la plataforma de CVV2 dinámico del proveedor, de las tarjetas de crédito Mastercard vencidas (caducadas) y las bloqueadas/anuladas en la fecha, cuya baja en línea no se pudo efectivizar.
- API o interfaz ISO8583 del proveedor (en función a lo que el Banco defina) integrado al componente de software de la empresa (IZIPAY) que procesa a nombre del Banco de la Nación las solicitudes de autorización de transacciones provenientes de Mastercard, de tal forma que este API/ interfaz ISO8583 atienda los requerimientos de validación de CVC2 dinámico, cuyo resultado (positivo o negativo) es requisito indispensable para continuar con el proceso de autorización. Si se optó por la interfaz ISO8583, la integración debió efectuarse usando el formato ISO de Mastercard.
- El proveedor proporcionará URL y credenciales de acceso a portal web que usarán las áreas del back office del Banco de la Nación para atender consultas, requerimientos y reclamos de clientes, así como de entidades externas, relacionados al uso del CVC2 dinámico durante la realización de operaciones con tarjeta NO presente. El proveedor deberá presentar un acta de conformidad firmada por la Subgerencia Banca Personal (Gerencia Productos e Inclusión Financiera), dando conformidad de la correcta operatividad de las funcionalidades requeridas en este portal y que se detallan en el numeral 7. ALCANCE Y DESCRIPCIÓN DEL SERVICIO.
- Acta firmada por la Subgerencia Producción y la Subgerencia Construcción de Aplicaciones, ambas pertenecientes a la Gerencia de

Tecnologías de Información, dando conformidad del mecanismo implementado para la entrega por parte del proveedor de los logs para auditoría de las actividades relacionadas al consumo de los componentes de software de su solución, considerando para tal efecto las 2 alternativas posibles descritas en el numeral 7.1 de este documento.

### 10.1.3. Soporte Técnico

- Acta firmada por la Subgerencia Construcción de Aplicaciones, de la Gerencia de Tecnologías de Información, dando conformidad de la disponibilidad y accesos al Ambiente Pre-Productivo.
- Acta firmada por la Subgerencia Producción, de la Gerencia de Tecnologías de Información, dando conformidad de la disponibilidad y accesos al Ambiente Productivo.
- Acta firmada por la Subgerencia Producción, de la Gerencia de Tecnologías de Información, dando conformidad de la recepción de lo siguiente como parte de la puesta en marcha de la Mesa de Ayuda del proveedor:
  - o Número(s) telefónicos y direcciones de correo donde reportar incidencias
  - o Matriz de escalamiento con los nombres y datos de contacto a donde recurrir en segunda o tercera instancia en caso de demoras en la gestión de incidentes.
- Acta firmada por la Subgerencia Producción, de la Gerencia de Tecnologías de Información, dando conformidad de la recepción de lo siguiente como parte de la puesta en marcha del Sistema de Tickets del proveedor:
  - o URL y credenciales de acceso a portal web donde personal de la Subgerencia Producción, de la Gerencia de Tecnologías de Información y áreas del back office del Banco ingresarán para hacer seguimiento de los tickets en proceso de atención por incidentes reportados o por requerimientos efectuados por el Banco.
  - o Manual de operación del sistema de tickets.

## 10.2. ENTREGABLES MENSUALES UNA VEZ IMPLEMENTADOS LOS SERVICIOS

### 10.2.1. Por las Atenciones de los Componentes Transaccionales del Servicio

- El proveedor deberá emitir dentro de los 5 primeros días de cada mes un informe sobre las atenciones prestadas al Banco durante el mes anterior, el que sustentará su facturación; informe que deberá contener al menos lo siguiente:
  - o Total de tarjetas activas en la plataforma del proveedor en el mes a facturar.
  - o Total de CVV2 dinámicos generados y total de validados en el periodo (a solicitud del autorizador del Banco), precisándose en este último caso cuantos fueron CVV2 válidos y cuantos no.
  - o Respecto a las tarjetas enroladas en la plataforma de CVV2 dinámico del proveedor:
    - ✓ Total de tarjetas enroladas en la plataforma al inicio del periodo a facturar.
    - ✓ Total de tarjetas que fueron enroladas en la plataforma del proveedor durante el periodo a facturar.
    - ✓ Total de tarjetas dadas de baja en la plataforma del proveedor durante el periodo a facturar.
    - ✓ Total de tarjetas enroladas en la plataforma al final del periodo a facturar.

- En complemento al informe mensual antes mencionado, el proveedor deberá entregar también dentro de los 5 primeros días de cada mes los siguientes reportes:
  - Reporte, en formato CSV o XLS, con el detalle de las tarjetas que se consideraron activas en el periodo facturado. Insumo para el proceso de conciliación interna que el Banco debe efectuar para emitir su conformidad del servicio.
  - Reporte, en formato CSV o XLS, con el detalle de las tarjetas a las que se generó al menos un CVV2 dinámico en el periodo facturado. Insumo para el proceso de conciliación interna que el Banco debe efectuar para emitir su conformidad del servicio.
- Informe mensual que incluya estadísticas de cada componente de software del proveedor: (1) TPS promedio, (2) TPS máximo alcanzado, (3) número total de transacciones procesadas, (4) Tiempos de respuesta promedio por día (en milisegundos), (5) porcentaje de disponibilidad mensual, (6) tasa de errores y (7) evidencia de escalabilidad del servicio durante picos de demanda.
- El proveedor deberá entregar API(s) (y asegurar la disponibilidad de estos), que permitan al Banco obtener reportes con el detalle que sustenta cada uno de los totales consignados en el informe mensual del proveedor.

#### 10.2.2. Soporte Técnico

El proveedor deberá emitir dentro de los 5 primeros días de cada mes un informe sobre las atenciones prestadas al Banco como parte del servicio de soporte técnico, el que por lo menos debe contener:

- Número de incidentes reportados en el periodo, cantidad de resueltos y en proceso, tiempos de atención de estos incidentes agrupados por rangos de horas.
- Total de tickets de registrados en el periodo, precisando cuantos están relacionados a incidentes y cuantos a otro tipo de requerimientos, situación de los tickets y tiempos de atención por rangos de tiempo.

#### 11. RECURSOS DE PERSONAL DEL PROVEEDOR

El proveedor asignará recursos dedicados a la implementación de los componentes del servicio que prestará al Banco, al que colectivamente se llamará "Equipo del Proyecto del Proveedor", el mismo que es calificado como **personal clave**.

El equipo del proyecto del proveedor estará compuesto por:

- **Un (01) Jefe de Proyecto**, quien desarrollara las siguientes funciones entre otras que se presenten durante la ejecución del servicio:
  - Organiza la reunión de lanzamiento del proyecto.
  - Lidera con su par del Banco la etapa inicial de planificación del proyecto de implementación de los componentes del servicio.
  - Se encarga de las actividades de seguimiento del proyecto
  - Gestiona la solución de inconvenientes o levantamiento de bloqueantes del proyecto, velando por el cumplimiento del plan de trabajo establecido durante la etapa de planificación.
  - Se apoya en los otros miembros del equipo del proyecto del proveedor para completar la configuración y puesta en marcha de los componentes del servicio.
- **Un (01) Ingeniero de Integración y Seguridad**, quien desarrollara las siguientes funciones:
  - Lidera la ejecución de las tareas de integración y configuración en los ambientes de Pre-productivo y Producción en coordinación con el equipo técnico del Banco.

- Se encarga, en coordinación con el equipo técnico del Banco, de la definición e implementación de la conectividad entre las redes del proveedor y el Banco de la Nación para ISO, lotes y flujos API en los ambientes de Preproducción y Producción, garantizando la seguridad de la solución definida.
- **Un ingeniero de Soporte de Componentes de Software**, quien desarrollara las siguientes funciones
  - Se encarga de liderar la capacitación y acompañamiento al equipo de desarrollo del Banco sobre el SDK móvil y API(s) del proveedor y su integración a los componentes de software y canales de atención del Banco (como el App BN o el home banking), como parte de la implementación de los componentes del servicio.
  - Se encarga de liderar el acompañamiento al Banco durante las actividades de certificación ante las redes de pago (Visa, Mastercard).

El proveedor se compromete a no reasignar ni remover ningún miembro de su personal clave asignado, sólo en caso fortuito o motivo de fuerza mayor se permitirá el reemplazo previa evaluación del Banco.

El Banco de la Nación podrá solicitar al proveedor el reemplazo de miembros de su personal, comprometiéndose el proveedor a asignar personal de calificaciones similares o superiores a las previstas en el requerimiento para el personal a ser reemplazado. De aplicarse este caso, el proveedor debe proponer a un nuevo personal en un plazo de siete (07) días hábiles, el Banco tendrá hasta dos (02) días calendario para realizar la aprobación del personal propuesto a través de correo electrónico, el proveedor tiene tres (03) días calendario como máximo (posterior a la aprobación) para presentar al Banco al nuevo personal. Durante este periodo, el proveedor deberá de asegurar el soporte técnico con un personal provisional, por lo tanto, no excluye al proveedor el cumplimiento del SLA.

De producirse un reemplazo de algún personal por caso fortuito o motivo de fuerza mayor (como por ejemplo la renuncia irrevocable de un miembro del equipo del proyecto del proveedor), el proveedor comunicará la salida del personal con un plazo máximo de 24 horas de ocurrido el evento, el proveedor debe proponer a un nuevo personal en un plazo máximo de diez (10) días hábiles, el Banco tendrá hasta un (01) día calendario para realizar la aprobación del personal propuesto a través de correo electrónico. El proveedor tiene dos (02) días calendario como máximo (posterior a la aprobación) para presentar al Banco al nuevo personal. Durante este periodo, el proveedor deberá de asegurar el soporte técnico con un personal provisional, por lo tanto, no excluye al proveedor el cumplimiento del SLA. Se indica que el personal reemplazante debe tener características iguales o superiores a las previstas en el requerimiento para el personal a ser reemplazado.

## 12. ADMINISTRADOR DEL CONTRATO Y MEDIDAS DE CONTROL

### c) **Administrador del Contrato**

La Subgerencia Canales Alternos de la Gerencia Banca Digital, a través de la Sección Canales Virtuales, se encargará de la administración del contrato, siendo responsable de la supervisión y coordinación de la prestación contratada.

### d) **Medidas de Control**

La Subgerencia Canales Alternos, de la Gerencia Banca Digital, a través de la Sección Canales Virtuales, durante la ejecución contractual desarrollará las siguientes actividades de control:

- Verificar el cumplimiento de las características y condiciones técnicas establecidas en los presentes términos de referencia.
- El personal designado por la Sección Canales Virtuales al detectar observaciones durante la prestación del servicio, las mismas serán puestas de

conocimiento al proveedor, otorgándosele un plazo de dos (02) a ocho (08) días calendario para sus subsanaciones. La subsanación de las observaciones no exime al proveedor de ser penalizado.

### 13. CONFORMIDAD DEL SERVICIO

La conformidad por la implementación del servicio será dada de la siguiente manera:

- La conformidad por la "Implementación/Configuración del servicio de Generación y Validación de CVV2 Dinámico para Tarjetas de Débito Visa" la darán la Subgerencia Innovación Digital, la Sección Canales Virtuales y la Subgerencia Canales Alternos de la Gerencia de Banca Digital.
- La conformidad por la "Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para tarjetas de crédito Mastercard" la darán la Subgerencia Innovación Digital, la Sección Canales Virtuales y la Subgerencia Canales Alternos de la Gerencia de Banca Digital; así como la Subgerencia Banca Personal de la Gerencia de Productos e Inclusión Financiera.

Respeto a la conformidad del servicio luego de su puesta en operación, esta será dada por la Sección Canales Virtuales y la Subgerencia Canales Alternos de la Gerencia Banca Digital del Banco de la Nación.

Respecto al servicio de generación y validación del CVV2 Dinámico para las tarjetas de crédito Mastercard, la Subgerencia Banca Personal (Gerencia Productos e Inclusión Financiera) remitirá a la Sección Canales Virtuales un informe dando conformidad del servicio recibido en el periodo facturado por el proveedor.

Recibidos los entregables descritos en el numeral 10, el Banco tendrá el plazo de veinte (20) días calendarios para emitir el acta de conformidad por la implementación de los componentes del servicio y diez (10) días calendarios por la prestación del servicio transaccional mensual y el de soporte técnico.

### 14. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

#### 14.1 Lugar

La prestación del servicio se prestará de forma remota.

#### 14.2 Plazo

El plazo de prestación del servicio queda establecido en:

- a) Dos semanas (15 días calendarios) para el Kick off y la planificación del proyecto.
- b) Ocho (08) meses calendarios por la Implementación del servicio de generación y validación del CVV2 dinámico para tarjetas de débito del BN (lo que se evidenciará con la emisión del acta de conformidad correspondiente por parte del Banco)
- c) Ocho (08) meses calendarios por la Implementación del servicio de generación y validación del CVC2 dinámico para tarjetas de crédito del BN (lo que se evidenciará con la emisión del acta de conformidad correspondiente por parte del Banco)
- d) Servicio Transaccional (generación y validación de CVV2/CVC2 dinámico): Treinta y seis (36) meses. Se empieza a ejecutar una vez culminada la implementación del primer componente transaccional (independientemente de cuál de los 2 sea) en el ambiente de producción.

- e) Soporte Técnico: Treinta y seis (36) meses, paralelo a la prestación del servicio transaccional en producción.

Las implementaciones descritas en los literales b) y c) se deben ejecutar en paralelo.

El plazo de EL CONTRATO será por un periodo de cuarenta y cuatro (44) meses y dos semanas, el cual rige desde la fecha de su firma, conforme se establece en el numeral 14.2 de los Términos de Referencia. Por la prestación del servicio transaccional y de soporte técnico (que ambos tienen un plazo de 36 meses), éstos podrán ser renovados antes de su vencimiento y por el mismo periodo de 36 meses; lo cual se materializara mediante la suscripción de una adenda.

Sin perjuicio de ello, cualquiera de LAS PARTES podrá resolver EL CONTRATO de forma unilateral sin expresión de causa, comunicándolo por escrito a su contraparte con al menos un (1) año de anticipación antes del vencimiento del plazo contractual en curso.

**a) Plazos de Implementación de componentes transaccionales del Servicio**

A continuación, los plazos en los que el proveedor debe implementar en paralelo los 2 componentes transaccionales del servicio:

Componente del Servicio	Plazo de Implementación
Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de débito Visa	8 meses calendarios
Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para tarjetas de crédito Mastercard	8 meses calendarios

**b) Plan de implementación base**

Considerando los recursos requeridos para las integraciones, la secuencia de implementación de los componentes transaccionales del servicio será la siguiente:

Componente del servicio	2 semanas	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8
Kick off y planificación del proyecto									
Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de débito Visa									
Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para tarjetas de crédito Mastercard									

Se consideran como parte del plazo de implementación 2 semanas iniciales (14 días calendarios), dentro las cuales se conformarán los equipos de trabajo de ambas partes, se realizará el Kick off del proyecto y se elaborará la forma conjunta (equipos del proveedor y Banco de la Nación) el detalle del plan de trabajo a ejecutar para implementar en paralelo los 2 componentes transaccionales del servicio, plan que será firmado por ambas partes, con las actividades e hitos que se deben cumplir para la puesta en producción del servicio. El plan de trabajo resultante formará parte de estos términos de referencia y considerará para su elaboración los lineamientos establecidos en la metodología del Ciclo de Vida del Software del Banco.

El plazo máximo establecido para implementar cada componente transaccional del servicio empezará a correr una vez concluidas las 2 semanas de planificación del proyecto.

## 15. FORMA DE PAGO

El Banco realizará el pago de la contraprestación pactada a favor del Proveedor en Soles, previa conformidad de la prestación, debiéndose exigir al Proveedor el fiel cumplimiento de las obligaciones contraídas.

### a) Por Implementación del Servicio

Se efectuará en pago único por cada servicio de implementación de los siguientes componentes transaccionales:

- Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para Tarjetas de Débito Visa.
- Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para Tarjetas de Crédito Mastercard.

Para que este pago único por cada componente transaccional implementado se pueda efectivizar, el proveedor debe cumplir con presentar la siguiente documentación:

- Remitir todos los documentos que se indican en el numeral 10. ENTREGABLES del presente documento, en lo que corresponda al componente del servicio por cuya implementación se va realizar el pago.
- Comprobante de pago emitido por el proveedor.
- Presentar Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- Presentar Informe Técnico emitido por la Subgerencia de Producción de la Gerencia de Tecnologías de Información confirmando el despliegue del servicio en ambiente productivo, tanto de los componentes del proveedor como de los componentes que el Banco haya tenido que implementar como parte de la integración.
- Presentar Acta de conformidad, emitida por la Subgerencia Innovación Digital, Sección Canales Virtuales y Subgerencia Canales Alternos de la Gerencia de Banca Digital. En caso el componente del servicio implementado esté relacionado a la tarjeta de crédito, el acta de conformidad será también firmada por la subgerencia Banca Personal. Una vez el proveedor haya remitido todos los entregables descritos en el numeral 10 de este documento, el Banco tendrá 20 días hábiles(laborables) para emitir el acta de conformidad respectiva.

### b) Por Servicios Transaccionales

#### - Costo por tarjeta activa en la plataforma del proveedor:

El Banco efectuará un pago mensual dependiente del número de PAN activos en la plataforma del proveedor en el periodo facturado, bajo las siguientes consideraciones:

- El enrolamiento de las tarjetas del Banco de la Nación en la plataforma del proveedor no las convierte en activas por defecto.
- Un PAN enrolado se convierte activo cuando se genera con éxito el primer CVV2/CVC2 dinámico para esta tarjeta, independientemente de si se llega luego a utilizar o no como parte de un requerimiento de autorización de una operación con tarjeta no presente.

Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

- Se cobra por el PAN activo en el periodo, independientemente del número de CVV2 dinámicos generados o validados para el PAN.
- Un PAN permanece con la condición de activo en la plataforma del proveedor (independientemente si transacciona o no) hasta el mes en el que el Banco solicita su baja o eliminación mediante el API/SDK correspondiente.

El costo mensual a pagar por el Banco se define por rango de número de tarjetas (PAN) activas en la plataforma del proveedor y se aplica el modelo de precios escalonados. Es decir, el precio total a pagar es igual a la suma del número de PAN activos multiplicado por el respectivo costo unitario (CU) por la ejecución del servicio en cada rango.

A continuación, los rangos para los que los postores deberán presentar sus propuestas de costos unitarios:

N° de PAN Activos	Costo Unitario por PAN Activo (S/ inc. IGV)	Demanda Mensual Estimada de PAN Activos Año 01	Demanda Mensual Estimada de PAN Activos Año 02	Demanda Mensual Estimada de PAN Activos Año 03	Requerimiento Total estimado del servicio
De 1 hasta 200,000		200,000			2,400,000
De 200,001 hasta 1,000,000			350,000	500,000	10,200,000
De 1,000,001 hasta 3,000,000					
Más de 3,000,000					

Así, si en un mes determinado hubiese 800.000 tarjetas del BN enroladas y activas en la plataforma de CVV2 dinámico del proveedor, el Banco debería pagar:

$$\text{Total a pagar} = (200.000 * \text{CU Rango 1}) + (600.000 * \text{CU Rango 2})$$

(CU = Costo Unitario)

Para que el pago por los servicios transaccionales pueda efectivizarse, todos los meses el proveedor debe presentar la siguiente documentación:

- Comprobante de pago emitido por el proveedor.
- Los documentos que se indican en el numeral 10. ENTREGABLES del presente documento, en lo que respecta a los informes por las atenciones brindadas por los componentes transaccionales.
- Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- Acta de conformidad, emitida por la Sección Canales Virtuales y firmada además por la Subgerencia Canales Alternos de la Gerencia de Banca Digital y la Subgerencia Banca Personal de la Gerencia de Productos e Inclusión Financiera. Una vez el proveedor haya remitido todos los entregables descritos en el numeral 10 de este documento, el Banco tendrá 10 días hábiles (laborables) para emitir el acta de conformidad respectiva.
- Documentación que evidencie certificación vigente del proveedor como PCI DSS.

**c) Por Servicio de Soporte Técnico**

Pago fijo mensual, para que el pago pueda efectivizarse el proveedor todos los meses debe presentarse la siguiente documentación:

- Comprobante de pago emitido por el proveedor.

- Carta simple dirigida al Subgerente de Compras de la Gerencia de Administración y Logística.
- Acta de conformidad, emitida por la Sección Canales Virtuales y Subgerencia Canales Alternos de la Gerencia de Banca Digital. Una vez el proveedor haya remitido todos los entregables descritos en el numeral 10 de este documento, el Banco tendrá 10 días hábiles(laborables) para emitir el acta de conformidad respectiva.
- Si se trata del primer pago: un informe de la Subgerencia de Producción, de la Gerencia de Tecnologías de Información, confirmando el despliegue/entrega en el ambiente productivo de todas los entregables que se indican en el numeral 10. ENTREGABLES del presente documento, en lo que corresponda este componente del servicio.

#### **Lugar de entrega de documentación requerida para el pago**

La documentación se debe presentar en la Sede Principal del Banco de la Nación, sito en Av. Javier Prado Este N° 2499 – Distrito de San Borja, Lima, 1er Piso, Modulo de Sección Seguimiento Administrativo de Contratos – Subgerencia Compras.

#### **Plazo para el Pago**

La Entidad pagará las contraprestaciones pactadas a favor del proveedor dentro de los quince (15) días calendario siguiente a la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello.

#### **16. RESPONSABILIDAD POR VICIOS OCULTOS**

La recepción conforme de la prestación por parte del BN no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos. El plazo máximo de responsabilidad del proveedor por la calidad ofrecida y por los vicios ocultos de los servicios ofertados es de un (01) año contado a partir de la última conformidad otorgada.

#### **17. SUBCONTRATACION**

Se permitirá que el proveedor pueda como máximo subcontratar actividades complementarias (No la principal o principales, que en este caso serían los componentes para generar y validar el CVV2 Dinámico) hasta por el 40% del monto del contrato inicial.

Es importante precisar que la subcontratación no enerva la responsabilidad del proveedor, pues este mantiene la responsabilidad por la ejecución total de su contrato frente al BN.

#### **18. PENALIDADES**

##### **18.1 Penalidad por Mora**

##### **Por Moras en la Implementación del Servicio**

En caso de retraso injustificado del Proveedor en la implementación y puesta en producción de los componentes transacciones del servicio (generación y validación de CVV2 dinámico para tarjeta de débito Visa y para tarjeta de crédito Mastercard), el Banco de la Nación aplicará automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria (S/)} = \frac{0.10 * (\text{Costo de implementación del componente transaccional})}{0.25 * (\text{Plazo en días para implementación del componente transaccional})}$$

## 18.2 Otras Penalidades

### Por Cambio en el Equipo del Proyecto del Proveedor

N°	Penalidad	Monto de Penalidad	Procedimiento de Aplicación de la Penalidad
1	Por realizar el cambio de cualquiera de los miembros del equipo del proyecto del proveedor (Jefe de Proyecto, Ingeniero de Integración y Seguridad, Ingeniero de Soporte de Componentes de Software), sin previo aviso y sin la autorización/conformidad del Banco. La penalidad se aplicará por ocurrencia.	2 U.I.T.	La Subgerencia Canales Alternos remitirá informe y otra documentación requerida a la Sección Ejecución y Seguimiento de contratos.

### Por Niveles de Servicio

Si por alguna razón distinta a las descritas en el numeral 9, no se cumplieran los niveles de servicio requeridos por el Banco, se aplicarán las penalidades según tabla adjunta:

Penalidades			
N°	Supuestos de Aplicación de Penalidad	Monto de la Penalidad	Procedimiento de Aplicación de la Penalidad
1	Menos del 99.99% en la disponibilidad de los componentes transaccionales (para generación y validación de CVV2 dinámico)	5% del importe de facturación mensual en el que se presenta el problema, por cada día en el que se presente la intermitencia.	Informe de la Subgerencia de Producción con evidencia del incumplimiento del SLA.
2	Falta de soporte AD HOC (24x7) durante 07 días calendarios contados a partir de la fecha de pase a producción de cada componente transaccional del servicio	5% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia Canales Alternos con las evidencias y sustentos correspondientes
3	Incumplimiento de SLA en otros componentes de soporte (los no descritos en el ítem 2 de este cuadro)	1% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia Canales Alternos con las evidencias y sustentos correspondientes
4	No reporte oportuno al Banco de la no disponibilidad de componentes transaccionales del servicio por mantenimientos programados, urgentes o correctivos	3% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia Canales Alternos con las evidencias y sustentos correspondientes

5	Incumplimiento de SLA respecto a tiempos para primer contacto, primera respuesta, reportes periódicos, solución del incidentes o solución de Problemas; lo que incluye el incumplimiento en la entrega o entrega tardía del informe de cierre de la atención (aplicable para incidentes críticos y moderados; así como la gestión de los problemas)	3% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia de Producción con evidencia de monitoreo de la plataforma.
---	---	--	--

**Por Falta de Certificación Vigente durante la prestación del servicio**

N°	Supuestos de Aplicación de Penalidad	Monto de la Penalidad	Procedimiento de Aplicación de la Penalidad
1	Por no contar con la certificación vigente como PCI DSS	El 10% de la facturación mensual	Para el caso de la certificación como PCI DSS, debe solicitarse al proveedor el certificado de cumplimiento vigente.  La Subgerencia Canales Alternos remitirá informe y otra documentación requerida a la Sección Ejecución y Seguimiento de contratos.

No existe un límite de multas mensual durante la prestación del servicio.

Se precisa que cada uno de los tipos de penalidad (penalidad por mora y otras penalidades) pueden alcanzar un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, después de lo cual el Banco podrá resolver el contrato por incumplimiento.

**19. GARANTÍA COMERCIAL**

• **Alcance de la Garantía:**

Contra defectos de diseño y/o desarrollo del software, disponibilidad o fallas de funcionamiento de los componentes alojados en la nube, entre otros supuestos ajenos al uso normal o habitual de los servicios y no detectables al momento que se otorgó la conformidad, sin perjuicio a la entidad.

Para el periodo de garantía, los recursos asignados por el proveedor deben ser totalmente independientes a los recursos asignados a los servicios de soporte y mejoras continuas.

Se considerarán como garantía todos los errores detectados durante la operación en producción, los cuales hayan sido originados por fallas en la etapa de construcción respecto de las definiciones realizadas, aun cuando estos procesos hayan sido aprobados por el Banco de la Nación en etapa de pruebas integrales.

Las mejoras por garantía consideran los mismos SLA's declarados en este documento.

- **Periodo de la Garantía:**

La garantía debe incluir la corrección de cualquier error o diferencia con lo definido hasta 12 meses después de poner en producción el último componente transaccional del servicio.

- **Inicio del Cómputo de la Garantía:**

La garantía entrará en vigor después de poner en producción el último componente transaccional del servicio.

## 20. GARANTÍA FINANCIERA

El postor adjudicado con la buena pro del concurso de méritos entregará para el perfeccionamiento del contrato la garantía financiera (carta fianza) de fiel cumplimiento de contrato.

La garantía que se presente debe ser incondicional, solidaria, irrevocable y de realización automática en el país, al solo requerimiento del Banco de la Nación. Asimismo, debe ser emitida por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de Bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

La garantía financiera (cartas fianza) deberá ser emitida a favor del Banco de la Nación, por los conceptos, montos y vigencias siguientes:

- ✓ Garantía de fiel cumplimiento del contrato: por una suma equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

## 21. SEGUROS

### Póliza Tech E&O

Debe tener una Suma Asegurada mínima de US\$ 500,000.00 (quinientos mil y 00/00 dólares americanos) y debe detallar el alcance de los servicios que realizará el proveedor para tener cobertura.

La contratación de las pólizas de seguro a que hace referencia esta cláusula (en adelante, las "Pólizas") deberá cumplir las siguientes condiciones especiales:

- ✓ Incluir al Banco de la Nación como asegurado adicional.
- ✓ En el supuesto caso que las pólizas de seguros sean insuficientes o no puedan ejecutarse por cualquier motivo, ante la eventualidad de un siniestro, El proveedor asumirá directamente el pago de la indemnización a terceras personas, así como a la Entidad y/o a su personal y siempre que la responsabilidad sea atribuible a El proveedor.
- ✓ La no contratación de pólizas necesarias y adicionales, no libera de responsabilidad a el proveedor por los daños ocasionados al BN.
- ✓ En caso de siniestro, el importe del deducible será asumido por el proveedor. La Entidad, su personal y terceros afectados, serán íntegramente indemnizados.
- ✓ El pago de las primas de seguros correspondientes a las pólizas mencionadas, serán asumidas por el proveedor y corren por cuenta y riesgo de estos. El proveedor deberá evidenciar el pago total de los seguros presentados o en su defecto de ser

fraccionado el pago de las pólizas, deberá presentar copia del pago de la primera cuota, así como el convenio de pago respectivo.

- ✓ Las Pólizas deberán ser otorgadas por compañías de seguros de primer nivel (en adelante, el "Asegurador"), entendiéndose por éstas a las compañías de seguros calificadas como Categoría A conforme con lo establecido en el Reglamento para la Clasificación de Empresas de los Sistemas Financieros y de Seguros aprobado mediante la Resolución SBS N° 18400-2010, o la norma que la sustituya o modifique.
- ✓ El proveedor acepta que será de su total responsabilidad y asumirá a su total riesgo y responsabilidad, toda responsabilidad, gastos y costos por pérdidas y/o daños materiales y/o daños corporales, incapacidad o muerte de cualquier personas o personas, en la eventualidad que un accidente ocurra y el proveedor no haya provisto adecuadas coberturas cuando fuesen necesarias durante el desarrollo del presente Contrato.
- ✓ Si llegase a ocurrir un siniestro cuyo costo implique un monto mayor al asegurado por las Pólizas del proveedor, éste se compromete a resarcir todos los daños ocasionados, comprometiéndose a mantener indemne al Banco de la Nación.
- ✓ Las pólizas deberán indicar expresamente que el Asegurador renuncia a su derecho de subrogación contra el Banco de la Nación y/o funcionarios y/o empleados y/o clientes.
- ✓ Las Pólizas deberán especificar que el Banco de la Nación y/o funcionarios y/o empleados y/o clientes son asegurados adicionales, e incluir una cláusula en donde se especifique que serán considerados también como terceros en caso de siniestro.
- ✓ El Proveedor se obliga a entregar a Banco de la Nación, de manera previa al inicio de las actividades, copia de las Pólizas, el cronograma de pago y de las constancias de pago de las respectivas primas.
- ✓ Todos y cada uno de los deducibles y el pago de las primas de seguros correspondientes a las Pólizas, serán asumidas por el Proveedor.
- ✓ El Proveedor deberá cumplir con acreditar la renovación de las Pólizas (si corresponde) y, además, deberá comunicar al Banco de la Nación dentro de los treinta (30) Días calendario previo al vencimiento de cada una de las Pólizas la renovación de las mismas, adjuntando el cronograma de pago y las constancias de pago respectivas.
- ✓ Las Pólizas deberán indicar que son primarias en relación a cualquier otra póliza que tenga contratada BANCO DE LA NACIÓN.
- ✓ Independientemente de los requerimientos de los seguros a ser contratados, según este apéndice, la insolvencia, quiebra o falta de pago de los reclamos que surjan en virtud del contrato por parte de la compañía de seguros, no deberá ser interpretada como una renuncia a cualquiera de las disposiciones del contrato y la existencia de las coberturas de seguro requeridas en el presente documento no será interpretada de ninguna manera como una limitación de la responsabilidad que deberá asumir el proveedor hacia Banco de la Nación y/o cualquier otra persona, resultante de sus operaciones en virtud del contrato o relacionado de alguna otra manera con el contrato.

## 22. GESTIÓN DE AUDITORIA Y RIESGOS

### LINEAMIENTOS GENERALES:

- ❖ El Proveedor se obliga, siempre que se limite a información relacionada con la ejecución del contrato, a permitir la revisión, supervisión e inspección de los servicios prestados y de las condiciones que garanticen la seguridad de información, tratamiento de la información, protección de datos personales, continuidad del negocio y gestión de sus riesgos, por parte de la Dependencia Responsable del Contrato y la Unidad de Auditoría Interna del Banco, así como de la Sociedad Auditora Externa, la Superintendencia de Banca, Seguros y AFP, en la oportunidad que cualquiera lo solicite, con un aviso previo por escrito de diez (10) días hábiles (laborables), el cual

será remitido a la dirección indicada por el proveedor en el contrato. En dicho comunicado se designarán a las personas que efectuarán la mencionada revisión, supervisión e inspección. Consecuentemente el proveedor se compromete a facilitar todos los recursos y medios necesarios a las personas antes mencionadas para efectuar dichas revisiones.

- ❖ Los costos que implique la contratación de terceros, así como los costos de desplazamiento, hospedaje y alimentación del personal del Banco de la Nación con motivo de estas auditorías, revisiones, inspecciones, supervisiones, serán cubiertos por el Banco.
- ❖ El proveedor debe asegurar el acceso adecuado a la información, en tiempos razonables y a solo requerimiento, por parte de la SBS (Superintendencia de Banca, Seguros y AFP), Auditoría Interna y la Sociedad de Auditoría Externa.
- ❖ El incumplimiento de las obligaciones que asume el proveedor en las cláusulas referidas, constituye causal de resolución automática y de pleno derecho del presente contrato, de conformidad con lo previsto en el artículo 1430° del Código Civil, sin perjuicio de la obligación del proveedor de pagar al Banco la indemnización correspondiente.
- ❖ En caso el Banco incurriera en costos y/o multas establecidas por parte de un organismo regulador u otro, mediante una resolución o sentencia firme producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables a el Proveedor, éste se hará totalmente responsable de dichas penalidades, asumiendo el importe de las mismas sin reserva ni limitación alguna. Por lo que EL BANCO, podrá evaluar la aplicación de penalidades o el pago de indemnización:

## LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

### SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El PROVEEDOR declara conocer que está obligado a garantizar la integridad, disponibilidad, confidencialidad y privacidad de la información de El BANCO que involucra el servicio provisto; por lo que El PROVEEDOR debe cumplir con los lineamientos de seguridad de la información y ciberseguridad aplicables al servicio contratado, establecidos en las siguientes normativas:

- ✓ **Resolución SBS N°504-2021 “Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad”, según los siguientes aspectos:**

- En atención al Artículo 22. Servicios provistos por terceros:

El PROVEEDOR se obliga a adoptar las medidas necesarias para que sus trabajadores, representantes y terceros que intervienen en el servicio contratado, cumplan con las disposiciones relacionadas a la seguridad de información y ciberseguridad establecidas en la normativa interna del Banco.

El PROVEEDOR es el responsable del resguardo y protección de los activos de información (equipos, dispositivos informáticos, aplicaciones, información, entre otros) de propiedad del Banco involucrados en el servicio contratado, que se encuentren bajo la administración del PROVEEDOR o formen parte de dicho servicio.

El PROVEEDOR permitirá, facilitará y/u otorgará a EL BANCO, la revisión del cumplimiento de las medidas de seguridad de la información y ciberseguridad relacionadas al servicio contratado.

El PROVEEDOR debe documentar las especificaciones técnicas de las API para la provisión del servicio, de forma que facilite su auditoría y su uso, dichos documentos deben ser proporcionados al Banco, considerando las siguientes medidas:

- a) Contar con mecanismos para la autenticación mutua de los sistemas con los que se interconecta o utiliza las API.
- b) Utilizar buenas prácticas de desarrollo seguro de las API y revisar periódicamente su codificación.

El PROVEEDOR declara que tiene pleno conocimiento que EL BANCO se encuentra sujeto a las exigencias de la Resolución SBS N°504-2021 "Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad"; por lo que EL PROVEEDOR se compromete a implementar en sus sistemas de información los requerimientos de seguridad sobre el uso de APIs para la provisión de servicios en línea y las responsabilidades respecto a las medidas de seguridad que debe mantener en la provisión del servicio; los cuales deben ser coordinados con el Banco.

El PROVEEDOR, previo a la puesta en producción del servicio contratado, debe evidenciar que cuenta con las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes relevantes al servicio contratado y posterior a la puesta en producción del servicio, debe evidenciar anualmente la vigencia de dichas certificaciones. El PROVEEDOR debe proporcionar al BN, copia o indicar el enlace web donde se visualicen las referidas certificaciones.

✓ **Norma Técnica Peruana NTP-ISO/IEC 27001-2022 "Seguridad de la Información, Ciberseguridad y Protección de la Privacidad", según los siguientes aspectos:**

- En atención al numeral 5.19 Seguridad de la información en las relaciones con los proveedores

El PROVEEDOR debe contar con un proceso de gestión de riesgos, alertas e incidentes de seguridad de la información, relacionados con el servicio contratado. Las evidencias de la existencia y ejecución de dicho proceso deben ser remitido al inicio del servicio o a solicitud del Banco.

El PROVEEDOR se obliga a cumplir con los controles de seguridad de la información y ciberseguridad establecidos por el Banco, respecto al control de los accesos, cifrado de la información, la revisión del desempeño, el seguimiento de la ejecución del servicio, presentación de informes y auditorías, así como las obligaciones regulatorias enmarcadas en los requisitos de seguridad de la información.

El PROVEEDOR debe contar con las medidas apropiadas para garantizar la seguridad en el procesamiento, almacenamiento, transmisión, autenticación, trazabilidad y adaptabilidad de la información del BN que se utilice en el servicio contratado.

**CONFIDENCIALIDAD DE LA INFORMACIÓN**

- EL BANCO es propietaria de toda la información confidencial que, por razones del alcance del presente contrato, entregue a EL PROVEEDOR.
- El PROVEEDOR se compromete a mantener la confidencialidad y reserva absoluta y no revelar a terceros, sin previa autorización escrita del Banco, toda información a la que tenga acceso, que le sea suministrada o conozca directa o indirectamente durante la ejecución del servicio contratado.
- El compromiso de confidencialidad se prolonga hasta por 10 años después de terminado el servicio y se hace extensivo al personal de EL PROVEEDOR aun cuando hayan dejado de tener vínculo laboral con EL PROVEEDOR.
- Para los efectos del presente acuerdo, se entenderá como "Información Confidencial" toda aquella información comercial, financiera, técnica, de inteligencia comercial, metodologías, procesos, políticas, procedimientos, estándares, estrategias,

productos, bases de datos, matrices y programas de cómputo, códigos, claves, nombres y/o experiencia de empleados y consultores, propiedad intelectual, fórmulas, negocios, lista de clientes, estados financieros, información sobre productos de software y hardware de EL BANCO, que sea entregada a EL PROVEEDOR, ya sea de manera escrita, oral, visual y/o digital; que por sus características le signifique a EL PROVEEDOR obtener y mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas.

- En caso el Banco otorgue información confidencial, para ser utilizada y custodiada por EL PROVEEDOR para la provisión del servicio contratado, deberá ser devuelta a EL BANCO en un plazo no mayor a diez (10) días calendarios, así como la eliminación de la información ante la culminación del servicio.
- EL PROVEEDOR está autorizado para que su personal pueda hacer uso de la información confidencial provista por EL BANCO siempre que dicho personal esté directamente relacionado a la ejecución del presente contrato, haya sido informado de la naturaleza confidencial del mismo y haya sido instruido sobre las medidas de protección adoptadas por EL PROVEEDOR, las cuales deberá aplicar para la protección de la confidencialidad de esta. EL PROVEEDOR será responsable por las infracciones comprobadas de incumplimiento del acuerdo de confidencialidad que hayan sido cometidas por el personal asignado para la ejecución del servicio objeto del presente Contrato.
- El PROVEEDOR no debe capturar, utilizar, almacenar, acceder, visualizar ni desviar la información de los clientes y usuarios de El BANCO, sin la autorización expresa de El BANCO.
- Los aplicativos, sistemas, softwares e información que EL PROVEEDOR desarrolle en el marco del servicio que el Banco contrata es de titularidad del Banco por lo tanto EL PROVEEDOR no podrá asumir ningún derecho, de ningún tipo, sobre la creación o desarrollo. La divulgación de la creación o desarrollo no implica el licenciamiento de derecho de patentes o derecho de autor o ningún otro derecho por parte de EL PROVEEDOR, que no sean los establecidos en el contrato.
- El PROVEEDOR declara conocer que la vulneración y/o divulgación de secretos empresariales se encuentra tipificada como delito en conformidad con lo estipulado en el Código Penal.
- El proveedor debe reportar cualquier incidente de seguridad que implique la exposición, alteración o pérdida de datos de clientes e implementar procedimientos para identificar y reportar incidentes de seguridad de este tipo. Se debe considerar que el Banco debe reportar a la Autoridad Nacional de Protección de Datos Personales este tipo de incidentes en un máximo de 48 horas de ocurrido

**PROTECCIÓN DEL SECRETO BANCARIO, DATOS PERSONALES, DELITOS INFORMATICOS, REGLAMENTO DE TARJETAS DE CREDITO Y DEBITO Y ESTANDAR PCI DSS:**

- El PROVEEDOR declara conocer que está obligado a salvaguardar y mantener la confidencialidad del secreto bancario, de los datos personales de los usuarios y clientes del Banco de la Nación, de acuerdo con la Constitución Política del Perú, Ley N°29733 Ley de Protección de datos personales, su Reglamento y Directivas de Seguridad, Ley N°26702, Secreto Bancario, sus modificatorias y actualizaciones; aplicables al servicio asociado al contrato.
- EL PROVEEDOR declara conocer las sanciones tipificadas en la Ley N° 30096, Ley de Delitos Informáticos (integridad de datos informáticos, tráfico ilegal de datos, interceptación de datos informáticos), y la Ley N° 30171 que modifica la Ley 30096, Ley de Delitos Informáticos, bajo la cual se obliga a dar estricto cumplimiento de estas disposiciones.

- EL PROVEEDOR se somete a las disposiciones previstas de la Resolución S.B.S. N.º 6523 -2013 Reglamento de Tarjetas de Crédito y Débito - Art. 18º Medidas en Materia de Seguridad de la Información, aplicables al servicio, bajo la cual se obliga a dar estricto cumplimiento.
- EL PROVEEDOR declara conocer que asume la condición de responsable de la seguridad de los datos de las tarjetas de pago que posee o almacena, procesa o transmite en el marco del presente contrato, o en la medida en que puedan afectar a la seguridad del entorno de datos de tarjetas de pago de EL BANCO.
- EL PROVEEDOR se obliga a adoptar las disposiciones para la protección de los datos del titular de la tarjeta y medidas sólidas de control de acceso previstas por EL BANCO relacionadas al Estándar de Seguridad de Datos de Payment Card Industry - PCI DSS, bajo la cual deberá dar estricto cumplimiento.
- EL PROVEEDOR en caso corresponda, acepta y reconoce la responsabilidad del cumplimiento de las medidas de seguridad de datos de las tarjetas de pago de los servicios que EL PROVEEDOR, a su vez, contrata con terceros (contratación en cadena) para lograr el cumplimiento general del servicio en el marco del presente contrato.

#### LINEAMIENTOS DE CONTINUIDAD DEL NEGOCIO

EL PROVEEDOR debe desarrollar la gestión de continuidad para el servicio objeto del contrato mediante la aplicación de la Resolución S.B.S N° 877-2020 Reglamento para la gestión de la continuidad del negocio o buenas prácticas para en la Gestión de Continuidad del Negocio (ISO 22301) para este tipo de servicio.

EL PROVEEDOR se compromete a mantener la continuidad del servicio contratado por EL BANCO; para lo cual, debe contar con procedimientos documentados que permitan responder, recuperar, reanudar y restaurar el servicio objeto del contrato; además, los referidos procedimientos deben formar parte de un Plan de Recuperación de Tecnología de Información o en su defecto de un Plan de Continuidad de Negocio, de tal modo que su ejecución asegure la alta disponibilidad y recuperación del servicio conforme al tiempo objetivo de recuperación requerido en el **numeral 9.1**.

EL PROVEEDOR debe entregar a EL BANCO: el Plan de Recuperación de Tecnología de Información y/o Plan de Continuidad de Negocio, los cuales deben estar actualizados y probados cuando menos una vez al año; asimismo, EL PROVEEDOR deberá contar con un Programa de Pruebas anuales que permitan verificar el cumplimiento de los procedimientos de recuperación documentados. Al respecto, EL PROVEEDOR deberá remitir cada primer trimestre del año el Plan(es) y Programa de Pruebas, y concluido el año y ante requerimiento de EL BANCO deberá remitir los informes de pruebas que indiquen los resultados alcanzados.

EL PROVEEDOR podrá programar pruebas en horarios de madrugada a fin de reducir la afectación del servicio; para casos de pruebas que implique la interrupción del servicio, estas deben ser identificadas y coordinadas con EL BANCO previo a su ejecución. Dichas pruebas deben contemplar la validación de alta disponibilidad de los componentes tecnológicos que soportan el servicio contratado, ante una interrupción. Asimismo, EL BANCO podrá solicitar, por correo y/o por carta, su participación en el desarrollo de dichas pruebas (con cinco (05) días hábiles de anticipación) y, de tener alguna observación sobre los resultados podrá remitir a EL PROVEEDOR para que subsane la(s) observación(es) y/o No Conformidad(es) y EL PROVEEDOR comunique las acciones realizadas en un periodo no mayor a veinte (20) días calendarios.

Asimismo, para casos de pruebas que el Banco de la Nación requiera realizar esta será coordinada con el Proveedor, y podría realizarse una vez al año.

Ante la eventual interrupción del servicio objeto del contrato; por causales imputables a EL PROVEEDOR, siempre que dicha interrupción sea por un tiempo mayor a 1 hora; EL PROVEEDOR deberá comunicar a EL BANCO de forma inmediata, o máximo cuatro horas después del incidente que origino la interrupción, comunicación que debe incluir la hora de inicio y fin (en caso que el incidente se encuentre superado) y posteriormente deberá remitir un informe de la incidencia, la cual debe contener como mínimo la fecha, hora, duración, causa/origen, responsabilidad, estado de los servicio(s) afectado(s), descripción del incidente, acciones de recuperación realizadas ,diagnostico general, impacto del servicio, acción de mejora y recomendaciones, conclusiones, en un plazo máximo de tres (03) días hábiles, para su reporte se contabiliza a partir de la ocurrencia del evento. En caso de que no se haya concluido las acciones de superen o implementen las recomendaciones estas deberán reportarse hasta que se encuentre superada.

Para casos que EL PROVEEDOR realice cambios a sus configuraciones u otros componentes que involucren/afecten la operatividad del servicio objeto del contrato, deben ser comunicados a EL BANCO con siete (07) días calendarios de anticipación a la Gerencia de Tecnología de la Información.

Lo antes mencionado puede ser sustentado con él envió de un Certificado ISO 22301 que se encuentre vigente, de requerir información adicional (referidos a los planes, cronograma de pruebas e informes de las pruebas) EL BANCO podrá solicitar a EL PROVEEDOR información en el cumplimiento de la cláusula de continuidad del negocio.

### **GESTIÓN DE RIESGOS OPERATIVOS**

El proveedor debe aplicar las medidas de control para la gestión de los riesgos operacionales, que sean aplicables al servicio contratado por el Banco; que permita identificar, evaluar, tratar, controlar y monitorear los diversos riesgos asociados a dicho servicio, siendo responsable frente al Banco en caso de la materialización de algún riesgo operativo que, en el marco de la prestación del servicio, afecte al Banco y/o sus clientes.

### **23. DOCUMENTOS A PRESENTARSE A LA SUSCRIPCION DEL CONTRATO**

El ganador de la Buena Pro en concordancia a condiciones establecidas en los términos de referencia, a la suscripción del contrato deberá presentar la siguiente documentación:

- a) Garantía Financiera (carta fianza) de fiel cumplimiento de contrato, acorde a lo precisado en el numeral 20 de los presentes Términos de Referencia.
- b) Póliza Tech E&O con las características y condiciones establecidas en el numeral 21 de los presentes Términos de referencia.
- c) Declaración Jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo y su Reglamento, acorde a lo precisado en el numeral 25 de los presentes Términos de Referencia.
- d) Documentación exigida en el numeral 26. Prevención del Lavado de Activos y del Financiamiento del Terrorismo.
- e) Documentación exigida en el numeral 27. Registro de Deudores de Reparación Civil - REDERECI.

### **24. REQUISITOS DE CALIFICACIÓN**

<b>A.</b>	<b>CAPACIDAD LEGAL</b>
	<b>HABILITACION</b>
	<p><b><u>Requisitos:</u></b></p> <p>El postor debe acreditar la certificación vigente como PCI DSS.</p>

	<p><b><u>Acreditación:</u></b></p> <p>Copia de la Certificación vigente como PCI DSS.</p>
<b>B.</b>	<b>CAPACIDAD TÉCNICA Y PROFESIONAL DEL PERSONAL CLAVE</b>
<b>B.1</b>	<b>FORMACIÓN ACADÉMICA</b>
	<p><b><u>Requisitos:</u></b></p> <ul style="list-style-type: none"> <li>• <b>Jefe del Proyecto</b></li> </ul> <p>Mínimo Título universitario en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial o carreras afines a Tecnología de la Información (*).</p> <ul style="list-style-type: none"> <li>• <b>Ingeniero de Integración y Seguridad</b></li> </ul> <p>Mínimo grado de bachiller en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial o carreras afines a Tecnología de la Información (*).</p> <ul style="list-style-type: none"> <li>• <b>Ingeniero de Soporte de Componentes de Software</b></li> </ul> <p>Mínimo grado de bachiller en Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería Industrial o carreras afines a Tecnología de la Información (*).</p> <p>(*):El párrafo "o carrera, afines a tecnología de la información" se refiere a cualquiera de las carreras listadas a continuación: Ingeniería de Sistemas, Ingeniería Informática, Ingeniería Industrial, Ingeniería Electrónica, Ingeniería de Computación y Sistemas, Ingeniería de Telecomunicaciones, Ingeniería Industrial y de Sistemas, Ingeniería de Sistemas e Informática, Ingeniería de Sistemas Empresariales, Ingeniería de Software , Ingeniería de Sistemas de Información, Ingeniería de Telecomunicaciones y Redes, Ingeniería de Computación y de Sistemas, Ingeniería Informática y de Sistemas, Ingeniería de Redes y Comunicaciones, Ingeniería de Seguridad Informática, Ingeniería Empresarial y de Sistemas, Ingeniería de Estadística e Informática; Ingeniería de Sistemas y Cómputo, Ingeniería de Sistemas e Informática, Ingeniería Empresarial, Computación e Informática, Ingeniería de Computación, Licenciado (a) en Computación, Ingeniería de Sistemas y Computación, Ciencias de la Computación, Ciencias de la Información, Licenciado (a) Administración y Sistemas.</p> <p><b><u>Acreditación:</u></b></p> <p>El título profesional o grado académico será verificado por el comité del concurso de méritos en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <a href="https://enlinea.sunedu.gob.pe/">https://enlinea.sunedu.gob.pe/</a> // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <a href="http://www.titulosinstitutos.pe/">http://www.titulosinstitutos.pe/</a>, según corresponda.</p> <p>El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado requerido.</p> <p>En caso de que el título profesional o grado académico de bachiller no se encuentre inscrito</p>

	<p>en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p> <p>Para el caso de títulos profesionales o grados académicos obtenidos fuera del territorio peruano, estos deberán estar legalizados ante el Consulado Peruano en el país de origen. En adición, si estos documentos se presentan en otro idioma que no sea el español, los mismos deberán contar con traducción juramentada o traducción simple.</p>
<b>B.2</b>	<b>EXPERIENCIA DEL PERSONAL CLAVE</b>
	<p><b><u>Requisitos:</u></b></p> <ul style="list-style-type: none"> <li>• <b>Jefe del Proyecto</b>  Mínimo cinco (05) años de experiencia como Gerente de Proyectos, Jefe de Proyectos, Administrador de Proyectos, en implementaciones relacionadas al servicio de generación y validación de CVV2 dinámico o similares que tengan que ver con la implementación de mecanismos de seguridad para reforzar seguridad en operaciones con tarjeta NO presente en las redes de pago.</li> <li>• <b>Ingeniero de Integración y Seguridad</b>  Mínimo tres (03) años de experiencia en la ejecución de tareas de integración, conectividad de redes y configuraciones de seguridad, como parte de proyectos relacionados a la implementación de servicio de generación y validación de CVV2 dinámico o similares que tengan que ver con la implementación de mecanismos de seguridad para reforzar seguridad en operaciones con tarjeta NO presente en las redes de pago.</li> <li>• <b>Ingeniero de Soporte de Componentes de Software</b>  Mínimo tres (03) años de experiencia en la ejecución de tareas de integración de componentes de software (SDK, APIs, tramas ISO8583), como parte de proyectos relacionados a la implementación de servicio de generación y validación de CVV2 dinámico o similares que tengan que ver con la implementación de mecanismos de seguridad para reforzar seguridad en operaciones con tarjeta NO presente en las redes de pago.</li> </ul> <p><b><u>Acreditación:</u></b></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p>
<b>C.</b>	<b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b>
	<p><b><u>Requisitos:</u></b></p> <p>a) El postor debe acreditar un monto facturado acumulado equivalente a S/ 250,000.00 (Doscientos cincuenta mil con 00/100 Soles), por la contratación de servicios del objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de propuestas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. El proveedor podrá sustentar este monto facturado presentando documentación que certifique pagos por la contratación del</p>





servicio de generación y validación de CVV2 dinámico.

- b) El postor debe acreditar mínimo un (01) servicio de implementación del objeto de la contratación, efectuados en entidades bancarias del sistema financiero peruano que cuenten con calificación de riesgo mínimo "A" o en bancos de países latinoamericanos con calificación de riesgo "Grado de Inversión". En ambos casos la clasificación debe haber sido otorgada por entidades clasificadoras de riesgo de prestigio internacional (como Standard & Poors, Grupo Moody's o Fitch Ratings). El proveedor podrá efectivizar esta acreditación presentando documentación que certifique implementaciones del servicio de generación y validación del CVV dinámico

**Acreditación:**

- a) Se acreditará con copia simple de (i) contratos u órdenes de servicios, 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, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el correspondiente.

Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo correspondiente, referido a la Experiencia del Postor en la Especialidad.

- b) Se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación y. (ii) Copia del documento emitido por entidad clasificadora de riesgo que establezca la Clasificación otorgada a la entidad bancaria que contrató el servicio del proveedor.

**25. SEGURIDAD Y SALUD EN EL TRABAJO**

El ganador de la buena pro, a la suscripción del contrato deberá presentar obligatoriamente una declaración jurada que cumple las disposiciones establecidas en la Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo y su Reglamento.

**26. PREVENCIÓN DEL LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO**

El postor declara conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015 – Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, que tiene implementado un sistema de prevención de LA/FT con componentes de cumplimiento y de gestión de riesgos de LA/FT. Por tanto, el postor se obliga a respetar la mencionada norma, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia.

Como parte de la gestión del Riesgo de Lavado de Activos y Financiamiento del Terrorismo, EL BANCO no se vincula con personas (ya sea con personas naturales como tal o estas en calidad de representantes de personas jurídicas privadas o de Entidades con personería jurídica de derecho público), respecto de las cuales se les haya atribuido, en sede judicial, responsabilidad por delitos precedentes de lavado de activos y financiamiento del terrorismo. Para tales efectos, EL BANCO, conforme a la Resolución SBS N° 2660-2015, aplica procedimientos de debida diligencia en el conocimiento de sus proveedores.

El ganador de la buena pro, deberá presentar una Declaración Jurada de conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015 - Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo; asimismo, para la suscripción del contrato deberá presentar la siguiente información:

- Nombres y Apellidos completos o denominación o razón social, en caso se trate de una persona jurídica.
- Registro Único de Contribuyentes (RUC), o registro equivalente para no domiciliados, de ser el caso.
- Tipo u número de documento de Identidad, en caso de trate de una persona natural.
- Dirección de la oficina o local principal.
- Años de Experiencia en el mercado.
- Rubros en los que el proveedor brinda sus productos o servicios.
- Identificación de los accionistas, socios o asociados que tengan directa o indirectamente el 25 % del capital social, aporte o participación de la persona jurídica y del nombre del representante legal, considerando la información requerida para las personas naturales.
- Declaración Jurada de no contar con antecedentes penales del proveedor, de ser el caso.

El ganador de la buena pro se compromete a actualizar la información en forma periódica, cada 02 años, y en caso no haya modificación de la información, deberá dejarse constancia de ello. Sin perjuicio de lo anterior debe comunicar a EL BANCO cualquier modificación de la información declarada.

La información a la que tiene acceso el ganador de la buena pro sólo podrá ser utilizada, para los fines señalados en el presente contrato, de modo tal, que se obliga a guardar estricta y severa reserva de la información a la que tiene acceso.

## 27. REGISTRO DE DEUDORES DE REPARACIÓN CIVIL - REDERECI

El Proveedor no deberá encontrarse en el Registro de Deudores de Reparaciones Civiles (REDERECI). EL BANCO realizará la verificación de dicho requisito para la suscripción del Documento Contractual.

## ANEXO 1

### NORMATIVA INTERNA

- a) Manual de políticas del sistema gestión de seguridad de la información
- b) Lineamientos de seguridad de la información para la adquisición, desarrollo y mantenimiento de los sistemas de información
- c) Ciclo de vida del software
- d) Lineamientos de seguridad para la operación de los sistemas de información
- e) Parámetros de acceso de los sistemas de información, servicios informáticos y plataformas tecnológicas
- f) Gestión de accesos e identidades a los sistemas de información, servicios informáticos y plataformas tecnológicas
- g) Gestión de cuentas principales y de integración de los sistemas de información, servicios informáticos y plataformas tecnológicas
- h) Seguridad de la información en canales digitales del banco de la nación
- i) Privacidad y confidencialidad de la información del banco de la nación
- j) Lineamientos de seguridad de la información para el uso de los sistemas, servicios y dispositivos informáticos del banco de la nación
- k) Lineamientos de seguridad para el cifrado de la información
- l) Gestión de incidentes de seguridad de información
- m) Manual de políticas de protección de datos personales
- n) Lineamientos de seguridad de la información para el uso de servicios tecnológicos en la nube Lineamientos de seguridad de información para la protección de datos de tarjetas de crédito y débito del BN

## Anexo N° 2

### PROYECTO DE CONTRATO

#### Importante

*Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, previo acuerdo de partes.*

### **CONTRATO DEL SERVICIO FINANCIERO "SERVICIO DE IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD EN TRANSACCIONES CON TARJETA BN (DE CRÉDITO Y DÉBITO) NO PRESENTE"**

Conste por el presente documento, la Contratación del "Servicio Financiero de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente", que celebra de una parte EL BANCO DE LA NACIÓN", en adelante "EL BANCO", con RUC N° 20100030595, con domicilio legal Av. Javier Prado Este N° 2499 - San Borja, representada por [...], identificado con DNI N° [...] y por [...], identificado con DNI N° [...], ambos con poderes inscritos en la Partida Electrónica N° 11013341 del Registro de Personas Jurídicas de la Oficina Registral de Lima, a quien en adelante se le denominará "EL BANCO" y de otra parte [...], con RUC No. [...] con domicilio en [...], debidamente representado por [...], identificado(a) con DNI N° [...], según poderes inscritos en la Partida Electrónica [...] del Registro de Personas Jurídicas de Lima, a quien en adelante se le denominará EL PROVEEDOR o EL CONTRATISTA en los términos y condiciones siguientes:

#### **CLÁUSULA PRIMERA: ANTECEDENTES**

[...] (EL PROVEEDOR) es [...].

EL BANCO es una empresa con potestades públicas, integrante del Sector Economía y Finanzas, que opera con autonomía económica, financiera y administrativa, el cual se rige por su Estatuto, aprobado por Decreto Supremo N°07-94-EF, por el Decreto Legislativo N° 1693, que ordena, sistematiza y optimiza la eficiencia de la actividad empresarial del Estado y fortalece la estructura y gestión del FONAFE y su Reglamento aprobado por Decreto Supremo N° 292-2024-EF, y el artículo 33° de la Ley N° 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, y supletoriamente por los demás artículos de dicha Ley General o sus modificatorias..

Mediante Resolución SBS N° 2286-2024, se modifica, entre otros, la Resolución SBS N° 6523-2013, "Reglamento de Tarjetas de Crédito y Débito" con la finalidad, conforme a la parte considerativa de aquella Resolución, de modificar el marco normativo considerando el actual funcionamiento de los productos y/o servicios ofrecidos por las empresas del sistema financiero a los usuarios, entre ellas, EL BANCO, así como el impacto del uso de las nuevas tecnologías, y por lo tanto resulta necesario precisar la responsabilidad de las empresas en los procedimientos de validación de identidad de los usuarios y la obtención del consentimiento al momento de realizar operaciones, ante casos de operaciones no reconocidas y de aquellas que fueron procesadas sin requerir autenticación reforzada, esto es, implementar mecanismos para la validación de la identidad y la obtención del consentimiento desde el momento de la contratación así como durante su ejecución. Es así como, mediante la citada Resolución SBS N° 2286-2024, se incorpora la definición de Operaciones con tarjeta no presente que son cuando el instrumento de pago no interactúa con el dispositivo de captura de la información.

De conformidad con lo establecido en el literal a) del artículo 7° de la Ley N°32069 - Ley General de Contrataciones Públicas, así como lo señalado por la Ley N° 26702 - Ley General del Sistema

Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP, sobre el término "servicio financiero" incluido en el Anexo - Glosario, el presente es un contrato de naturaleza bancaria y/o financiera, por lo que se encuentra fuera del ámbito de aplicación de la normativa de Contrataciones del Estado.

En el marco del Concurso de Méritos N° 0004-2026-BN, EL PROVEEDOR presentó su propuesta de Servicios mediante ....., adjuntando la propuesta Económica y la Propuesta Técnica, las cuales forman parte integrante del presente CONTRATO como Anexo N° 002. En caso de discrepancia entre este Anexo N° 002 con el presente CONTRATO y sus Términos de referencia (Anexo N° 001), prevalecerán estos últimos sobre aquel.

**CLÁUSULA SEGUNDA: OBJETO**

El presente contrato, en adelante, EL CONTRATO, tiene como objeto que EL PROVEEDOR brinde a EL BANCO el Servicio de Financiero de implementación de mecanismos de seguridad en transacciones con tarjeta BN (de crédito y débito) no presente, mediante la implementación del CVV2 Dinámico como segundo factor de autenticación durante la realización de operaciones con tarjeta no presente, dando cumplimiento a lo dispuesto en la citada Resolución SBS N° 2286-2024, en adelante, EL SERVICIO:

Servicio	Componentes
Generación y Validación de CVV2 Dinámico	Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de débito Visa
	Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para tarjetas de crédito Mastercard
	Servicio de generación y validación de CVV2/CVC2 Dinámico
Soporte Técnico	Soporte Técnico, de acuerdo con lo descrito en el numeral 7.2 de los términos de referencia (Anexo N° 001 de EL CONTRATO)

EL PROVEEDOR declara conocer y aceptar que, al implementar los componentes transaccionales de EL SERVICIO, deberá tener en cuenta que EL BANCO autoriza y procesa por sí mismo las operaciones de su tarjeta de débito Visa y se vale de un tercero (la empresa Izipay) para autorizar y procesar las operaciones de su tarjeta de crédito Mastercard, por lo que EL PROVEEDOR debe cumplir con los estándares de seguridad de las redes de pago (Visa y Mastercard) para la generación y validación del CVV2 Dinámico.

EL PROVEEDOR declara conocer que la contratación de EL SERVICIO tiene como objetivos los siguientes:

- Reforzar la seguridad durante la realización de operaciones con tarjeta NO presente en las redes de pago Visa y Mastercard, cumpliendo así con las disposiciones dadas por la SBS (Superintendencia de Banca, Seguros y AFP) respecto a estos temas.
- Reducir el riesgo de pérdidas para EL BANCO a causa de reclamos de clientes por el reconocimiento de operaciones con tarjeta NO presente en comercios que no participan de 3DS.

Los alcances y descripción de EL SERVICIO se encuentran descritos en el numeral 7 de los Términos de Referencia - TDR que, como Anexo N° 001 forma parte integrante de EL CONTRATO, cuyas condiciones y términos EL PROVEEDOR se obliga a cumplir en su integridad.

Del mismo modo, las características de la solución tecnológica requerida por EL BANCO que deberá observar EL PROVEEDOR se encuentran descritas en el numeral 8 de los Términos de

Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

Referencia (Anexo N° 001), lo cual EL PROVEEDOR se obliga a cumplir en su integridad.

**CLÁUSULA TERCERA: MONTO CONTRACTUAL**

El monto total del presente CONTRATO es conforme al siguiente detalle:

CONCEPTO	PRECIO TOTAL EN SOLES (S/)
Por la Implementación de EL SERVICIO (pago único) <ul style="list-style-type: none"> <li>- Implementación/Configuración del servicio de Generación y Validación de CVV2 Dinámico para Tarjetas de Débito Visa;</li> <li>- Implementación/Configuración del servicio de Generación y Validación de CVC2 Dinámico para Tarjetas de Crédito Mastercard</li> </ul>	
Por Servicios Transaccionales (pagos mensuales) <ul style="list-style-type: none"> <li>- COSTO POR LAS ATENCIONES DE LOS COMPONENTES TRANSACCIONALES DEL SERVICIO</li> <li>- COSTO POR SERVICIO DE SOPORTE TÉCNICO</li> </ul>	
<b>TOTAL (S/)</b>	

Este monto comprende el costo del SERVICIO, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución del SERVICIO materia del presente CONTRATO.

**CLÁUSULA CUARTA: DEL LUGAR Y PRESTACIÓN DEL SERVICIO, DEL PAGO Y DE LA GARANTÍA**

EL BANCO se obliga a pagar la contraprestación del SERVICIO a EL PROVEEDOR en moneda Soles (S/), previa conformidad de la prestación, y de acuerdo al siguiente detalle:

1. Por el Servicio de implementación. Se efectuará en pago único por cada servicio de implementación de los siguientes componentes transaccionales, debiendo EL PROVEEDOR cumplir con los plazos siguientes:

Componentes del Servicio de Implementación	Plazos de Implementación
Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de débito Visa	8 meses calendarios
Implementación/configuración del servicio de generación y validación de CVC2 Dinámico para tarjetas de crédito Mastercard	8 meses calendarios

- Dichos plazos inician a las dos semanas (14 días calendario) desde la firma de EL CONTRATO. Dentro de dicho periodo, LAS PARTES elaborarán un Plan de Trabajo conjunto, el cual formará parte integrante de EL CONTRATO, y considerará para su elaboración los lineamientos establecidos en la metodología del Ciclo de Vida del Software de EL BANCO.

2. Por Servicios Transaccionales. Se efectuará en pagos mensuales por un periodo de treinta y seis (36) meses, dependiente del número de PAN activos en la plataforma de EL PROVEEDOR en el periodo facturado, bajo las consideraciones que se establecen en el literal b) del numeral 15 de los Términos de Referencia (Anexo N° 001). El Soporte Técnico será prestado por EL PROVEEDOR en forma paralela a la prestación de los servicios transaccionales, por un periodo de treinta y seis (36) meses, mediante armadas (pagos) mensuales iguales. Los Servicios Transaccionales y de soporte técnico iniciarán una vez concluido el servicio de implementación en el ambiente de producción de uno de los 2 componentes transaccionales que se describen en el numeral precedente de la presente cláusula (independientemente de cuál de los dos sea).

La prestación del SERVICIO se realizará de forma remota (no presencial), y las coordinaciones para la ejecución del CONTRATO se realizarán con la Sección Canales Virtuales de la Subgerencia Canales Alternos de la Gerencia Banca Digital del BANCO.

Para efectos del pago de las contraprestaciones ejecutadas por EL PROVEEDOR, deberá presentar a EL BANCO la documentación que se detalla en los Términos de Referencia (Anexo N° 001) que resulta aplicable por cada componente que aplica a EL SERVICIO.

#### **Plazo para el Pago**

EL BANCO pagará las contraprestaciones pactadas a favor de EL PROVEEDOR dentro de los quince (15) días calendario siguiente a la conformidad del SERVICIO, siempre que se verifiquen que la documentación presentada por EL PROVEEDOR este completa y conforme con las condiciones establecidas en EL CONTRATO y Términos de Referencia (Anexo N° 001) para ello.

De existir observaciones, EL BANCO las comunica a EL PROVEEDOR, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de cinco (05) días calendario. Si pese al plazo otorgado, EL PROVEEDOR no cumpliera a cabalidad con la subsanación, corresponde aplicar la penalidad por mora (por incumplimiento en los plazos) desde el vencimiento del plazo para subsanar. Este procedimiento no resulta aplicable cuando EL SERVICIO manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso EL BANCO no otorga la conformidad, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

La emisión de conformidad por parte de EL BANCO no convalida los defectos o vicios ocultos que no sean posibles advertir al momento de su revisión y/o certificación por parte de EL BANCO, estando facultado EL BANCO para aplicar penalidades incluso sobre conformidades ya emitidas, siempre que se verifique el incumplimiento por parte de EL PROVEEDOR.

#### **Garantía Comercial**

EL PROVEEDOR deberá brindar como parte de EL SERVICIO un periodo de garantía por cada SERVICIO brindado, con las siguientes características:

- Alcance de la garantía:

Contra defectos de diseño y/o desarrollo del software, disponibilidad o fallas de funcionamiento de los componentes alojados en la nube, entre otros supuestos ajenos al uso normal o habitual del SERVICIO y no detectables al momento que EL BANCO otorgó la conformidad.

Para el periodo de garantía, los recursos asignados por EL PROVEEDOR deben ser totalmente independientes a los recursos asignados a los servicios de soporte y mejoras continuas.

Se considerarán como garantía todos los errores detectados durante la operación en

producción, los cuales hayan sido originados por fallas en la etapa de construcción respecto de las definiciones realizadas, aun cuando estos procesos hayan sido aprobados por EL BANCO en etapa de pruebas integrales.

- Período de garantía: Un periodo de garantía de doce (12) meses, que rige después de la puesta en producción del último componente transaccional del SERVICIO (CVV2 Dinámico para tarjetas de débito y crédito).

#### **CLÁUSULA QUINTA: VIGENCIA DEL CONTRATO**

El plazo de EL CONTRATO será por un periodo de cuarenta y cuatro (44) meses y dos semanas, el cual rige desde la fecha de su firma, el mismo que podrá ser renovado antes de su vencimiento por 36 meses (sobre los servicios transaccionales) mediante la suscripción de una adenda. Sin perjuicio de ello, cualquiera de LAS PARTES podrá resolver EL CONTRATO de forma unilateral sin expresión de causa, comunicándolo por escrito a su contraparte con al menos un (1) año de anticipación antes del vencimiento del plazo contractual en curso.

En las dos semanas iniciales de la vigencia de EL CONTRATO, se elaborará en forma conjunta (entre LAS PARTES) el detalle del plan de trabajo a ejecutar para implementar en paralelo los dos componentes transaccionales del SERVICIO, con las actividades e hitos que se deben cumplir para la puesta en producción del SERVICIO. El plan de trabajo formará parte de EL CONTRATO y será firmado por LAS PARTES, debiendo considerar para su elaboración los lineamientos establecidos en la metodología del Ciclo de Vida del Software del BANCO. Posterior a ello, EL PROVEEDOR deberá cumplir con los plazos establecidos para el servicio de implementación y servicios transaccionales que se describen en la cláusula cuarta de EL CONTRATO y en los Términos de Referencia (Anexo N° 001).

#### **CLÁUSULA SEXTA. - OBLIGACIONES DE EL PROVEEDOR**

EL PROVEEDOR se compromete a cumplir con las obligaciones, responsabilidades y condiciones de EL SERVICIO contratado, de acuerdo con las reglas de la buena fe y común intención de LAS PARTES, conduciéndose con honestidad y responsabilidad; y de manera general a cumplir con las siguientes obligaciones:

- 6.1. Ejecutar EL SERVICIO en la forma y oportunidad establecidos en EL CONTRATO y los Términos de Referencia (**ANEXO N° 001**).
- 6.2. Cumplir con las obligaciones y responsabilidades establecidos en los Términos de Referencia - TDR (**ANEXO N° 001**).
- 6.3. Presentar y suscribir el Plan de Trabajo, dentro en la forma y plazo establecido en los Términos de Referencia (**ANEXO N° 001**).
- 6.4. Presentar, a la firma de EL CONTRATO, una garantía de fiel cumplimiento (carta fianza) emitida a favor de EL BANCO por una suma equivalente al 10% del monto total contractual pactado, la cual deberá mantenerse vigente hasta la última conformidad otorgada por EL BANCO por la prestación de EL SERVICIO. La garantía que se presente debe ser incondicional, solidaria, irrevocable y de realización automática en el país, al solo requerimiento de EL BANCO. Asimismo, debe ser emitida por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, debe estar autorizada para emitir garantías; o estar considerada en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.
- 6.5. Para la ejecución de EL SERVICIO, EL PROVEEDOR debe contar como mínimo con el Personal que se detalla en el numeral 11 de los Términos de Referencia (**ANEXO N° 001**), con los requisitos mínimos establecidos. En caso se modifique al personal de la prestación de EL SERVICIO por motivo de caso fortuito o fuerza mayor, se deberá seguir el procedimiento establecido y cumplir con los plazos que se establecen en el último párrafo del numeral 11 de los Términos de Referencia.

- 6.6. Proporcionar la información/documentación que requiera EL BANCO, relacionada con EL SERVICIO, en la forma y plazos establecidos por EL BANCO.
- 6.7. Cumplir oportunamente con los entregables de EL SERVICIO, los cuales se describen en el numeral 10 de los Términos de Referencia (Anexo N° 001).
- 6.8. Para la ejecución de EL SERVICIO, EL PROVEEDOR podrá subcontratar actividades complementarias (no la principal o principales que, en este caso, serían los componentes para generar y validar el CVV2 dinámico) hasta por un 40% del monto total contractual pactado, lo cual debe ser comunicado previamente a EL BANCO con el detalle de las actividades que serán materia de subcontratación para la autorización expresa previa de EL BANCO. La subcontratación no enerva la responsabilidad de EL PROVEEDOR frente a EL BANCO por el cumplimiento en la ejecución total de EL SERVICIO materia de EL CONTRATO.
- 6.9. EL PROVEEDOR declara conocer y aceptar frente a EL BANCO que éste mantendrá todos los derechos de propiedad intelectual, incluidos sin limitación, las patentes, derecho de autor, metodologías, documentación, procedimientos, personalizaciones efectuadas en los componentes del software, así como la construcción, adecuaciones de programas, que se genere durante la prestación de EL SERVICIO.
- 6.10. A la suscripción de EL CONTRATO, EL PROVEEDOR deberá presentar obligatoriamente todos los documentos que se describen en el numeral 23 de los Términos de Referencia (Anexo N° 001).
- 6.11. EL PROVEEDOR es responsable por la calidad ofrecida y por los vicios ocultos de EL SERVICIO prestado por un plazo de un (1) año contado a partir de la última conformidad otorgada por EL BANCO.
- 6.12. EL PROVEEDOR, a la firma de EL CONTRATO, deberá hacer entrega a EL BANCO de la póliza de seguro contratada (póliza Tech E&O), conforme a las características y condiciones que se establecen en el numeral 21 de los Términos de Referencia (ANEXO N° 001).
- 6.13. EL PROVEEDOR deberá cumplir en su integridad con la normativa interna de EL BANCO que se describe en el Anexo 1 de los Términos de Referencia, siendo que EL BANCO, a la firma de EL CONTRATO, le hará entrega de la misma para su estricto cumplimiento durante la ejecución de EL SERVICIO.
- 6.14. EL PROVEEDOR deberá cumplir con entregar la información/documentación que se establece en la cláusula Décimo Tercera de EL CONTRATO, en la forma, plazo y oportunidad que ahí se establece.

#### Garantía

EL PROVEEDOR entregó al perfeccionamiento del CONTRATO la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de EL BANCO por los conceptos, montos y vigencias siguientes:

- **Garantía de fiel cumplimiento del contrato:** Referida a la contratación del "Servicio de implementación de mecanismos de seguridad en transacciones con tarjeta BN (de crédito y débito) no presente", por el importe de [CONSIGNAR EL MONTO], a través de la Carta Fianza N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE]. Dicho monto es equivalente al diez por ciento (10%) del monto del contrato original, con vigencia desde el [CONSIGNAR FECHA DE INICIO DE LA VIGENCIA] la misma que debe mantenerse vigente hasta el [CONSIGNAR FECHA DE TERMINO DE LA VIGENCIA], la cual debe mantenerse vigente hasta la conformidad de la prestación.

#### CLÁUSULA SÉTIMA. - OBLIGACIONES DEL BANCO

- 7.1. EL BANCO deberá pagar la contraprestación pactada a favor de EL PROVEEDOR dentro del plazo establecido, siempre que se verifiquen las condiciones establecidas en la cláusula cuarta de EL CONTRATO y los Términos de Referencia (Anexo N° 001).
- 7.2. EL BANCO proporcionará a EL PROVEEDOR toda la información que, de común acuerdo entre LAS PARTES, consideren necesaria para la prestación de EL SERVICIO; para lo cual

EL PROVEEDOR deberá cumplir con las políticas de seguridad y confidencialidad de la información que se establecen en EL CONTRATO.

**CLÁUSULA OCTAVA.- PENALIDADES**

En caso de retraso injustificado del PROVEEDOR en la implementación y puesta en producción de los componentes transacciones del servicio (generación y validación de CVV2 Dinámico para tarjetas de débito Visa y tarjetas de crédito Mastercard), EL BANCO aplicará automáticamente una penalidad por mora por cada día de atraso. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad diaria (S/)} = \frac{0.10 * (\text{Costo de implementación del componente transaccional})}{0.25 * (\text{Plazo en días para implementación del componente transaccional})}$$

**Otras Penalidades Aplicables**

**Por Cambio en el Equipo del Proyecto del Proveedor**

N°	Penalidad	Monto de la Penalidad	Procedimiento de Aplicación de la Penalidad
1	Por realizar el cambio de cualquiera de los miembros del equipo del proyecto del proveedor (jefe de Proyecto, Ingeniero de Integración y Seguridad, Ingeniero de Soporte de Componentes de Software), sin previo aviso y sin la autorización/conformidad del Banco. La penalidad se aplicará por ocurrencia.	2 U.I.T.	La Subgerencia Canales Alternos remitirá informe y otra documentación requerida a la Sección Ejecución y Seguimiento de contratos de EL BANCO para la aplicación de la penalidad.

**Por Niveles de Servicio**

Si por alguna razón distinta a las descritas en el numeral 9 de los Términos de Referencia (Anexo N° 001), no se cumplieran los niveles de servicio requeridos por EL BANCO, se aplicarán a EL PROVEEDOR las penalidades según tabla adjunta:

Penalidades			
N°	Supuestos de Aplicación de Penalidad	Monto de la Penalidad	Procedimiento de Aplicación de la Penalidad
1	Menos del 99.99% en la disponibilidad de los componentes transaccionales (para generación y validación de CVV2 dinámico)	5% del importe de facturación mensual en el que se presenta el problema, por cada día en el que se presente la intermitencia.	Informe de la Subgerencia de Producción de EL BANCO con evidencia del incumplimiento del SLA.
2	Falta de soporte AD HOC (24x7) durante 07 días calendarios contados a partir de la fecha de pase a producción de cada componente transaccional del servicio	5% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia Canales Alternos de EL BANCO con las evidencias y sustentos correspondientes
3	Incumplimiento de SLA en otros componentes de soporte (los no descritos en el ítem 2 de este cuadro)	1% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia Canales Alternos de EL BANCO con las evidencias y sustentos correspondientes

4	No reporte oportuno al Banco de la no disponibilidad de componentes transaccionales del servicio por mantenimientos programados, urgentes o correctivos	3% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia Canales Alternos de EL BANCO con las evidencias y sustentos correspondientes
5	Incumplimiento de SLA respecto a tiempos para primer contacto, primera respuesta, reportes periódicos, solución del incidentes o solución de Problemas; lo que incluye el incumplimiento en la entrega o entrega tardía del informe de cierre de la atención (aplicable para incidentes críticos y moderados; así como la gestión de los problemas)	3% del importe de facturación mensual en el que se presenta el problema, por cada vez que se presente el problema.	Informe de la Subgerencia de Producción de EL BANCO con evidencia de monitoreo de la plataforma.

**Por Falta de Certificación Vigente durante la prestación del servicio**

N°	Supuestos de Aplicación de Penalidad	Monto de la Penalidad	Procedimiento de Aplicación de la Penalidad
1	Por no contar con la certificación vigente como PCI DSS	El 10% de la facturación mensual	Para el caso de la certificación como PCI DSS, debe solicitarse al proveedor el certificado de cumplimiento vigente.  La Subgerencia Canales Alternos de EL BANCO remitirá informe y otra documentación requerida a la Sección Ejecución y Seguimiento de contratos.

No existe un límite de penalidades mensuales durante la prestación del SERVICIO. No se requiere la aceptación de EL PROVEEDOR para la aplicación de las penalidades por parte de EL BANCO.

Se precisa que cada uno de los tipos de penalidad (penalidad por mora (por retraso injustificado) y otras penalidades aplicables) pueden alcanzar un monto máximo equivalente al diez por ciento (10%) del monto del CONTRATO vigente, después de lo cual EL BANCO podrá resolver el contrato de pleno derecho por causal de incumplimiento en aplicación al artículo 1430 del Código Civil.

Estas penalidades se deducen de los pagos a cuenta (mensuales) o del(los) pago(s) único(s), según corresponda.

Las multas impuestas a causa de sanciones por parte de los organismos reguladores como consecuencia de operaciones y/o deficiencias en EL SERVICIO y/o que estas deriven de una interrupción y/o algún error o falla en las condiciones de la prestación del SERVICIO brindado o por la falta de las certificaciones correspondientes, serán asumidas al 100% por EL PROVEEDOR, debiendo abonarse, de forma oportuna e inmediata, dicho importe en la cuenta corriente que determine EL BANCO, siendo que EL BANCO también se encuentra facultado para retener y cobrarse de manera directa de los montos que se encuentran pendientes de pago por EL SERVICIO prestado por EL PROVEEDOR.

### **CLÁUSULA NOVENA.- RESOLUCIÓN DEL CONTRATO**

LAS PARTES declaran que podrá resolverse EL CONTRATO, por cualquiera de los siguientes supuestos:

- EL PROVEEDOR o EL BANCO incumpla con alguna de las obligaciones establecidas en el presente CONTRATO y/o los Términos de Referencia (Anexo N° 001), para lo cual la previamente deberá enviarse una carta notarial para que subsane dicho incumplimiento en un plazo de quince (15) días calendario de recibida la misma. De continuar el incumplimiento, la resolución del CONTRATO se formalizará con la remisión de una carta notarial al domicilio señalado en la parte introductoria del CONTRATO. Esta estipulación no aplica para las cláusulas Décimo Tercera y Décimo Cuarta de EL CONTRATO, cuyo incumplimiento por parte de EL PROVEEDOR faculta a EL BANCO para dar por terminado EL CONTRATO de pleno derecho y de forma automática conforme al artículo 1430 del Código Civil.
- Por mutuo acuerdo de LAS PARTES, el que deberá constar por escrito.
- Por caso fortuito o fuerza mayor debidamente comprobado, que imposibilite el cumplimiento de las obligaciones contraídas en el presente CONTRATO.
- Por decisión unilateral de cualquiera de LAS PARTES; sin necesidad de expresar motivo, para lo cual la parte que desee resolverlo deberá comunicar notarialmente tal decisión a la otra parte con una anticipación no menor a doce (12) meses; vencido dicho plazo, **EL CONTRATO** quedará automáticamente resuelto de pleno derecho, sin generar ninguna penalidad o reparación.

La resolución del CONTRATO no libera a LAS PARTES del cumplimiento de todas las obligaciones adquiridas con anterioridad a la resolución y que se encuentren pendientes de ejecución, en los términos y condiciones establecidas en el presente CONTRATO, así como al cumplimiento de las obligaciones que surjan como consecuencia de la resolución antes señalada.

La finalización del CONTRATO por cualquier causa, exige el cumplimiento obligatorio de la transferencia a EL BANCO de toda la documentación, información y/o activo que pertenezca al EL BANCO y posea EL PROVEEDOR, en virtud del SERVICIO prestado dentro del marco del CONTRATO. Es así que, luego de resuelto EL CONTRATO, EL PROVEEDOR debe remitir a la Sede Principal de EL BANCO toda la documentación entregada por EL BANCO para la prestación de SERVICIO contratado, en un plazo máximo de 48 horas, bajo responsabilidades civiles y/o penales que se puedan generar.

### **CLÁUSULA DÉCIMA: MANDATORIOS DE LAS FRANQUICIAS**

EL PROVEEDOR realizará todo cambio y/o mejoras tecnológicas que se requieran para la prestación del SERVICIO con las franquicias Visa y Mastercard Internacional que sean de cumplimiento obligatorio. Los costos de estos cambios y/o mejoras deberán ser asumidos en su integridad por EL PROVEEDOR.

### **CLÁUSULA DÉCIMO PRIMERA.- INDEMNIDAD**

11.1 EL PROVEEDOR mantendrá indemne a EL BANCO de toda demanda o reclamo, ya sea administrativo, arbitral, judicial o extrajudicial, que pudiera ser interpuesto contra EL BANCO por cualquier tercero, como resultado del incumplimiento de las obligaciones de EL PROVEEDOR establecidas en EL CONTRATO, así como por cualquier falla y/o error en las condiciones de la prestación EL SERVICIO. En ese sentido, EL PROVEEDOR se responsabiliza de los daños y perjuicios que su incumplimiento pudiera generar a EL BANCO, así como de cualquier sobre costo que pudiera derivarse de los actos señalados sin límite alguno.

- 11.2 EL PROVEEDOR se obliga a reembolsar íntegramente las costas, costos y cualquier importe que tenga que pagar a EL BANCO para hacer frente a acciones judiciales, extrajudiciales o administrativas iniciadas en su contra, como consecuencia del incumplimiento de las obligaciones de EL PROVEEDOR, siempre que este no se haya originado por un hecho fortuito o fuerza mayor o a cualquier causa imputable debidamente comprobada a EL BANCO.
- 11.3 Esta obligación se extiende a las indemnizaciones, multas o cualquier pago que EL BANCO sea requerido a pagar, ya sea por una autoridad judicial o administrativa, por resolución o sentencia en última instancia, por haber sido declarado responsable solidario de EL PROVEEDOR, que se originen en el incumplimiento de las obligaciones por causa imputable a EL PROVEEDOR.
- 11.4 Si como consecuencia de los eventos señalados en los párrafos anteriores una autoridad judicial o administrativa requiere a EL BANCO el pago de cualquier suma de dinero, EL BANCO comunicará el requerimiento de pago a EL PROVEEDOR, debiendo adjuntar a dicho requerimiento copia legalizada o certificada de la sentencia o resolución correspondiente, expedida en última instancia, solicitando su cancelación en un plazo no mayor de diez (10) días hábiles. Vencido el plazo sin que EL PROVEEDOR haya cancelado el importe respectivo, EL BANCO quedará autorizado automáticamente a debitar el importe adeudado de la(s) factura(s) que tuviera pendiente de cobro EL PROVEEDOR en EL BANCO por la prestación de EL SERVICIO, quedando de este modo automáticamente compensada la suma adeudada. Este mismo procedimiento se aplicará para el reembolso de los gastos que haya incurrido EL BANCO por la tramitación del proceso o procedimiento, presentando EL BANCO una liquidación de los gastos sustentada.
- 11.5 En caso de que EL BANCO sea sancionado con multas regulatorias y con medidas correctivas como consecuencia del incumplimiento de las obligaciones previstas en EL CONTRATO, estas serán asumidas por EL PROVEEDOR cuando hayan sido impuestas por causas imputables a la gestión de EL PROVEEDOR. Para efectos de establecer esta responsabilidad, EL BANCO comunicará oportunamente el incumplimiento de las obligaciones y/o el requerimiento de la información que se requiera, para que, en este último caso, sea entregada en su momento para presentarse en la contestación del reclamo y/o denuncia.
- 11.6 Los daños, perjuicios, reclamaciones, subrogación de gastos, indemnizaciones, sanciones o cualquier otro concepto establecido en la presente cláusula, en los que incurriese o su personal o empresas subcontratadas y que hayan sido como consecuencia del incumplimiento de las obligaciones de EL PROVEEDOR, por causas fehacientemente demostradas e imputables a EL PROVEEDOR, y debidamente establecidas por una resolución o sentencia en última instancia, esta se hará responsable de dichos costos o penalidades o cualquier otro concepto sin límite alguno.

**CLÁUSULA DÉCIMO SEGUNDA: PREVENCIÓN DE LAVADO DE ACTIVOS Y ANTICORRUPCIÓN**

- 12.1. EL PROVEEDOR declara conocer que EL BANCO es una empresa sujeta a la Resolución SBS N° 2660-2015 - Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, que tiene implementado un sistema de prevención de LA/FT con componentes de cumplimiento y de gestión de riesgos de LA/FT. Por tanto, EL PROVEEDOR se obliga a respetar la mencionada norma, así como cualquier otra norma legal sobre esta materia, desde su entrada en vigencia.
- 12.2. Como parte de la gestión del Riesgo de Lavado de Activos y Financiamiento del Terrorismo, EL BANCO no se vincula con personas (ya sea con personas naturales como tal o estas en calidad de representantes de personas jurídicas privadas o de Entidades

con personería jurídica de derecho público), respecto de las cuales se les haya atribuido, en sede judicial, responsabilidad por delitos precedentes de lavado de activos y financiamiento del terrorismo. Para tales efectos, EL BANCO, conforme a la Resolución SBS N° 2660-2015, aplica procedimientos de debida diligencia en el conocimiento de sus proveedores.

12.3. EL PROVEEDOR, para la suscripción de EL CONTRATO, deberá presentar la siguiente información:

- ✓ Nombres y Apellidos completos o denominación o razón social, en caso se trate de una persona jurídica.
- ✓ Registro Único de Contribuyentes (RUC), o registro equivalente para no domiciliados, de ser el caso.
- ✓ Tipo y número de documento de Identidad, en caso se trate de una persona natural.
- ✓ Dirección de la oficina o local principal.
- ✓ Años de Experiencia en el mercado.
- ✓ Rubros en los que el proveedor brinda sus productos o servicios.
- ✓ Identificación de los accionistas, socios o asociados que tengan directa o indirectamente más del 25 % del capital social, aporte o participación de la persona jurídica y del nombre del representante legal, considerando la información requerida para las personas naturales.
- ✓ Declaración Jurada de no contar con antecedentes penales del proveedor, de ser el caso.

12.4. EL PROVEEDOR deberá actualizar la información en forma periódica, cada 02 años, sin perjuicio de comunicar a EL BANCO cualquier modificación de la información declarada.

12.5. La información a la que tiene acceso EL PROVEEDOR sólo podrá ser utilizada, para los fines señalados en el presente CONTRATO, de modo tal, que se obliga a guardar estricta y severa reserva de la información a la que tiene acceso.

### **CLÁUSULA DÉCIMO TERCERA.- GESTIÓN DE AUDITORIA Y RIESGOS**

#### **Lineamientos Generales:**

13.1. EL PROVEEDOR se obliga, siempre que se limite a información relacionada con la ejecución del CONTRATO a permitir la revisión, supervisión e inspección de los servicios prestados y de las condiciones que garanticen la seguridad de información, tratamiento de la información, protección de datos personales, continuidad del negocio y gestión de sus riesgos, por parte de la Dependencia Responsable del Contrato y la Unidad de Auditoría Interna del Banco, así como de la Sociedad Auditora Externa, la Superintendencia de Banca, Seguros y AFP, en la oportunidad que cualquiera lo solicite, con un aviso previo por escrito de diez (10) días hábiles, el cual será remitido a la dirección indicada por EL PROVEEDOR en el CONTRATO. En dicho comunicado se designarán a las personas que efectuarán la mencionada revisión, supervisión e inspección.

13.2. Consecuentemente EL PROVEEDOR se compromete a facilitar todos los recursos y medios necesarios a las personas antes mencionadas para efectuar dichas revisiones.

13.3. Los costos que implique la contratación de terceros, así como los costos de desplazamiento, hospedaje y alimentación del personal del Banco de la Nación con motivo de estas auditorías, revisiones, inspecciones, supervisiones, serán cubiertos por EL BANCO.

- 13.4. EL PROVEEDOR debe asegurar el acceso adecuado a la información, en tiempos razonables y a solo requerimiento, por parte de la SBS (Superintendencia de Banca, Seguros y AFP), Auditoría Interna y la Sociedad de Auditoría Externa.
- 13.5. En caso EL BANCO incurriera en costos y/o multas establecidas por parte de un organismo regulador u otro, mediante una resolución o sentencia firme producto de la interrupción y/o algún error o falla en las condiciones de la prestación del servicio por causas imputables a EL PROVEEDOR, éste se hará totalmente responsable de dichas penalidades, asumiendo el importe de las mismas sin reserva ni limitación alguna. Por lo que EL BANCO, podrá evaluar la aplicación de penalidades o el pago de indemnización.

### **Lineamientos de Seguridad de la Información**

#### **Seguridad de la Información y Ciberseguridad**

- 13.6. Para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de la información; así como la debida autenticación del cliente para la autorización y trazabilidad de sus operaciones; EL PROVEEDOR debe cumplir con los lineamientos de seguridad de la información y ciberseguridad establecidos en las siguientes normativas:

#### **Resolución SBS N° 504-2021, Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad y sus modificaciones.**

- 13.7. EL PROVEEDOR se obliga a adoptar las medidas necesarias para que sus trabajadores, representantes y terceros que intervienen en el servicio contratado, cumplan con las disposiciones relacionadas a la seguridad de información y ciberseguridad establecidas en la normativa interna del BANCO.
- 13.8. El PROVEEDOR es el responsable del resguardo y protección de los activos de información (equipos, dispositivos informáticos, aplicaciones, información, entre otros) de propiedad del BANCO involucrados en el servicio contratado, que se encuentren bajo la administración del PROVEEDOR o formen parte de dicho servicio.
- 13.9. El PROVEEDOR permitirá, facilitará y/u otorgará a EL BANCO, la revisión del cumplimiento de las medidas de seguridad de la información y ciberseguridad relacionadas al servicio contratado.
- 13.10. El PROVEEDOR debe documentar las especificaciones técnicas de las API para la provisión del SERVICIO, de forma que facilite su auditoría y su uso, dichos documentos deben ser proporcionados al BANCO, considerando las siguientes medidas:
- a) Contar con mecanismos para la autenticación mutua de los sistemas con los que se interconecta o utiliza las API.
  - b) Utilizar buenas prácticas de desarrollo seguro de las API y revisar periódicamente su codificación.
- 13.11. El PROVEEDOR declara que tiene pleno conocimiento que EL BANCO se encuentra sujeto a las exigencias de la Resolución SBS N°504-2021 "Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad"; por lo que El PROVEEDOR se compromete a implementar en sus sistemas de información los requerimientos de seguridad sobre el uso de APIs para la provisión de servicios en línea y las responsabilidades respecto a las medidas de seguridad que debe mantener en la provisión del servicio; los cuales deben ser coordinados con EL BANCO.
- 13.12. El PROVEEDOR, previo a la puesta en producción del SERVICIO contratado, debe evidenciar que cuenta con las certificaciones ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, y que cuenta con un reporte SOC 2 tipo 2 u otros equivalentes relevantes al

SERVICIO contratado y posterior a la puesta en producción del SERVICIO, debe evidenciar anualmente la vigencia de dichas certificaciones. El PROVEEDOR debe proporcionar al BANCO, copia o indicar el enlace web donde se visualicen las referidas certificaciones.

**Norma Técnica Peruana NTP - ISO/IEC 27001-2022 - Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, según los siguientes aspectos:**

- 13.13. EL PROVEEDOR debe contar con un proceso de gestión de riesgos, alertas e incidentes de seguridad de la información y ciberseguridad, relacionados con EL SERVICIO contratado. Las evidencias de la existencia y ejecución de dicho proceso deben ser remitido al inicio del SERVICIO y posteriormente a solicitud del BANCO.
- 13.14. EL PROVEEDOR se obliga a cumplir con los controles de seguridad de la información y ciberseguridad establecidos por EL BANCO, respecto al control de los accesos, cifrado de la información, la revisión del desempeño, el seguimiento de la ejecución del servicio, presentación de informes y auditorías, así como las obligaciones regulatorias enmarcadas en los requisitos de seguridad de la información.
- 13.15. EL PROVEEDOR debe contar con las medidas apropiadas para garantizar la seguridad en el procesamiento, almacenamiento, transmisión, autenticación, trazabilidad y adaptabilidad de la información del BANCO que se utilice en EL SERVICIO contratado.

**Confidencialidad de la Información**

- 13.16. EL BANCO es propietario de toda la información que, por razones del alcance del presente CONTRATO, entregue al PROVEEDOR.
- 13.17. EL PROVEEDOR se compromete a mantener la confidencialidad y reserva absoluta y no revelar a terceros, sin previa autorización escrita del BANCO, toda información a la que tenga acceso, que le sea suministrada o conozca directa o indirectamente durante la ejecución del servicio contratado.
- 13.18. El compromiso de confidencialidad se prolonga hasta por 10 años después de terminado el servicio y se hace extensivo al personal de EL PROVEEDOR aun cuando hayan dejado de tener vínculo laboral con EL PROVEEDOR.
- 13.19. Para los efectos de EL CONTRATO, se entenderá como "Información Confidencial" toda aquella información comercial, financiera, técnica, de inteligencia comercial, metodologías, procesos, políticas, procedimientos, estándares, estrategias, productos, bases de datos, matrices y programas de cómputo, códigos, claves, nombres y/o experiencia de empleados y consultores, propiedad intelectual, fórmulas, negocios, lista de clientes, estados financieros, información sobre productos de software y hardware de EL BANCO, que sea entregada a EL PROVEEDOR, ya sea de manera escrita, oral, visual y/o digital; que por sus características le signifique a EL PROVEEDOR obtener y mantener una ventaja competitiva o económica frente a terceros en la realización de actividades económicas.
- 13.20. En caso EL BANCO otorgue información confidencial, para ser utilizada y custodiada por EL PROVEEDOR para la provisión del SERVICIO contratado, deberá ser devuelta a EL BANCO en un plazo no mayor a diez (10) días calendarios, así como la eliminación de la información ante la culminación del SERVICIO.

- 13.21. EL PROVEEDOR está autorizado para que su personal pueda hacer uso de la información confidencial provista por EL BANCO siempre que dicho personal esté directamente relacionado a la ejecución del presente CONTRATO, haya sido informado de la naturaleza confidencial del mismo y haya sido instruido sobre las medidas de protección adoptadas por EL PROVEEDOR, las cuales deberá aplicar para la protección de la confidencialidad

de esta. EL PROVEEDOR será responsable por las infracciones comprobadas de incumplimiento del acuerdo de confidencialidad que hayan sido cometidas por el personal asignado para la ejecución del SERVICIO objeto del presente CONTRATO.

13.22. El PROVEEDOR no debe capturar, utilizar, almacenar, acceder, visualizar ni desviar la información de los clientes y usuarios de El BANCO, sin la autorización expresa de El BANCO.

13.23. Los aplicativos, sistemas, softwares e información que EL PROVEEDOR desarrolle en el marco del servicio que EL BANCO contrata es de titularidad del BANCO por lo tanto EL PROVEEDOR no podrá asumir ningún derecho, de ningún tipo, sobre la creación o desarrollo. La divulgación de la creación o desarrollo no implica el licenciamiento de derecho de patentes o derecho de autor o ningún otro derecho por parte de EL PROVEEDOR, que no sean los establecidos en EL CONTRATO.

13.24. El PROVEEDOR declara conocer que la vulneración y/o divulgación de secretos empresariales se encuentra tipificada como delito en conformidad con lo estipulado en el Código Penal.

13.25. EL PROVEEDOR debe reportar cualquier incidente de seguridad que implique la exposición, alteración o pérdida de datos de clientes e implementar procedimientos para identificar y reportar incidentes de seguridad de este tipo. Se debe considerar que EL BANCO debe reportar a la Autoridad Nacional de Protección de Datos Personales este tipo de incidentes en un máximo de 48 horas de ocurrido

**Protección del Secreto Bancario, Datos Personales, Delitos Informáticos, Reglamento de Tarjetas de Crédito y Débito y Estándar PCI DSS:**

13.26. El PROVEEDOR declara conocer que está obligado a salvaguardar y mantener la confidencialidad del secreto bancario, de los datos personales de los usuarios y clientes del BANCO, de acuerdo con la Constitución Política del Perú, Ley N° 29733 Ley de Protección de datos personales, su Reglamento y Directivas de Seguridad, Ley N° 26702, Secreto Bancario, sus modificatorias y actualizaciones; aplicables al servicio asociado al CONTRATO.

13.27. EL PROVEEDOR declara conocer las sanciones tipificadas en la Ley N° 30096, Ley de Delitos Informáticos (integridad de datos informáticos, tráfico ilegal de datos, interceptación de datos informáticos), y la Ley N° 30171 que modifica la Ley N° 30096, Ley de Delitos Informáticos, bajo la cual se obliga a dar estricto cumplimiento de estas disposiciones.

13.28. EL PROVEEDOR se somete a las disposiciones previstas de la Resolución S.B.S. N.º 6523 -2013 Reglamento de Tarjetas de Crédito y Débito - Art. 18º Medidas en Materia de Seguridad de la Información, aplicables al SERVICIO, bajo la cual se obliga a dar estricto cumplimiento.

13.29. EL PROVEEDOR declara conocer que asume la condición de responsable de la seguridad de los datos de las tarjetas de pago que posee o almacena, procesa o transmite en el marco del presente contrato, o en la medida en que puedan afectar a la seguridad del entorno de datos de tarjetas de pago de EL BANCO.

13.30. EL PROVEEDOR se obliga a adoptar las disposiciones para la protección de los datos del titular de la tarjeta y medidas sólidas de control de acceso previstas por EL BANCO relacionadas al Estándar de Seguridad de Datos de Payment Card Industry - PCI DSS, bajo la cual deberá dar estricto cumplimiento.

13.31. EL PROVEEDOR en caso corresponda, acepta y reconoce la responsabilidad del cumplimiento de las medidas de seguridad de datos de las tarjetas de pago de los servicios

que EL PROVEEDOR, a su vez, contrata con terceros (contratación en cadena) para lograr el cumplimiento general del SERVICIO en el marco del presente CONTRATO.

### Lineamientos de continuación de Negocios

13.32. EL PROVEEDOR debe desarrollar la gestión de continuidad para el servicio objeto del contrato mediante la aplicación de la Resolución S.B.S N° 877-2020 Reglamento para la gestión de la continuidad del negocio o buenas prácticas para en la Gestión de Continuidad del Negocio (ISO 22301) para este tipo de SERVICIO.

13.33. EL PROVEEDOR se compromete a mantener la continuidad del SERVICIO contratado por EL BANCO; para lo cual, debe contar con procedimientos documentados que permitan responder, recuperar, reanudar y restaurar el SERVICIO objeto del CONTRATO; además, los referidos procedimientos deben formar parte de un Plan de Recuperación de Tecnología de Información o en su defecto de un Plan de Continuidad de Negocio, de tal modo que su ejecución asegure la alta disponibilidad y recuperación del servicio conforme al tiempo objetivo de recuperación requerido en el numeral 9.1 de los Términos de Referencia (Anexo N° 001).

13.34. EL PROVEEDOR debe entregar a EL BANCO: el Plan de Recuperación de Tecnología de Información y/o Plan de Continuidad de Negocio, los cuales deben estar actualizados y probados cuando menos una vez al año; asimismo, EL PROVEEDOR deberá contar con un Programa de Pruebas anuales que permitan verificar el cumplimiento de los procedimientos de recuperación documentados. Al respecto, EL PROVEEDOR deberá remitir cada primer trimestre del año el Plan(es) y Programa de Pruebas, y concluido el año y ante requerimiento de EL BANCO deberá remitir los informes de pruebas que indiquen los resultados alcanzados.

13.35. EL PROVEEDOR podrá programar pruebas en horarios de madrugada a fin de reducir la afectación del servicio; para casos de pruebas que implique la interrupción del servicio, estas deben ser identificadas y coordinadas con EL BANCO previo a su ejecución. Dichas pruebas deben contemplar la validación de alta disponibilidad de los componentes tecnológicos que soportan el servicio contratado, ante una interrupción. Asimismo, EL BANCO podrá solicitar, por correo y/o por carta, su participación en el desarrollo de dichas pruebas (con cinco (05) días hábiles de anticipación) y, de tener alguna observación sobre los resultados podrá remitir a EL PROVEEDOR para que subsane la(s) observación(es) y/o No Conformidad(es) y EL PROVEEDOR comunique las acciones realizadas en un periodo no mayor a veinte (20) días calendarios.

13.36. Asimismo, para casos de pruebas que EL BANCO requiera realizar esta será coordinada con EL PROVEEDOR, y podría realizarse una vez al año.

13.37. Ante la eventual interrupción del SERVICIO objeto del CONTRATO; por causales imputables a EL PROVEEDOR, siempre que dicha interrupción sea por un tiempo mayor a 1 hora; EL PROVEEDOR deberá comunicar a EL BANCO de forma inmediata, o máximo cuatro horas después del incidente que origino la interrupción, comunicación que debe incluir la hora de inicio y fin (en caso que el incidente se encuentre superado) y posteriormente deberá remitir un informe de la incidencia, la cual debe contener como mínimo la fecha, hora, duración, causa/origen, responsabilidad, estado de los servicio(s) afectado(s), descripción del incidente, acciones de recuperación realizadas, diagnostico general, impacto del servicio, acción de mejora y recomendaciones, conclusiones, en un plazo máximo de tres (03) días hábiles, para su reporte se contabiliza a partir de la ocurrencia del evento. En caso de que no se haya concluido las acciones de superen o implementen las recomendaciones estas deberán reportarse hasta que se encuentre superada.

13.38. Para casos que EL PROVEEDOR realice cambios a sus configuraciones u otros componentes que involucren/afecten la operatividad del servicio objeto del contrato, deben ser comunicados a EL BANCO con siete (07) días calendarios de anticipación a la Gerencia de Tecnología de la Información de EL BANCO.

13.39. Lo antes mencionado puede ser sustentado con el envío de un Certificado ISO 22301 que se encuentre vigente, de requerir información adicional (referidos a los planes, cronograma de pruebas e informes de las pruebas) EL BANCO podrá solicitar a EL PROVEEDOR información en el cumplimiento de la cláusula de continuidad del negocio.

#### Gestión de Riesgos Operativos

13.40. EL PROVEEDOR debe aplicar las medidas de control para la gestión de los riesgos operacionales, que sean aplicables al servicio contratado por EL BANCO; que permita identificar, evaluar, tratar, controlar y monitorear los diversos riesgos asociados a dicho servicio, siendo responsable frente al BANCO en caso de la materialización de algún riesgo operativo que, en el marco de la prestación del SERVICIO, afecte al BANCO y/o sus clientes.

El incumplimiento de las obligaciones que asume **EL PROVEEDOR** en la presente cláusula Décimo Tercera constituye causal de resolución automática y de pleno derecho del presente CONTRATO, de conformidad con lo previsto en el artículo 1430° del Código Civil, sin perjuicio de la obligación de **EL PROVEEDOR** de pagar a **EL BANCO** la indemnización correspondiente.

#### CLÁUSULA DÉCIMA CUARTA. - ANTICORRUPCIÓN

14.1. EL PROVEEDOR promete desde la suscripción de EL CONTRATO, que EL SERVICIO se brindará con sujeción a las normas legales aplicables a este tipo de servicios en el Perú, absteniéndose de realizar cualquier práctica o acción que no se ajuste o no esté contemplada en las referidas normas o que pueda poner en tela de juicio su calidad profesional y/o moral, ante cualquier autoridad pública o privada, medios de comunicación o cualquier tercero.

14.2. EL PROVEEDOR declara que, durante el proceso de negociación y formalización de EL CONTRATO, no se ha generado ningún evento, situación o hecho que involucre algún indicio de corrupción que pueda comprometer el servicio, que se ofrece a EL BANCO ni a las obligaciones que se adquieren a la suscripción de EL CONTRATO.

14.3. En caso EL PROVEEDOR o sus representantes o personas vinculadas sean condenadas, en el país o el extranjero, mediante sentencia consentida o ejecutoriada por delitos de concusión, peculado, corrupción de funcionarios, enriquecimiento ilícito, tráfico de influencias, delitos cometidos en remates o procedimientos de selección, o delitos equivalentes en caso estos hayan sido cometidos en otros países; asimismo, en caso EL PROVEEDOR directamente o a través de sus representantes, hubiesen admitido y/o reconocido la comisión de cualquiera de los delitos antes descritos ante alguna autoridad nacional o extranjera competente; EL BANCO tendrá la facultad de resolver EL CONTRATO de pleno derecho y de forma automática en aplicación al artículo 1430 del Código Civil, sin perjuicio de la obligación de EL PROVEEDOR de pagar a EL BANCO la indemnización correspondiente.

#### CLÁUSULA DÉCIMO QUINTA. - VÍNCULO CONTRACTUAL ENTRE LAS PARTES

Queda perfectamente entendido que, entre LAS PARTES no se generará vínculo laboral alguno con motivo del cumplimiento de la prestación de EL SERVICIO contratado, por lo que LAS PARTES declaran que:

- 15.1. Reconocen expresamente que la naturaleza de EL CONTRATO es estrictamente bancaria y/o financiera y por ese motivo no estará EL BANCO en obligación de reconocer extremo o concepto laboral alguno a favor de EL PROVEEDOR o del personal que éste asigne para la prestación de EL SERVICIO. Por lo tanto, no habrá ninguna relación laboral de dependencia o subordinación entre EL BANCO y EL PROVEEDOR o el personal que éste contrate laboralmente para los fines de la prestación de EL SERVICIO, siendo de cuenta de EL PROVEEDOR todas las responsabilidades de carácter laboral y previsional con respecto a dicho personal, así como el pago de cualquier monto que pudiera ser ordenado a pagar dentro de un eventual proceso judicial de carácter laboral, incluyendo las costas y costos derivados del mismo.
- 15.2. En caso de que, EL BANCO autorice por escrito la subcontratación de terceras empresas o personas por EL PROVEEDOR, EL BANCO no incurrirá en responsabilidad u obligación hacia tales trabajadores, contratistas independientes u otras partes empleadas por EL PROVEEDOR para cumplir las obligaciones señaladas en EL CONTRATO. Tales personas serán consideradas en todo momento como trabajadores, agentes o contratistas independientes (cualquiera que sea aplicable) de EL PROVEEDOR.

#### **CLÁUSULA DÉCIMO SEXTA: PROTECCIÓN DE DATOS PERSONALES**

- 16.1. A través de la presente cláusula de Protección de Datos Personales se establecen las obligaciones y responsabilidades de cada una de las partes intervinientes respecto al adecuado tratamiento de los datos personales de los clientes, usuarios, proveedores y/o trabajadores de LAS PARTES. Todos los aspectos contemplados en el presente documento son de conformidad con la Ley N° 29733 - Ley de Protección de Datos Personales y su reglamento aprobado mediante Decreto Supremo N° 016-2024- JUS.
- 16.2. LAS PARTES, declaran que se someten a las disposiciones previstas por la Ley N° 29733 - Ley de Protección de Datos Personales, su reglamento- Decreto Supremo N° 016-2024- JUS, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias.
- 16.3. LAS PARTES declaran que los datos personales que se proporcionen entre sí, así como aquellos generados o recopilados con motivo de la prestación del servicio contratado, serán tratados de forma confidencial y estarán sujetos a estrictas medidas de seguridad, conforme lo dispone la citada Ley N° 29733, su reglamento, directiva y demás normas conexas, complementarias, modificatorias y/o sustitutorias. De ningún modo, la entrega de los datos personales tiene efectos legales de cesión de datos, al ser un elemento estrictamente necesario y proporcionado únicamente para los servicios contemplados en el presente CONTRATO.
- 16.4. RESPONSABLE DEL TRATAMIENTO (BANCO DE LA NACIÓN): Es quien decide sobre la finalidad y medios del tratamiento de datos personales. Esta definición no se restringe al titular del banco de datos, sino que incluye a cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales. Para efectos del presente contrato EL BANCO DE LA NACIÓN se constituye como RESPONSABLE DEL TRATAMIENTO.
- 16.5. ENCARGADO DE TRATAMIENTO DE DATOS PERSONALES: Es quien sola o actuando juntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento sin la existencia de un banco de datos personales. En adelante, cuando la presente cláusula haga mención a EL ENCARGADO se refiere a EL PROVEEDOR.

- 16.6. EL PROVEEDOR declara conocer que asume las condiciones de ENCARGADO del tratamiento cuando EL BANCO entrega o pone a disposición de manera directa o indirecta de EL PROVEEDOR información que contenga datos personales en virtud de una relación jurídica que los vincula. Del mismo modo, asume las condiciones de ENCARGADO cuando genera o recopila datos personales en el marco del presente contrato.
- 16.7. EL ENCARGADO únicamente realizará el tratamiento de datos personales siguiendo las instrucciones de EL BANCO y para los fines específicos del presente CONTRATO, sin que pueda decidir por cuenta propia la finalidad o los medios del tratamiento.

**OBLIGACIONES GENERALES DE EL ENCARGADO:**

- 16.8. EL ENCARGADO se compromete a cumplir con la normativa de protección de datos personales, así como implementar las medidas técnicas y organizativas necesarias evitando su alteración, pérdida, tratamiento, acceso no autorizado, de conformidad con el estado de la tecnología en cada momento, la naturaleza de los datos y los posibles riesgos a que estén expuestos.
- 16.9. Los datos contenidos en los bancos de datos encargados son de propiedad exclusiva de EL BANCO, esta titularidad se extiende a las recopilaciones, generaciones, elaboraciones, evaluaciones, segmentaciones o procesos similares que, en relación con los datos entregados, realice EL ENCARGADO de acuerdo con los servicios que presta. Las partes declaran que estos datos son confidenciales, por lo que están sujetos al más estricto secreto profesional, incluso una vez finalizada toda relación contractual entre las partes derivada de los servicios prestados.
- 16.10. EL ENCARGADO se obliga a utilizar los datos personales proporcionados por EL BANCO, así como aquellos que se generen o recopilen con motivo de la prestación del servicio contratado, exclusivamente para las finalidades establecidas en el presente contrato y conforme a las instrucciones que emita EL BANCO. En ningún caso podrá emplear dichos datos para fines propios o para propósitos distintos a los expresamente contemplados en este contrato.
- 16.11. Cuando EL ENCARGADO recopile directamente datos personales, deberá obtener consentimiento informado, conservar evidencia documental y acreditar que fue otorgado conforme al artículo 13 de la Ley N° 29733 - Ley de Protección de Datos Personales.
- 16.12. EL ENCARGADO garantiza que las personas autorizadas para acceder a los Bancos de Datos Personales se hayan comprometido, de forma expresa, a respetar la confidencialidad a través de una declaración jurada suscrita, lo cual debe encontrarse documentado y encontrarse a disposición de EL BANCO.
- 16.13. EL ENCARGADO solo concederá el acceso a los datos personales tratados en nombre de EL BANCO a personas bajo la autoridad de EL ENCARGADO que se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación legal de confidencialidad y solo si necesitan conocerlos. La lista de personas a quienes se haya concedido el acceso debe ser objeto de revisiones periódicas. Sobre la base de esta revisión, podrá retirarse el acceso a los datos personales si este acceso ya no es necesario, y, en consecuencia, esas personas ya no podrán acceder a los datos personales, asegurando que solo los empleados autorizados manejen los datos necesarios para el cumplimiento del servicio y

con sujeción al secreto profesional y confidencialidad que no se extingue con la culminación del contrato.

16.14. EL ENCARGADO se encuentra prohibido de transferir a terceros los datos personales recibidos o recopilados sin autorización previa por escrito de EL BANCO.

16.15. EL ENCARGADO se encuentra prohibido de subcontratar el tratamiento de los datos personales proporcionados, generados o recopilados con motivo de la prestación del servicio contratado, salvo autorización previa, expresa y por escrito de EL BANCO, debiendo el subcontratista cumplir las mismas obligaciones aquí establecidas, siendo solidariamente responsable con EL ENCARGADO frente a EL BANCO.

16.16. EL ENCARGADO debe implementar un Plan de Capacitación Anual para el personal que tiene acceso a los bancos de datos personales o se encarguen del tratamiento de los datos personales, con el objetivo de capacitarlos y entrenarlos en el cumplimiento de la regulación en materia de protección de datos personales y buenas prácticas para el tratamiento de la información y medidas de seguridad aplicables. Este Plan de Capacitación debe estar orientado al cumplimiento de la normativa vigente y a las obligaciones establecidas en el presente contrato, asimismo, debe estar documentado y las evidencias de su ejecución deben conservarse durante cinco (5) años y estar a disposición de EL BANCO.

16.17. EL ENCARGADO debe implementar un Plan de Inducción para el personal nuevo bajo las mismas condiciones mencionadas en el numeral precedente.

16.18. EL ENCARGADO y EL BANCO deben designar y acreditar a una persona de contacto, para cualquier comunicación y coordinación referente al tratamiento de los datos que se viene realizando en cumplimiento del presente contrato. EL ENCARGADO y EL BANCO se encuentran obligados a informar inmediatamente de cualquier cambio de la persona de contacto. Los datos de la persona de contacto (nombres y apellidos, número de documento de identidad, cargo y correo electrónico) serán entregados a su contraparte al día hábil siguiente de la firma del presente Contrato, mediante el envío de un correo electrónico u otro medio que permita acreditar la entrega de dichos datos.

16.19. Las PARTES convienen que EL ENCARGADO mantendrá indemne, defenderá y eximirá de responsabilidad a EL BANCO de toda demanda, queja o reclamo, ya sea administrativo, arbitral, judicial o extrajudicial, que pudiera ser interpuesto por cualquier tercero, como resultado del incumplimiento de las obligaciones de EL ENCARGADO pactadas en esta cláusula, incluidos los daños directos, indirectos, lucro cesante y sanciones administrativas, sin limitación alguna EL ENCARGADO se obliga a reembolsar íntegramente las costas, costos y cualquier importe que tenga que pagar EL BANCO para hacer frente a acciones judiciales, extrajudiciales o administrativas iniciadas en su contra, como consecuencia del incumplimiento de sus obligaciones pactadas en esta cláusula. Esta obligación se extiende a las indemnizaciones, multas o cualquier pago que EL BANCO sea requerido a pagar, ya sea por una autoridad judicial o administrativa, por resolución o sentencia en última instancia, por haber sido declarado responsable solidario que se originen como consecuencia del incumplimiento de las obligaciones pactadas en esta cláusula a cargo de EL ENCARGADO.





16.20. Si como consecuencia de los eventos señalados en los párrafos anteriores una autoridad judicial o administrativa requiere a EL BANCO el pago de cualquier suma de dinero, ésta comunicará el requerimiento de pago a EL ENCARGADO debiendo adjuntar a dicho requerimiento copia legalizada o certificada de la sentencia o resolución correspondiente, expedida en última instancia, solicitando su cancelación en un plazo no mayor de diez (10) días hábiles. En el caso que vencido el plazo sin que se haya cancelado el importe respectivo, EL BANCO quedará autorizado automáticamente a debitar el importe adeudado de la(s) factura(s) que tuviera pendiente de cobro EL ENCARGADO por la prestación de EL SERVICIO, quedando de este modo automáticamente compensada la suma adeudada. Este mismo procedimiento se aplicará para el reembolso de los gastos que haya incurrido EL BANCO por la tramitación del proceso o procedimiento, presentando EL BANCO una liquidación de los gastos debidamente sustentado. En caso no existan facturas por debitar para efectos de hacer el cobro respectivo, EL BANCO iniciará las acciones legales respectivas.

**OBLIGACIONES SOBRE FLUJO TRANSFRONTERIZO:**

16.21. EL ENCARGADO se obliga a comunicar a EL BANCO si realiza flujo transfronterizo de datos personales en el marco del presente contrato, debiendo indicar el lugar y nombre de la empresa, comprometiéndose a garantizar que la información que contenga datos personales que se transmita y/o transfiera entre el Perú y cualquier otro país, a causa directa o indirecta del servicio o producto contratado, mantiene y mantendrá los niveles de protección adecuados garantizando el nivel suficiente de protección para los datos personales que se vayan a tratar conforme a la Ley N° 29733, su reglamento, directivas y normas conexas, de manera tal que garanticen el nivel de seguridad apropiado para abordar los riesgos asociados al tratamiento de datos personales. Si los países a los que se van a transferir los datos no garantizan un nivel de protección adecuado, EL ENCARGADO deberá acreditar que el tratamiento está en disposición de ofrecer garantías adecuadas y, en todo caso, garantizar que los interesados cuenten con derechos exigibles y acciones legales efectiva.

**OBLIGACIONES DE SEGURIDAD:**

16.22. EL ENCARGADO se obliga a implementar, como mínimo, los siguientes controles de seguridad para el tratamiento de datos personales con motivo de la prestación del servicio contratado:

<b>Controles para mantener las áreas seguras</b>	
1	Perímetros de seguridad que protegen áreas donde se realice el tratamiento de datos personales.
2	Controles apropiados de ingreso para asegurar que se le permita el acceso solo al personal autorizado.
3	Sistema contra desastres naturales, ataque maliciosos o accidentes.
4	Procedimientos para el trabajo en áreas seguras.
5	Control de puntos de acceso, áreas de despacho, carga y otros donde personas no autorizadas pueden ingresar al local, y de ser el caso aislar las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
<b>Controles para mantener los equipos seguros dentro y fuera de las instalaciones</b>	
1	Ubicación y protección de equipos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.

2	Protección de equipos contra fallas de electricidad y otras alteraciones causadas por desperfectos en los servicios de suministro.
3	Protección de interceptación, interferencia y/o daño del cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte.
4	Imposibilidad de retirar equipos, información o software sin la autorización previa.
5	Asegurar, antes de su disposición o reutilización, que los equipos que contengan medios de almacenamiento de datos sensibles, hayan sido eliminados o sobre escritos.
6	Asegurar que los equipos informáticos cuenten con protección apropiada en caso sean desatendidos por los usuarios.
7	Implementación de una política de escritorio y pantalla limpios de papeles y de medios de almacenamiento removibles, para las instalaciones de procesamiento de la información.
<b>Controles para garantizar la generación de copias de respaldo seguras y continuas y verificación de integridad de las mismas</b>	
1	Las copias de respaldo se realizan con una frecuencia semanal como mínimo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos personales. Dicho procedimiento debe contar con las medidas de seguridad para su almacenamiento, transferencia y destrucción si fuese el caso.
2	Se debe verificar la integridad de los datos almacenados en las copias respaldo, incluyendo, de ser el caso, la recuperación completa ante una interrupción o daño que garantice el retorno al estado en el que se encontraba al momento en que se produjo la interrupción o daño.
<b>Controles para la Transferencia lógica o electrónica de los datos personales</b>	
1	El intercambio de datos personales desde los ambientes de procesamiento o almacenamiento hacia cualquier destino fuera de las instalaciones físicas de la entidad, solo procede con la autorización del titular del banco de datos personales y se realiza utilizando los medios de transporte autorizados por el mismo, implementando las medidas necesarias (entre las que se encuentran el cifrado de datos, uso de firmas y certificados digitales, checksum de verificación, entre otros) para evitar el acceso no autorizado, pérdida o corrupción durante el tránsito hacia su destino.
<b>Controles para el almacenamiento de documentación no automatizada</b>	
1	Los armarios, archivadores u otros elementos en los que se almacenen datos personales contenidos en documentos no automatizados son protegidos con puertas dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente.
2	Las áreas en las que se encuentren los datos personales permanecen cerradas cuando no sea preciso el acceso a los documentos.
3	Todas las llaves o mecanismos de apertura deben ser asignadas de manera formal, y de ser el caso, deben contar con procedimientos de traspaso y asignación. Si por las características de los locales que se dispusiera no fuera posible mantener cerradas las áreas donde se encuentran los armarios, archivadores u otros elementos en los que se almacenen documentos no automatizados con datos personales, se deben adoptar las medidas alternativas.
<b>Controles para la copia o reproducción de documentación automatizada y no automatizada</b>	
1	La generación de copias o la reproducción de los documentos que contienen datos personales, únicamente pueden ser realizadas bajo el control del personal autorizado.

*el*

*X*

*Handwritten signature*

2	Debe procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.
---	--

16.23. Cuando el ENCARGADO realice el tratamiento de datos personales a través de medios digitales, debe tener documentado e implementado, como mínimo, los siguientes controles de seguridad adicionales:

1	<p>El control de acceso a los datos personales que incluye:</p> <p>a) Gestión de accesos desde el registro de un usuario hasta su eliminación o baja, incluyendo eventualidades periódicas como periodos vacacionales o permisos esporádicos.</p> <p>b) Procedimientos de identificación y autenticación.</p> <p>c) Gestión de los privilegios asignados a dicho usuario, incluyendo la verificación periódica de los mismos, que debe ser ejecutado periódicamente en un intervalo mínimo de tiempo semestral.</p> <p>d) Mecanismos de autenticación del usuario ante el sistema que implica la asignación de uso de usuario contraseña, uso de certificados digitales, tokens, entre otros.</p>
2	El monitoreo y revisión periódica de las medidas de seguridad y los planes de capacitación del personal, dependiendo de sus roles y responsabilidades, respecto al tratamiento de datos personales que efectúan.
3	La generación y el mantenimiento de registros que provean evidencia de las interacciones con los datos lógicos, incluyendo para los fines de la trazabilidad, la información de cuentas de usuario con acceso al sistema, horas de inicio y cierre de sesión y acciones referidas a procesamiento, visualización, modificación, eliminación, importación y exportación de datos personales. Estos registros deben ser legibles, oportunos y tener un procedimiento de disposición, almacenamiento, transferencia, destrucción una vez que los registros ya no sean útiles y generarse y/o ejecutarse de manera periódica. Dichos registros deben conservarse por un periodo mínimo de dos (2) años. Los registros de interacción lógica correspondientes a trazabilidad de las acciones realizadas por los operadores de los sistemas empleados para realizar el tratamiento de los datos personales deben generarse de manera continua y deben encontrarse disponibles de manera inmediata.
4	Las medidas de seguridad que impidan al personal no autorizado la generación de copias o la reproducción de documentos digitales que contengan datos personales. En el caso de uso de sistemas, aplicaciones de mensajería instantánea, uso de cuentas de correo electrónico y/o redes sociales no institucionales, estos deben ser debidamente aprobados y formalmente establecidos, a efectos de evitar generar riesgos y transferencias no autorizadas de datos personales.

16.24. En caso de que el servicio objeto del presente contrato sea calificado como un servicio de tipo Software as a Service (SaaS), EL ENCARGADO deberá acreditar y mantener vigente durante toda la vigencia del contrato, la certificación ISO/IEC 27001, PCI-DSS u otro estándar de seguridad de información equivalente o superior, que deberá ser previamente aprobado por EL BANCO.

16.25. EL ENCARGADO deberá evaluar al menos una vez al año la eficacia de los controles de seguridad implementados, documentando los resultados y planes de mejora. La evaluación deberá estar documentada y encontrarse a disposición de EL BANCO.

16.26. Independientemente de lo señalado en la presente cláusula referente a "Obligaciones de Seguridad", EL ENCARGADO deberá garantizar, en todo momento y durante la vigencia del contrato, las medidas de seguridad adecuadas para cautelar los datos personales que

EL BANCO le proporcione, así como aquellos generados o recopilados en el marco del presente Contrato.

**OBLIGACIONES PARA LA NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE DATOS PERSONALES:**

16.27. EL ENCARGADO informará de forma inmediata a EL BANCO a través de los correos electrónicos [seguridad-digital@bn.com.pe](mailto:seguridad-digital@bn.com.pe) y [proteccion.datos.personales@bn.com.pe](mailto:proteccion.datos.personales@bn.com.pe) sobre cualquier incidente de seguridad de los datos personales, que sean detectados o respecto de los cuales exista sospecha fundada de que los sistemas, soportes o datos hayan sido comprometidos o utilizados sin autorización, así como de cualquier vulneración o sospecha de vulneración que pueda ocasionar la destrucción, pérdida, alteración ilícita, comunicación o exposición no autorizada de dichos datos personales.

16.28. EL ENCARGADO deberá proporcionar un informe de auditoría del incidente a EL BANCO que identifique la causa del incidente e incluya revisiones forenses de las violaciones de la seguridad de los datos personales a su cargo y toda la evidencia documentada. El informe deberá ser remitido en un plazo no mayor de veinticuatro (24) horas de identificado el incidente o de haber tenido la sospecha fundada de la ocurrencia y deberá contener, como mínimo, la información establecida en el artículo 34° numeral 2 del Reglamento de Protección de Datos Personales, así como aquella requerida en los formularios y formatos oficiales aprobados por las autoridades correspondientes.

16.29. En caso EL ENCARGADO no pueda entregar toda la información en el plazo señalado en la cláusula anterior, deberá entregarla de manera progresiva, asumiendo EL ENCARGADO toda responsabilidad por la demora en la entrega.

16.30. EL ENCARGADO mantendrá una bitácora actualizada de incidentes y reportará semestralmente a EL BANCO los eventos registrados, indicando medidas de mitigación y estado de cierre.

**OBLIGACIONES PARA EL EJERCICIO DE DERECHOS DE LOS TITULARES DE DATOS PERSONALES**

16.31. EL ENCARGADO recibirá cualquier solicitud de ejercicio de derechos de acceso, rectificación, cancelación, oposición, portabilidad o revocatoria y deberá trasladarlo a EL BANCO en un plazo no mayor a un (01) día hábil de recibido, a través del siguiente correo: [proteccion.datos.personales@bn.com.pe](mailto:proteccion.datos.personales@bn.com.pe) para que este pueda brindar la atención correspondiente.

16.32. EL ENCARGADO deberá notificar al solicitante del traslado al que se refiere el numeral anterior, el mismo día en que esta se realice.

16.33. EL ENCARGADO llevará un registro actualizado de las solicitudes recibidas y las fechas de traslado a EL BANCO.

**OBLIGACIONES PARA EL USO DE INTELIGENCIA ARTIFICIAL**

16.34. Cuando EL ENCARGADO utilice inteligencia artificial para procesar datos personales proporcionados por EL BANCO o generados o recopilados como parte del servicio, se obliga a cumplir con la Ley N° 31814 y su Reglamento aprobado mediante Decreto

Supremo N° 115-2025-PCM y demás normas conexas, complementarias, modificatorias y/o sustitutorias.

16.35. EL ENCARGADO comunicará al EL BANCO de forma inmediata, bajo responsabilidad, cuando utilice inteligencia artificial para procesar datos personales que han sido proporcionados, así como aquellos generados o recopilados con motivo de la prestación del servicio contratado.

16.36. EL ENCARGADO se encuentra prohibido de usar sistemas basados en inteligencia artificial calificados como de uso indebido según la normativa vigente.

16.37. EL ENCARGADO deberá garantizar que los sistemas basados en inteligencia artificial usados sean auditables, trazables y explicables, y que no generen sesgos o tratamientos discriminatorios

#### **OBLIGACIONES SOBRE REVISIONES Y/O AUDITORÍAS**

16.38. EL BANCO directamente o a través de terceros contratados, podrá, en cualquier momento, de forma presencial o electrónica revisar o auditar a EL ENCARGADO sobre las medidas de seguridad aplicadas en cumplimiento de la Ley de Protección de Datos Personales, su reglamento, directivas y demás normas conexas, complementarias, modificatorias y/o sustitutorias. De comprobarse algún incumplimiento por parte de EL ENCARGADO, se enviará previamente una comunicación informando dicha situación, otorgándole un plazo para su cumplimiento. De persistir el incumplimiento EL BANCO podrá, de considerarlo necesario, interponer las acciones legales a que hubiera lugar, sin perjuicio de tener la facultad de proceder con la resolución del presente contrato de forma automática y de pleno derecho, conforme al artículo 1430 del Código Civil. EL ENCARGADO será responsable por cualquier perjuicio que se cause a EL BANCO como consecuencia directa e indirecta del incumplimiento de cualquiera de las obligaciones que se desprenden de la presente cláusula.

16.39. Las auditorías e inspecciones se podrán realizar en cualquier local donde exista información, archivos o datos de EL BANCO o se preste el servicio, incluidas las sedes de EL ENCARGADO.

16.40. Las auditorías se efectuarán previa notificación a EL ENCARGADO y con un preaviso de cinco (5) días naturales, salvo que EL BANCO comunique a EL ENCARGADO circunstancias de urgencia en las que prevalecerá un preaviso inferior determinado a tal efecto por EL BANCO.

16.41. En ningún caso el hecho de que EL BANCO haya realizado una auditoría a EL ENCARGADO liberará a este último de la responsabilidad del cumplimiento de sus obligaciones ante autoridades y terceros que se puedan haber visto afectados con el incumplimiento.

#### **OBLIGACIONES PARA LA ENTREGA Y SUPRESIÓN DE DATOS PERSONALES**

16.42. Al finalizar el contrato, EL ENCARGADO queda obligado a entregar la información sobre los datos personales que fue proporcionado EL BANCO, generado o recopilado en el marco del presente contrato por EL BANCO.

16.43. Cuando EL ENCARGADO realice la entrega de los datos personales debe cumplir con eliminar todos los datos personales proporcionados por EL BANCO, así como los generados o recopilados en el marco del presente contrato, y suprimirá de forma segura las copias existentes, acreditando la eliminación a través de un certificado de destrucción (mediante técnicas de borrado seguro o destrucción física certificada) del banco de datos.

16.44. El ENCARGADO puede conservar una copia de los datos, una vez culminado el contrato, con los datos debidamente bloqueados e informando de ello a EL BANCO mientras puedan derivarse responsabilidades de la ejecución de la prestación como máximo dos (2) años. La apertura solo será autorizada por EL BANCO o autoridad competente.

#### **OBLIGACIONES DE EL BANCO COMO RESPONSABLE DEL TRATAMIENTO:**

16.45. EL RESPONSABLE DEL TRATAMIENTO asegura que tiene el consentimiento de los titulares de los datos personales contenidos en los bancos de datos personales que se le entregan en encargo a EL ENCARGADO, o que estos datos se encuentran en alguna de las excepciones establecidas en el art. 14 de la Ley de Protección de Datos Personales.

16.46. EL BANCO se obliga a proporcionar a EL ENCARGADO el acceso a los bancos de datos necesarios en el marco del presente contrato.

#### **RESOLUCIÓN DEL CONTRATO**

16.47. El incumplimiento de cualquiera de las obligaciones de EL ENCARGADO mencionadas en la presente cláusula sobre Protección de Datos Personales podrá ser causal de resolución del contrato de forma automática y de pleno derecho, conforme al artículo 1430 del Código Civil.

#### **CLÁUSULA DÉCIMO SÉTIMA: LEY APLICABLE Y SOLUCIÓN DE CONTROVERSIAS**

El presente CONTRATO se encuentra sujeto a las disposiciones de la Ley N° 26702, el Código Civil y a cualquier otra disposición vigente que resulte aplicable.

Todo litigio, controversia, desavenencia, reclamación o interpretación resultante, o relacionada o derivada de este Contrato o que guarde relación con él, incluidas las relativas a su nulidad, validez, eficacia o terminación incluso las del convenio de arbitraje serán resueltas mediante conciliación y/o arbitraje de Derecho ante la Cámara de Comercio de Lima, de conformidad con los reglamentos de dicho Centro.

Si la conciliación concluyera por inasistencia de una o ambas partes, con un acuerdo parcial o sin acuerdo, las partes se someterán a un Arbitraje de Derecho para que resuelvan las controversias definitivamente. No es obligatoria la conciliación previa al Arbitraje.

El arbitraje antes referido tendrá las siguientes características y regulaciones:

- ✓ El arbitraje será de derecho e institucional, bajo la administración de la Cámara de Comercio de Lima, a cuyos reglamentos y estatutos las partes acuerdan someterse en forma expresa e irrevocable. El arbitraje será en Lima y en idioma español, y bajo las leyes peruanas.
- ✓ En caso de que el monto de la cuantía de la solicitud de arbitraje sea menor a 50 (cincuenta) Unidades Impositivas Tributarias - UIT, vigentes a la fecha de la solicitud, la controversia será resuelta por Árbitro Único designado por la Cámara de Comercio de Lima.
- ✓ En caso de que el monto de la cuantía de la solicitud de arbitraje sea mayor o igual a 50 (cincuenta) Unidades Impositivas Tributarias - UIT, vigentes a la fecha de la solicitud, la

controversia será resuelta por un Tribunal compuesto por tres (03) árbitros.

- ✓ Cada parte interviniente designará un árbitro y los dos árbitros designados escogerán al Presidente del Tribunal, a falta de acuerdo de los dos árbitros para escoger al Presidente, éste será designado por la Cámara de Comercio de Lima.
- ✓ Las partes acuerdan que respecto a los honorarios de los árbitros y del Presidente del Tribunal Arbitral, cada parte interviniente asumirá el costo de los honorarios del Árbitro que designe y además asumirá el 50% de los honorarios del Presidente del Tribunal Arbitral, de darse el caso, salvo el referente a los honorarios de los abogados que serán asumidos por cada una de **LAS PARTES**.
- ✓ El laudo arbitral emitido obligará a las partes y pondrá fin al procedimiento de manera definitiva, siendo el mismo inapelable ante el Poder Judicial o cualquier instancia administrativa, tiene el valor de cosa juzgada y se ejecutará como una sentencia. Queda perfectamente entendido que las partes no le confieren al Tribunal o al Árbitro Único la posibilidad de ejecutar el laudo.

En el caso que las partes o el árbitro tuvieran que recurrir al Poder Judicial, queda establecido que, en estos casos, serán competentes los jueces y tribunales del distrito judicial de Lima, Perú, renunciando las Partes al fuero de los jueces que les pudiera corresponder por razón de su domicilio.

Queda entendido que los acuerdos contenidos en la presente Cláusula sobrevivirán a la terminación o resolución del presente Contrato y serán aplicables a cualquier conflicto que pudiera generarse entre las partes con relación al presente Contrato y los derechos y obligaciones que se deriven de éste, incluyendo los conflictos derivados o relativos a su extinción, salvo acuerdo distinto y posterior de las partes.

**CLÁUSULA DÉCIMO OCTAVA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL**

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE EL BANCO: Av. Javier Prado Este N° 2499 San Borja - Lima

DOMICILIO DEL PROVEEDOR: .....

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases integradas, la propuesta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de Lima a los ..... del mes de ..... del año 2026.


  
\_\_\_\_\_  
EL BANCO

  
\_\_\_\_\_  
EL BANCO

  
\_\_\_\_\_  
EL PROVEEDOR

**ANEXO N° 001**

**Términos de Referencia**



**ANEXO N° 002**

**Propuestas Técnica y Económica de EL PROVEEDOR**

4

○ M

○

TA

K

el

# Formatos

H

## Formato N° 1

### DECLARACIÓN JURADA DE DATOS DEL POSTOR

**Señores**  
**COMITÉ DEL CONCURSO DE MERITOS**  
**Concurso de Méritos N° 0004-2026-BN**  
**Presente.-**

El que se suscribe, [.....], Representante Legal de [.....], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de en la Ficha N° [.....] Asiento N° [.....], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Razón Social :		
Domicilio Legal :		
RUC :	Teléfono(s) :	
Correo electrónico :		

#### **Autorización de notificación por correo electrónico:**

... [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la propuesta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o  
Representante legal, según corresponda**

Importante

**La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada.**



Concurso de Méritos N° 0004-2026-BN  
 Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

Importante
<b>Cuando se trate de consorcios, la declaración jurada es la siguiente:</b>

**Formato N° 1**

**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

**Señores  
 COMITÉ DEL CONCURSO DE MERITOS  
 Concurso de Méritos N° 0004-2026-BN  
 Presente.-**

El que se suscribe, [...], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Datos del consorciado 1			
Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s):		
Correo electrónico:			

Datos del consorciado 2			
Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s):		
Correo electrónico:			

Datos del consorciado ...			
Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s):		
Correo electrónico:			

**Autorización de notificación por correo electrónico:**

Correo electrónico del consorcio:

..... [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la propuesta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.



Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del representante  
común del consorcio**



Importante

*La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada.*



## Formato N° 2

### DECLARACIÓN JURADA DE CUMPLIR REQUISITOS PARA SER POSTOR

**Señores**  
**COMITÉ DEL CONCURSO DE MERITOS**  
**Concurso de Méritos N° 0004-2026-BN**  
**Presente.-**

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el proceso de concurso de méritos ni para contratar con el Estado.
- iii. Que mi información (en caso de que el postor sea persona natural) o la información de la persona jurídica que represento, se encuentra actualizada.
- iv. Conocer las sanciones contenidas en la Ley General de Contrataciones Públicas y su Reglamento, así como las disposiciones aplicables del TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- v. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- vi. Conocer, aceptar y someterme a las bases, condiciones y reglas del proceso de concurso de méritos.
- vii. Ser responsable de la veracidad de los documentos e información que presento en el presente proceso de concurso de méritos.
- viii. Comprometerme a mantener la propuesta presentada durante el proceso de concurso de méritos y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o  
Representante legal, según corresponda**

Importante

***En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.***

**Formato N° 3**

**DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TERMINOS  
DE REFERENCIA: REQUISITOS, CARACTERISTICAS Y  
CONDICIONES TECNICAS**

Señores  
**COMITÉ DEL CONCURSO DE MERITOS**  
Concurso de Méritos N° 0004-2026-BN  
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del proceso de concurso de méritos de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribê ofrece el **Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente**, de conformidad con los requisitos, características y condiciones técnicas que se indican en Anexo N° 01 - Términos de Referencia de las bases; así como; los documentos derivados del proceso de concurso de méritos que establezcan obligaciones para las partes.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o  
Representante legal o común, según corresponda**



### Formato N° 4

## DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores  
**COMITÉ DEL CONCURSO DE MERITOS**  
Concurso de Méritos N° 0004-2026-BN  
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del proceso de concurso de méritos de la referencia, me comprometo a prestar el servicio objeto del presente proceso de concurso de méritos en el plazo:

1. El plazo de ejecución del **Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente** será de cuarenta y cuatro (44) meses y dos (2) semanas el concordante al detalle presentado en el numeral 1.3.3 Lugar y Plazo de la Prestación del Servicio, subnumeral 1.3.3.2 Plazo, del Capítulo I de la presente bases.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o  
Representante legal o común, según corresponda**

## Formato N° 5

### PROMESA DE CONSORCIO

(Sólo para el caso en que un consorcio se presente como postor)

Señores  
**COMITÉ DEL CONCURSO DE MERITOS**  
**Concurso de Méritos N° 0004-2026-BN**  
**Presente.-**

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el proceso de concurso de méritos, para presentar una propuesta conjunta al **CONCURSO DE MERITOS N° 0004-2026-BN**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, bajo las siguientes condiciones:

a) Integrantes del consorcio

1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al proceso de concurso de méritos, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

c) Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

d) Fijamos nuestro domicilio legal común en [.....].

e) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] : % ]<sup>1</sup>  
[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]
2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] : % ]<sup>2</sup>  
[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

**TOTAL OBLIGACIONES** **100 %]**<sup>3</sup>

<sup>1</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>2</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>3</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

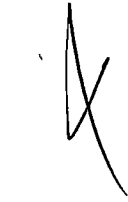
[CONSIGNAR CIUDAD Y FECHA]

.....  
**Consoiciado 1**  
**Nombres, apellidos y firma del**  
**Consoiciado 1 o de su**  
**Representante Legal**  
**Tipo y N° de Documento de**  
**Identidad**

.....  
**Consoiciado 2**  
**Nombres, apellidos y firma del**  
**Consoiciado 2 o de su**  
**Representante Legal**  
**Tipo y N° de Documento de**  
**Identidad**

Importante

***Las firmas de los integrantes del consorcio deben ser legalizadas.***









**Formato N° 7**

**DECLARACIÓN JURADA DE REORGANIZACION SOCIETARIA**

**Señores**  
**COMITÉ DEL CONCURSO DE MERITOS**  
**Concurso de Méritos N° 0004-2026-BN**  
**Presente.-**

Mediante el presente el suscrito, Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] absorbida como consecuencia de una reorganización societaria, no se encuentra sancionada.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o  
Representante legal, según corresponda**



**Formato N° 8**

**PROPUESTA ECONOMICA**

Señores  
**COMITÉ DEL CONCURSO DE MERITOS**  
Concurso de Méritos N° 0004-2026-BN  
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi propuesta económica para el **Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente** es la siguiente:

**a) Implementación del Servicio**

Componentes del Servicio de Implementación	Costo (US\$. inc. IGV)
Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de débito Visa	
Implementación/configuración del servicio de generación y validación de CVV2 Dinámico para tarjetas de crédito Mastercard	
<b>Costo del Servicio de Implementación (US\$. inc. IGV)</b>	

**b) Servicios Transaccionales**

Rango	N° de PAN Activos	Costo Unitario por PAN Activo (US\$. inc. IGV)	Demanda Mensual Estimada de PAN Activos Año 1	Demanda Mensual Estimada de PAN Activos Año 2	Demanda Mensual Estimada de PAN Activos Año 3	Requerimiento Total Estimado del Servicio	Costo (US\$. inc. IGV)
1	De 1 hasta 200,000		200,000	-	-	2,400,000	
2	De 200,001 hasta 1,000,000		-	350,000	500,000	10,200,000	
3	De 1,000,001 hasta 3,000,000		-	-	-	-	-
4	Más de 3,000,000		-	-	-	-	-
<b>Costo del Servicio Transaccional (US\$ inc. IGV)</b>							

**Nota:** Deberá registrarse los Costos Unitarios por PAN Activo para cada uno de los Rangos establecidos.

**c) Servicio de Soporte Técnico**

Descripción del Servicio	Costo Mensual (US\$. inc. IGV)	Costo (36 meses) (US\$. inc. IGV)
Servicio de Soporte Técnico		
<b>Costo del Servicio de Soporte Técnico (US\$. inc. IGV)</b>		

Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No  
Presente

<b>Costo Total del Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente (US\$. inc. IGV)</b>	
---	--

**Nota:** El Costo Total del Servicio = a) + b) + c)

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o  
Representante legal o común, según corresponda**

Importante

- ***El postor que goce de alguna exoneración legal debe indicar que su propuesta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:***

***Mi propuesta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN].***

A  
M



Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

**Formato N° 9**

**AUTORIZACIÓN DE NOTIFICACIONES DE LA ENTIDAD (BANCO DE LA NACION) DURANTE LA EJECUCION CONTRACTUAL MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN**

**(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)**

**Señores  
BANCO DE LA NACION  
Presente.-**

El que se suscribe, [.....], Representante Legal de [.....], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo al Banco de la Nación que se me notifique al correo electrónico: ..... [INDICAR EL CORREO ELECTRÓNICO], las notificaciones que se realicen durante la etapa de ejecución del contrato suscrito entre ambas partes.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o Representante legal, según corresponda**



Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

### Formato N° 10

## DECLARACIÓN JURADA RESOLUCIÓN SBS N° 2660-2015 - REGLAMENTO DE GESTIÓN DE RIESGOS DE LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO

Señores  
**BANCO DE LA NACIÓN**  
Presente.-

[CONSIGNAR NOMBRE DE LA EMPRESA], con Registro Único de Contribuyentes N° [CONSIGNAR], con domicilio legal en [CONSIGNAR], distrito de [CONSIGNAR], provincia y departamento de [CONSIGNAR], debidamente representada por su apoderado, el señor [CONSIGNAR], identificado con Documento de Identidad N° [CONSIGNAR], cuyo poder obra inscrito en la Partida Electrónica N° [CONSIGNAR], del Registro de Personas Jurídicas de [CONSIGNAR], declaro bajo juramento:

Conocer que EL BANCO DE LA NACIÓN es una Entidad Financiera sujeta al cumplimiento del Reglamento de Gestión de Riesgos de Lavado de Activos y del Financiamiento del Terrorismo, aprobado por Resolución SBS N° 2660-2015, y que por tanto no obligamos a proporcionar toda aquella información necesaria a fin de dar cumplimiento a lo dispuesto en los artículos 36° y 37° del referido Reglamento; así como, a cualquier otra norma legal sobre la materia desde su entrada en vigencia, para lo cual cumpla con presentar la siguiente información requerida para la firma del contrato, la misma que se detalla:

Por el presente documento, declaro bajo juramento, lo siguiente:

#### PERSONA JURÍDICA:

1	Denominación o razón social:			
2	Número de RUC:	Número de Registro equivalente, para no domiciliados:		
3	Dirección de la oficina o local principal donde desarrolla las actividades propias del negocio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto.- Int. N° /Urb. - Complejo - Zona - Sector /Distrito/Provincia/Departamento):			
4	Rubros en los que el proveedor brinda sus productos o servicios:			
5	Años de experiencia en el mercado:			
6	N° de Teléfono:			
7	Se encuentra incluida en los listados que contribuyen a la prevención LA/FT - Anexo N° 01 de la Resolución SBS N° 2660-2015: SI <input type="checkbox"/> - NO <input type="checkbox"/>			
<b>Representante legal:</b>				
Nombres y Apellidos:				
Tipo y número de documento de identidad (marque con una "X" según corresponda).				
DNI ( )		Pasaporte ( )		Carné de Extranjería ( )
Otro (Indique):				
8	Se encuentra incluida en los listados que contribuyen a la prevención LA/FT - Anexo N° 01 de la Resolución SBS N° 2660-2015: SI <input type="checkbox"/> - NO <input type="checkbox"/>			
Cuenta con antecedentes penales ( )		No contar con antecedentes penales ( )		
¿Es una persona políticamente expuesta (PEP)? SI <input type="checkbox"/> - NO <input type="checkbox"/>				

<b>Identificación de los accionistas, socios o asociados, que tengan directa o indirectamente más del 25% del capital social, aporte o participación de la persona jurídica. Respecto de cada uno de ellos, se debe indicar:</b>			
<b>En caso el accionista, socio o asociado sea persona natural:</b>			
Nombres, Apellidos y porcentaje del capital social:		Nombres, Apellidos y porcentaje del capital social:	
1.		1.	
2.		2.	
Tipo y número de documento de identidad (marque con una "X" según corresponda).			
DNI ( )	Pasaporte ( )	Carné de Extranjería ( )	Otro (Indique):
1.	1.	1.	1.
2.	2.	2.	2.
Se encuentran incluidos en los listados que contribuyen a la prevención de Lavado de Activos: SI <input type="checkbox"/> NO <input type="checkbox"/>			
De marcar SI, detallar Nombre y Apellidos de dicho (s) accionista (s), socio (s) o asociado (s), que se encuentra en los Listados que contribuyen a la prevención de Lavado de Activos,			
¿Es una persona políticamente expuesta (PEP)?			
SI <input type="checkbox"/> NO <input type="checkbox"/>			
De marcar Si, detallar Nombre y Apellidos de dicho (s) accionista (s), socio (s) o asociado (s), que se constituyen en PEP.			
1.			
2.			
<b>En caso el accionista, socio o asociado sea persona jurídica:</b>			
Denominación o razón social:			
Porcentaje del Capital Social:			
Número de RUC:		Número de Registro equivalente, para no domiciliados:	
<i>En este caso, se debe identificar a la persona natural que desempeña funciones de dirección y/o gestión sobre el accionista, socio o asociado, debiendo indica (persona natural que desempeñe funciones de dirección y/o gestión:</i>			
<i>- Nombres y Apellidos:</i>			
<i>- Tipo y número de documento de identidad (DNI, Pasaporte, Carné de Extranjería, u otro):</i>			
¿Es una persona políticamente expuesta (PEP)? SI <input type="checkbox"/> - NO <input type="checkbox"/>			
Tanto de la persona jurídica y natural se encuentran incluida en las listas que contribuyen a la prevención del Lavado de Activos - Anexo N° 01 de la Resolución SBS 2660-2015: SI <input type="checkbox"/> - NO <input type="checkbox"/>			
Afirmo y ratifico todo lo manifestado en la presente declaración jurada y me comprometo a presentarla cada dos (02) años de ejecución contractual		<b>NOMBRE:</b>	
		<b>FIRMA:</b>	
		<b>FECHA (día/mes/año):</b> /      /	
<b>*Importante:</b>			
- Cuando se trate de consorcios, la presente Declaración Jurada debe ser presentada por cada uno de los integrantes del consorcio.			
- La información debe ser completada en su totalidad.			
- Todas las hojas de la presente declaración jurada deber estar visadas.			
- Las Personas Expuestas Políticamente (PEP) son las personas naturales, nacionales o extranjeras, que cumplen o que en los últimos dos (2) años han cumplido funciones públicas destacadas o funciones prominentes en una organización internacional, sea en el territorio nacional o extranjero, y cuyas circunstancias financieras puedan ser objeto de interés público. Asimismo, se considera como PEP al colaborador directo de la máxima autoridad de la institución.			
En el caso de ser un PEP la persona natural relacionada al proveedor, se debe completar el Formato "Formulario de Persona Expuesta Políticamente - PEP".			

4

Ad

Por el presente documento, declaro bajo juramento, lo siguiente:

PERSONA NATURAL:	
1	Nombres: _____ Apellidos: _____
2	<b>Tipo y número de documento de identidad (marque con una "X" según corresponda).</b>
	DNI ( ) Pasaporte ( ) Carné de Extranjería ( ) Otro (Indique): _____ N° _____
3	Nacionalidad (en caso de extranjero): _____
4	Domicilio (Indicar: Jr. - Av. - Calle - Pasaje / N° / Dpto-Int. N° /Urb - Complejo - Zona – Sector /Distrito/Provincia/Departamento): _____
5	Rubros en los que el proveedor brinda sus productos o servicios: _____
6	Años de experiencia en el mercado: _____
7	N° Teléfono: _____ Correo electrónico: _____
8	Cuenta con antecedentes penales ( ) No cuenta con antecedentes penales ( )
9	¿Es una persona políticamente expuesta (PEP)? SI <input type="checkbox"/> - NO <input type="checkbox"/>
10	Se encuentra incluida en los listados que contribuyen a la prevención de Lavado de Activos FT – Anexo N° 01 de la Resolución SBS N° 2660-2015: SI <input type="checkbox"/> - NO <input type="checkbox"/>
Afirmo y ratifico todo lo manifestado en la presente declaración jurada y me comprometo a presentarla, de ser el caso, cada dos (02) años de ejecución contractual.	
<b>NOMBRE:</b> _____	
<b>FIRMA:</b> _____	
<b>FECHA (día/mes/año):</b> _____ / _____ / _____	
<p><b>*Importante:</b></p> <ul style="list-style-type: none"> <li>- La información debe ser completada en su totalidad.</li> <li>- Las Personas Expuestas Políticamente (PEP) son las personas naturales, nacionales o extranjeras, que cumplen o que en los últimos dos (2) años han cumplido funciones públicas destacadas o funciones prominentes en una organización internacional, sea en el territorio nacional o extranjero, y cuyas circunstancias financieras puedan ser objeto de interés público. Asimismo, se considera como PEP al colaborador directo de la máxima autoridad de la institución.</li> </ul> <p><i>En el caso de ser un PEP la persona natural relacionada al proveedor, se debe completar el Formato "Formulario de Persona Expuesta Políticamente - PEP".</i></p>	

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o Representante legal, según corresponda**

### Formato N° 11

#### FORMATO DE DECLARACIÓN JURADA DE NO ENCONTRARSE INSCRITO EN EL REGISTRO DE DEUDORES DE REPARACIONES CIVILES (REDERECI)

Señores  
**BANCO DE LA NACIÓN**  
Presente.—

Yo [CONSIGNAR NOMBRES Y APELLIDOS COMPLETOS] identificado con documento de identidad N° [CONSIGNAR NÚMERO DE DNI O DOCUMENTO DE IDENTIDAD ANÁLOGO], domiciliado en [CONSIGNAR EL DOMICILIO LEGAL], representante legal del postor [CONSIGNAR EL NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL POSTOR], declaro no encontrarme inscrito en el Registro de Deudores de Reparaciones Civiles (REDERECI) y, por lo tanto, de no contar con ninguno de los impedimentos establecidos en el artículo 5º de la Ley N° 30353 (Ley que crea el Registro de Deudores de Reparaciones Civiles - REDERECI) para acceder al ejercicio de la función pública y contratar con el Estado.

En caso de resultar falsa la información que proporciono, me sujeto a los alcances de lo establecido en el artículo 411 del Código Penal, concordante con el artículo 34 del Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por el Decreto Supremo N° 004-2019-JUS.

En mérito a lo expresado, firmo el presente documento.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o Representante legal o común, según corresponda**

**<sup>9</sup> Artículo 5. Impedimento para acceder al ejercicio de la función pública y contratar con el Estado**

Las personas inscritas en el REDERECI están impedidas de ejercer función, cargo, empleo, contrato o comisión de cargo público, así como postular y acceder a cargos públicos que procedan de elección popular. Estos impedimentos subsisten hasta la cancelación íntegra de la reparación civil dispuesta.

Lo dispuesto en el párrafo anterior es inaplicable a las personas condenadas por delitos perseguibles mediante el ejercicio privado de la acción penal.



Concurso de Méritos N° 0004-2026-BN  
Servicio de Implementación de Mecanismos de Seguridad en Transacciones con Tarjeta BN (de Crédito y Débito) No Presente

## Formato N° 12

### DECLARACIÓN JURADA DE NO ESTAR INHABILITADO PARA CONTRATAR CON EL ESTADO PERUANO

**SEÑORES:**  
**BANCO DE LA NACIÓN**  
**Presente.-**

De nuestra consideración:

Mediante el presente, el/la Sr./Sra. .... identificado/a con DNI N° ..... Representante Legal de la empresa ..... con domicilio en [CONSIGNAR INFORMACION DEL CONTRATISTA PERSONA JURIDICA O NATURAL]..... con número telefónico ..... [CONSIGNAR INFORMACION DEL CONTRATISTA PERSONA JURIDICA O NATURAL] y RUC N°..... [CONSIGNAR INFORMACION DEL CONTRATISTA PERSONA JURIDICA O NATURAL]

**DECLARO BAJO JURAMENTO lo siguiente:**

1. No tener impedimento para ser postor y/o contratar con el Estado, conforme al artículo 30 de la Ley General de Contrataciones Públicas.
2. Conocer, aceptar y someterme a los términos de referencia.
3. Ser responsable de la veracidad de los documentos e información que presento a efectos del presente requerimiento.
4. Conocer las sanciones contenidas en la Ley General de Contrataciones Públicas y su Reglamento, así como en la Ley N° 27444, Ley del Procedimiento Administrativo General.

[CONSIGNAR CIUDAD Y FECHA]

.....  
**Firma, Nombres y Apellidos del postor o Representante legal o común, según corresponda**

#### Importante

Aquellos socios, accionistas, participacionistas o titulares, de vuestra empresa que tengan participación individual o conjunta superior al 30% del capital o patrimonio social en otra empresa con el mismo objeto social, deberán suscribir de manera individual la presente declaración jurada, adjuntado la ficha RUC de la empresa que forman parte, siendo vuestra empresa responsable sobre la veracidad de dicha información.

Tratándose de consorcio, la declaración jurada es presentada por cada persona natural y/o jurídica integrante del consorcio.