RESOLUCIÓN ADMINISTRATIVA
GG-08-MAYO-2025-LASMF-DO[1]
De fecha 23 de mayo de 2025

LA GERENTE GENERAL DEL BANCO CENTRAL DE NICARAGUA

(…)

RESUELVE APROBAR

El siguiente,

REGLAMENTO PARA LA APLICACIÓN DE LA NORMA DE LOS PROVEEDORES DE TECNOLOGÍA FINANCIERA DE SERVICIOS DE PAGO Y DE LOS PROVEEDORES DE SERVICIOS DE ACTIVOS VIRTUALES

CAPÍTULO I
DEFINICIONES

Artículo 1. Definición de términos. Para efectos del presente Reglamento, además de las definiciones contenidas en el Artículo 2 de la Norma de los Proveedores de Tecnología Financiera de Servicios de Pago y de los Proveedores de Servicios de Activos Virtuales, se entenderá por:

a. **Activo virtual:** es una representación digital de valor, que se puede comercializar o transferir digitalmente, y que se puede utilizar para pagos o inversiones. Los activos virtuales no incluyen representaciones digitales de moneda fíat, valores y otros activos financieros.
b. **Administración Superior del BCN:** El Presidente del Banco Central y el Gerente General del Banco Central.
c. **Adquirente:** Proveedor de tecnología financiera de servicios de pago (PSP) autorizado que, en virtud de un contrato directo con un comercio (beneficiario), procesa las transacciones de pago aceptadas por este y liquida los fondos correspondientes directamente en una cuenta de depósito o cuenta de pago que el propio adquirente mantiene a favor del comercio.
d. **Agencias:** Establecimientos comerciales o personas naturales autorizadas contractualmente por un PSP o Proveedor de servicio de activos virtuales (PSAV) para brindar acceso a sus servicios, incluyendo la recepción/entrega de fondos o activos virtuales, conforme a los procedimientos establecidos por el proveedor.

[1] Contiene reformas aprobadas mediante Resolución Administrativa GG-13-JULIO-2025-LASMF-DO, del 23 de julio del año 2025.

e. **Agregador de pagos o subadquirente:** PSP autorizado que, bajo contrato con uno o más adquirentes, ofrece a múltiples comercios acceso a esquemas de pago que ha contratado con uno o más adquirentes, suministrando para estos fines tecnología y/o dispositivos de acceso (POS, mPOS, Pasarelas de Pago Online, entre otras) y recibiendo en nombre de estos, los fondos resultantes de las órdenes de pago.
f. **Autenticación reforzada de cliente:** proceso de verificación de identidad que exige al usuario presentar al menos dos factores de autenticación independientes, preferiblemente de categorías distintas, para acceder a su cuenta o autorizar operaciones sensibles. Estas categorías son:
   i. Conocimiento (algo que el usuario sabe): por ejemplo, contraseña, PIN u otra información secreta.
   ii. Posesión (algo que el usuario posee): por ejemplo, código generado por un token físico o una app en el móvil, mensaje SMS, notificación push o llave de seguridad USB.
   iii. Inherencia (algo que el usuario es): por ejemplo, datos biométricos, dentro de los cuales, huella dactilar, reconocimiento facial, reconocimiento de voz, patrón de iris, u otros.
g. **BCN:** Banco Central de Nicaragua.
h. **Cartera digital (también denominada billetera digital, billetera electrónica o e-wallet):** plataforma accesible desde navegadores web, aplicaciones móviles, dispositivos físicos o cualquier interfaz segura utilizada para llevar a cabo pagos en línea, pagos sin contacto y/o transferencias de fondos, a través de instrumentos de pago asociados a ella que incluyen, de manera enunciativa más no limitativa, tarjetas de crédito, débito y prepagadas. Asimismo, las carteras digitales permiten almacenar y realizar transacciones u operaciones con dinero electrónico y activos virtuales.
i. **Circuito de transacciones móviles (CTM):** el conjunto integrado de instrumentos de pago, mecanismos técnicos, procedimientos operativos y normas establecidas por un PSP autorizado para emitir dinero electrónico (emisor). Este circuito permite el almacenamiento y la transferencia de dinero electrónico en tiempo real, utilizando los instrumentos de pago definidos por el emisor, y opera dentro de la red conformada por los usuarios finales, agentes y comercios afiliados al emisor. Los CTM pueden interconectarse con circuitos operados por otros proveedores autorizados para facilitar la interoperabilidad.
j. **Consejo Directivo:** Consejo Directivo Monetario y Financiero.
k. **Cuentas de Manejo de Activos Virtuales (CMAV):** Cuentas bancarias segregadas abiertas por un PSAV en bancos autorizados por SIBOIF, destinadas exclusivamente a mantener los fondos en moneda fíat recibidos de clientes para la compra de activos virtuales o resultantes de la venta de los mismos, previo a su entrega al cliente.
l. **Cuentas de Manejo de Dinero Electrónico (CMDE):** Cuentas bancarias segregadas abiertas por un PSP en bancos autorizados por SIBOIF, destinadas exclusivamente a mantener los fondos correspondientes al dinero electrónico emitido.

m. **Débito directo:** orden de pago previamente autorizada por el titular de una cuenta o tarjeta de pago, para que, con cargo a la misma, se realice una transferencia o pago recurrente de fondos a favor de un tercero beneficiario o a otra cuenta de su propiedad.
n. **Día hábil:** los días laborales para el BCN, siendo estos de lunes a viernes. Se exceptúan los feriados nacionales, asuetos de ley y aquellos asuetos decretados por la Presidencia de la República a nivel nacional o aplicables únicamente para el sector público.
o. **Dinero electrónico:** valor monetario almacenado electrónicamente, representando un crédito exigible a su emisor, emitido contra la recepción previa de fondos, aceptado como medio de pago por terceros, y registrado en dispositivos móviles, tarjetas prepagadas, carteras digitales u otros soportes electrónicos. Las características del dinero electrónico son:
    - Convertible en efectivo a la par en todo momento.
    - No constituye un depósito ni genera intereses.
    - Registrado como pasivo en la contabilidad del emisor.
    - Aceptado dentro del mismo circuito transaccional autorizado por el emisor.
p. **Incidente operativo o de seguridad:** evento adverso que compromete la disponibilidad o integridad de los servicios o sistemas, o la confidencialidad de los datos o información, de un PSP/PSAV.
q. **Infraestructura tecnológica:** conjunto integrado de recursos físicos (hardware, redes) y lógicos (software, bases de datos, aplicaciones) esenciales para las operaciones seguras de un PSP/PSAV.
r. **Instrumento de pago electrónico:** medio físico o electrónico, que permite a su poseedor o usuario iniciar órdenes de pago o transferencia de fondos. Incluye, de manera enunciativa más no limitativa, herramientas tales como: tarjetas de pago (físicas o virtuales); carteras digitales, cuando se utilizan como interfaz para instruir pagos, entre otras.
s. **LA/FT/FP:** Lavado de Activos, Financiamiento al Terrorismo y Financiamiento a la Proliferación de Armas de Destrucción Masiva.
t. **Licencia o Registro:** autorización otorgada por el BCN para operar como PSP o PSAV.
u. **Mezcladores (Mixers/Tumblers):** servicios diseñados para ofuscar el origen o destino de las transacciones de activos virtuales, combinando fondos de múltiples usuarios.
v. **Moneda fíat:** moneda de curso legal emitida por el Banco Central de Nicaragua o por la autoridad monetaria del gobierno de un país y que es utilizada y aceptada como medio legal de pago. Las monedas fíat pueden ser representadas a través de moneda digital.
w. **Monedero sin custodia (Self-hosted/Un-hosted wallet):** monedero de activos virtuales cuya clave privada es controlada directamente por el usuario y no por un tercero (como un PSAV).
x. **Norma:** Norma de los Proveedores de Tecnología Financiera de Servicios de Pago y de los Proveedores de Servicios de Activos Virtuales (Resolución CDMF-XIII-2-25).
y. **Pasarelas de pagos online:** interfaz técnica segura que conecta la plataforma de comercio electrónico de un vendedor (sitio web, aplicación móvil) con el sistema del PSP (adquirente, agregador, banco, u otro procesador autorizado) para transmitir la información necesaria y

facilitar la autorización y procesamiento de transacciones de pago electrónico, independientemente del instrumento de pago utilizado por el comprador.

z. **Proveedor de servicio de activos virtuales (PSAV):** entidad autorizada por el BCN que realiza una o más de las siguientes actividades u operaciones, para o en nombre de otra persona natural o jurídica: (i) intercambio entre activos virtuales y monedas fíat; (ii) intercambio entre una o más formas de activos virtuales, (iii) transferencia de activos virtuales; (iv) custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre activos virtuales; (v) participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual; y (vi) otros servicios de activos virtuales, autorizados por el BCN.

aa. **Proveedor de tecnología financiera de servicios de pago (PSP):** entidad autorizada por el BCN para ofrecer una o más de los siguientes servicios de pago: i) servicios de ejecución de órdenes de pago; ii) servicios de aceptación de pagos para comercios; iii) emisión y administración de dinero electrónico; iv) emisión de instrumentos de pago; v) administración de redes de cajeros automáticos; vi) servicios de compraventa e intercambio de divisas de forma electrónica; y (vii) otros servicios de pago relacionados, autorizados por el BCN.

bb. **Puntos de venta móviles (mPOS, por sus siglas en inglés):** dispositivo portátil que está enlazado a una red de pagos con el fin de procesar y registrar transacciones de pago presenciales, a través de lectores compatibles con teléfonos móviles, bluetooth, u otros medios.

cc. **Regla de viaje:** obligación para los PSAV de obtener, mantener y transmitir información del originador y beneficiario en las transferencias de activos virtuales.

dd. **Red de cajeros automáticos:** conjunto de cajeros automáticos interconectados a través de una misma plataforma de servicio, gestionados por un PSP, que permite a sus usuarios realizar en dichos equipos las transacciones habilitadas, haciendo uso de tarjetas bancarias, dispositivos móviles u otros mecanismos.

ee. **Salvaguarda:** obligación y conjunto de medidas adoptadas por un PSP/PSAV para proteger los fondos (moneda fíat o dinero electrónico) o los activos virtuales pertenecientes a sus clientes, manteniéndolos separados de los fondos propios de la entidad.

ff. **Servicios de administración de redes de cajeros automáticos:** gestión y mantenimiento de una plataforma de servicio que sustenta la operatividad de una red de cajeros automáticos.

gg. **Servicios de compraventa e intercambio de divisas de forma electrónica:** plataformas tecnológicas que permiten realizar operaciones de compraventa e intercambio de divisa y activos virtuales, utilizando aplicaciones móviles, navegadores web, o cualquier interfaz segura.

hh. **Servicios de ejecución de órdenes de pago:** servicio que permite realizar operaciones de pago instruidas por un ordenante (pagador), o por un beneficiario con autorización previa del ordenante, resultando en el movimiento de fondos desde la cuenta de pago o línea de crédito del ordenante, pudiendo estas operaciones tener carácter nacional o transfronterizo. Esto incluye, entre otros, la ejecución de débitos directos (recurrentes o no recurrentes), la ejecución de transferencias de crédito (transferencias electrónicas) iniciadas por el ordenante, y las

transferencias de fondos entre particulares (P2P) realizadas mediante plataformas electrónicas accesibles por aplicaciones móviles o interfaces digitales, operadas o gestionadas por un PSP.

ii. **Servicios de aceptación de pagos para comercios:** servicios que permiten a los comercios (beneficiarios) aceptar instrumentos de pago (como tarjetas de pago, carteras digitales, transferencias iniciadas en el punto de venta, entre otros) y recibir los fondos correspondientes por la venta de bienes o servicios. Estos servicios son provistos a los comercios finales a través de:

- Un Adquirente (actuando directamente).
- Un Agregador de Pago o Subadquirente (actuando como intermediario autorizado).

Independientemente de quién lo preste al comercio, el servicio incluye típicamente:

i. El contrato con el comercio para la aceptación de pagos.
ii. La provisión o facilitación de las soluciones técnicas de aceptación (POS, mPOS, Pasarelas de pago online, entre otras).
iii. El procesamiento de la transacción (captura, autorización, compensación).
iv. La liquidación de los fondos al comercio.

jj. **SIBOIF:** Superintendencia de Bancos y de Otras Instituciones Financieras.

kk. **Tarjetas de pago:** tarjeta de débito, crédito o prepagada, asociada o no a una cuenta bancaria, que contiene credenciales de pago y es emitida por un PSP.

ll. **Terminal de Puntos de Venta (POS, por sus siglas en inglés):** dispositivo físico o solución de software que permite a los establecimientos comerciales afiliados aceptar pagos de los titulares de instrumentos de pago electrónicos en un entorno presencial.

mm. **Transferencia de activos virtuales:** cualquier movimiento de activos virtuales fuera o hacia la plataforma del PSAV, incluyendo específicamente las transferencias entre particulares (P2P) facilitadas o ejecutadas a través de plataformas electrónicas operadas o gestionadas por dicho PSAV.

nn. **Transferencia electrónica:** transacción iniciada por medios electrónicos a través de un PSP, instruida por un ordenante (persona natural o jurídica), con el fin de poner una cantidad de dinero o de activos virtuales, a disposición de un beneficiario a través del mismo u otro PSP, independientemente de si el ordenante y el beneficiario son la misma persona.

oo. **TGR:** Tesorería General de la República.

pp. **UAF:** Unidad de Análisis Financiero.

CAPÍTULO II
LICENCIA, REGISTRO E INICIO DE OPERACIONES

Artículo 2. Solicitud y documentación para la licencia o registro como PSP o PSAV. Las personas jurídicas interesadas en obtener la licencia o el registro como Proveedor de Tecnología Financiera de Servicios de Pago (PSP) o Proveedor de Servicios de Activos Virtuales (PSAV)

presentarán al Presidente del BCN una solicitud formal acompañada, como mínimo, de los siguientes documentos:

a. Formulario de solicitud conforme al Anexo 1, debidamente completado, firmado por el representante legal, con el sello oficial de la entidad solicitante.
b. Copia razonada notarialmente del Testimonio de Escritura Pública de Constitución Social, sus estatutos y reformas (si aplican), debidamente inscrita en el Registro Público Mercantil.
c. Copia razonada notarialmente del Poder Legal otorgado al Representante Legal y Gerente General, debidamente inscrito en el Registro Público Mercantil.
d. Copia razonada notarialmente de certificación de nombramiento de Junta Directiva vigente, inscrita en el Registro Público Mercantil. En caso de que algún puesto en la Junta Directiva sea ocupado por una persona jurídica, se deberá especificar el nombre de la persona natural que la representa.
e. Certificación emitida por el órgano societario correspondiente que refleje la lista de accionistas inscritos en el Libro de Registro de Acciones, y copia razonada notarialmente de certificado de inscripción actualizado del beneficiario final de la sociedad.
f. Certificado de antecedentes judiciales y policiales del Gerente General, Representante Legal y miembros de la Junta Directiva, en los que deberá constar que no poseen antecedentes penales o policiales en los cinco (5) años previos a dicha solicitud. Estos certificados deben tener como máximo sesenta (60) días de haber sido emitidos con respecto a la fecha de recepción de la solicitud de la licencia. Cuando se trate de personas que en los últimos cinco (5) años hayan sido residentes en el exterior, el certificado de antecedentes judiciales y/o policiales deberá ser expedido por las instancias y/o por los organismos competentes extranjeros, del país o países en que haya residido, con la correspondiente autenticación o apostilla.
g. Currículum vitae documentado del Gerente General, Representante Legal y de los miembros de la Junta Directiva, adjuntando copia razonada notarialmente de sus documentos de identificación vigentes.
h. Copia certificada notarialmente del Certificado de Registro vigente como Sujeto Obligado ante la UAF, si la entidad ya estuviese operando y le correspondiera dicho registro. Están exentos del presente requisito los PSP y/o PSAV de reciente constitución o que a la fecha de inicio del trámite ante el BCN no se encuentren registrados como sujeto obligado ante la UAF, sin embargo, una vez que su solicitud de registro o licencia sea autorizada, deberán presentar al BCN copia certificada notarialmente del certificado de registro ante la UAF, en un plazo no mayor a quince (15) días hábiles posteriores a la emisión de este.
i. Plan de negocio detallado, elaborado conforme a los requisitos mínimos establecidos en el artículo 10 del presente Reglamento.
j. Comprobante de haber depositado en el BCN, el diez por ciento (10%) del capital social inicial mínimo exigible conforme al Artículo 6 de la Norma.
k. Cualquier otra información o documentación que el BCN considere necesaria para evaluar la solicitud durante el proceso.

Excepciones

1. Los bancos sujetos a la supervisión de la SIBOIF sólo presentarán los documentos señalados en los literales a), c) e i), y copia certificada de la autorización para operar emitida por la SIBOIF.
2. Las instituciones de microfinanzas supervisadas por la CONAMI están exentas de presentar los requisitos f) y j) y además adjuntarán copia certificada de su registro ante esta.
3. Cuando un proveedor que ya posea licencia o registro como PSP solicite licencia o registro adicional como PSAV, o viceversa, bastará con presentar los documentos indicados en los literales a) e i) del presente artículo.
   Cuando la nueva licencia conlleve un incremento en el capital social mínimo pagado exigido conforme al Artículo 6 de la Norma, los proveedores distintos de los bancos supervisados por la SIBOIF deberán acreditar el cumplimiento del capital de la siguiente manera:
   i. Si el capital social pagado actual de la entidad, reflejado en sus últimos estados financieros (auditados o certificados por contador público autorizado, según corresponda) que hayan sido presentados previamente al BCN o se adjunten a la solicitud, es igual o superior al nuevo capital social mínimo requerido, se deberá presentar una certificación emitida por un contador público autorizado que confirme esta situación, haciendo referencia expresa a dichos estados financieros y al cumplimiento del requisito de capital establecido en el Artículo 6 de la Norma.
   ii. Si se requiere un aumento del capital social pagado para alcanzar el nuevo capital social mínimo exigido, se deberá presentar certificación del acta de la junta general de accionistas donde conste el acuerdo de incremento de capital, acompañada de una certificación de contador público autorizado que acredite el efectivo desembolso de los aportes.

Artículo 3. Evaluación, plazos y efectos de la solicitud.

1. **Revisión técnica.** Recibida la solicitud completa, las áreas técnicas del BCN verificarán el cumplimiento de los requisitos legales y normativos, evaluarán la idoneidad del solicitante y la viabilidad del proyecto, y emitirán un dictamen técnico. Durante el proceso de evaluación, el BCN podrá requerir información adicional y realizar verificaciones in situ. Si el solicitante no subsana los requerimientos en el plazo otorgado, la solicitud será denegada y, para reiniciar el trámite, deberá presentarse una nueva solicitud.
2. **Resolución.** El dictamen técnico será elevado a la Administración Superior del BCN, la cual resolverá sobre el otorgamiento o denegación de la licencia o registro en un plazo máximo de noventa (90) días hábiles contados desde la recepción de la solicitud completa. Este plazo se suspenderá mientras el solicitante atienda los requerimientos de información.

3. **Depósito inicial.** a) Si la solicitud se deniega, el diez por ciento (10 %) del depósito indicado en el literal j) del artículo 2 se transferirá a la TGR y el saldo será devuelto al solicitante. b) Si el solicitante desiste voluntariamente, el cincuenta por ciento (50 %) de dicho depósito se transferirá a la TGR y el saldo será devuelto.

Artículo 4. Autorización de inicio de operaciones.

1. **Plazo para la solicitud.** El PSP o PSAV al que se le haya otorgado licencia o registro, dispondrá de un plazo máximo de doscientos cincuenta (250) días, contados desde la entrada en vigencia de la licencia, para solicitar al Presidente del BCN la autorización de inicio de operaciones.
2. **Requisitos mínimos.** La solicitud se acompañará, según corresponda al servicio o actividad autorizada, de:
   a. Balance general de apertura suscrito por el Representante Legal y contador público autorizado.
   b. Copia certificada notarialmente del nombramiento del Gerente General (o ejecutivo principal). Si fue entregada en la solicitud, no deberá entregarse nuevamente.
   c. Listado de funcionarios principales con cargos y datos de contacto.
   d. Acreditación del cumplimiento de requisitos tecnológicos establecidos en el artículo 11 del presente Reglamento, mediante un Informe de Cumplimiento Tecnológico emitido por un tercero independiente y cualificado.
      Este informe deberá, como mínimo:
      i. verificar y certificar el cumplimiento por parte del PSP/PSAV de cada uno de los requisitos aplicables del artículo 11 (incluyendo, de manera específica, la forma en que se gestionan los riesgos y se cumplen los requisitos relativos al uso de servicios en la nube o proporcionados por terceros, cuando aplique), siendo específico para la plataforma y los servicios para los cuales se solicita la autorización de inicio de operaciones.
      ii. describir detalladamente la metodología, el alcance de la evaluación y las pruebas realizadas por el tercero (que podrán incluir auditorías de sistemas, pruebas de penetración, análisis de vulnerabilidades, revisión de configuraciones, entre otras pertinentes).
      iii. identificar cualquier hallazgo, desviación o incumplimiento, y presentar evidencia de las acciones correctivas implementadas satisfactoriamente por el PSP/PSAV para su subsanación.
      iv. incluir la documentación que acredite la independencia, la experiencia comprobada, y las certificaciones profesionales o capacitación especializada relevantes del tercero evaluador (ya sea una firma o profesionales individuales) para realizar este tipo de evaluaciones tecnológicas y de ciberseguridad.

Adicionalmente, o de forma complementaria al Informe de Cumplimiento Tecnológico, el PSP/PSAV podrá presentar:

i. Certificaciones: certificados vigentes y directamente aplicables a componentes particulares de su plataforma o servicios, emitidos por organismos reconocidos, que cubran aspectos puntuales de los requisitos del artículo 11.
ii. Mecanismos alternativos para requisitos puntuales: en situaciones debidamente justificadas por el PSP/PSAV y sujetas a la evaluación y aceptación del BCN, propuestas de controles o evidencias alternativas que demuestren de manera concluyente el cumplimiento de requisitos específicos del artículo 11, cuando la naturaleza del requisito o de la solución tecnológica implementada así lo amerite, asegurando un nivel de mitigación de riesgos que el BCN considere adecuado.

e. Contar con los siguientes documentos o sus equivalentes aprobados por su junta directiva:
   i. Plan de continuidad del negocio y de recuperación ante desastres, con objetivos de tiempo y punto de recuperación (RTO/RPO) definidos para los servicios críticos.
   ii. Plan de respaldo y recuperación de información.
   iii. Política de atención al cliente (incluye gestión de quejas y reclamos).
   iv. Política de seguridad de la información y ciberseguridad.
   v. Política de privacidad y protección de datos personales.
   vi. Procedimiento para gestión de incidentes de seguridad.
f. Copia certificada del Certificado de Registro ante la UAF.
g. Certificaciones de la industria de tarjetas, según corresponda, cuando la entidad administre redes de cajeros automáticos, emita instrumentos de pago electrónicos o brinde servicios de aceptación de pagos.
h. Contar con los siguientes elementos, según el tipo de servicio a prestar; todos deberán estar disponibles para verificación por parte del BCN en la forma que este disponga:
   i. una oficina principal y operativa en territorio nacional;
   ii. mecanismos de autenticación reforzada implementados y documentados, para los servicios que lo requieran;
   iii. copia de contratos de apertura de cuentas de respaldo para dinero electrónico (CMDE) o para activos virtuales (CMAV), cuando corresponda;
   iv. copia de contratos suscritos con proveedores críticos de tecnología y servicios;
   v. modelos de contratos de servicios con agencias, en caso de operar con estas; y
   vi. modelos de términos y condiciones a suscribir con los clientes finales, incluidas las tarifas aplicables y los procedimientos de reclamación.

3. **Excepciones.** Las instituciones de microfinanzas supervisadas por la CONAMI deberán acreditar únicamente los literales c), d), e), g) y h). Por su parte, los bancos supervisados por la SIBOIF deberán acreditar únicamente los literales e) y g).
4. **Verificación y decisión.** El BCN verificará el cumplimiento de los requisitos y, de encontrarlos conformes, la Administración Superior del BCN emitirá la autorización de funcionamiento dentro de los treinta (30) días hábiles siguientes a la presentación de la solicitud. De existir omisiones, el BCN notificará al solicitante y concederá un plazo para subsanarlas. El cómputo del plazo de resolución se suspenderá hasta que las omisiones sean corregidas.
5. **Consecuencias de la inacción.** Si el PSP o PSAV no presenta la solicitud de inicio de operaciones dentro del plazo de doscientos cincuenta (250) días, o presenta la solicitud, pero no cumple con los requisitos establecidos en este artículo o no subsana las omisiones señaladas dentro del plazo concedido, la licencia o registro quedará sin efecto. La Administración Superior emitirá la resolución de revocación, que se publicará en La Gaceta, Diario Oficial y en la página web del BCN.

Artículo 5. Publicación de las licencias. Otorgada la licencia, el solicitante deberá gestionar su publicación en La Gaceta, Diario Oficial, en un plazo máximo de sesenta (60) días, contados desde la notificación del otorgamiento, para que la misma surta sus efectos. Dentro de los diez (10) días hábiles siguientes a la fecha efectiva de publicación, el solicitante deberá notificar este hecho a la División de Operaciones Financieras del BCN, mediante comunicación electrónica o física, adjuntando copia de la publicación respectiva. Una vez recibida por el BCN dicha notificación con la copia de la publicación adjunta, éste procederá, en un plazo máximo de diez (10) días hábiles, a devolver al solicitante el monto correspondiente al depósito inicial referido en el literal j) del artículo 2 del presente Reglamento, cuando aplique.
La lista de entidades con licencias y registros se publicarán en la web del BCN con el detalle de los servicios.

Artículo 6. Notificaciones de las licencias y/o registros a entidades reguladoras. El BCN comunicará a la UAF el otorgamiento, cancelación o revocación de licencias o registros y las autorizaciones de inicio de operaciones otorgadas a los PSP o PSAV. Asimismo, informará tales actos a la SIBOIF y a la CONAMI cuando la entidad de que se trate esté sujeta a su supervisión.

Artículo 7. Registro de servicios adicionales.

1. **Solicitud.** El PSP o PSAV que cuente con licencia o registro y desee incorporar uno o más servicios distintos de los originalmente aprobados, deberán presentar a la División de Operaciones Financieras del BCN una carta de solicitud acompañada, como mínimo, de la siguiente información:

a. **Descripción del servicio adicional:** identificación del servicio PSP o de la actividad PSAV a ofrecer, detallando el flujo operativo de las transacciones, los instrumentos de pago o activos virtuales involucrados, los canales de distribución y la propuesta de valor diferencial para los clientes.
b. **Adecuación operativa y tecnológica:** descripción de las modificaciones en la plataforma tecnológica existente, en los procesos operativos y en la estructura organizativa; certificaciones o pruebas funcionales adicionales que resulten pertinentes; y, en su caso, actualización de los planes y procedimientos claves para el nuevo servicio.
c. **Análisis de mercado:** identificación del segmento de mercado objetivo, estimación de su tamaño y potencial, análisis de la competencia existente, estrategia de precios y tarifas, y plan de marketing y adquisición de clientes.
d. **Ajustes en el capital:** cuando la adición de un nuevo servicio conlleve un incremento en el capital social mínimo pagado exigido conforme al artículo 6 de la Norma, los proveedores distintos de los bancos supervisados por la SIBOIF deberán acreditar el cumplimiento del capital de la siguiente manera:
    i. Si el capital social pagado actual de la entidad, reflejado en sus últimos estados financieros (auditados o certificados por contador público autorizado, según corresponda) que hayan sido presentados previamente al BCN o se adjunten a la solicitud, es igual o superior al nuevo capital social mínimo requerido, se deberá presentar una certificación emitida por un contador público autorizado que confirme esta situación, haciendo referencia expresa a dichos estados financieros y al cumplimiento del requisito de capital establecido en el Artículo 6 de la Norma.
    ii. Si se requiere un aumento del capital social pagado para alcanzar el nuevo capital social mínimo exigido, se deberá presentar certificación del acta de la junta general de accionistas donde conste el acuerdo de incremento de capital, acompañada de una certificación de contador público autorizado que acredite el efectivo desembolso de los aportes.
e. **Cronograma de implementación:** plan detallado con fases, actividades clave y plazos estimados para inicio de operaciones.
f. **Otra información**: cualquier otra información o documentación que el BCN considere necesaria para evaluar la solicitud.

2. **Tramitación y plazos.** Plazos de aprobación e inicio de operaciones:

a. La Administración Superior del BCN resolverá la solicitud, basado en un informe técnico del área correspondiente del BCN, en un plazo máximo de treinta (30) días hábiles contados a partir de la recepción completa y conforme de la documentación.
b. Notificada la aprobación, el proveedor, dispondrá de doscientos cincuenta (250) días para solicitar la autorización de inicio de operaciones del servicio adicional, adjuntando evidencia de pruebas funcionales del servicio satisfactorias.

c. El BCN resolverá dicha solicitud en un plazo máximo de quince (15) días hábiles. El cómputo se suspenderá mientras el solicitante subsane omisiones.

3. **Efectos de la inacción.** Si el PSP o PSAV no presenta la solicitud de inicio de operaciones dentro del plazo de doscientos cincuenta (250) días, la aprobación del servicio adicional quedará sin efecto y el BCN emitirá la resolución de revocación correspondiente.

Artículo 8. Vigencia de la licencia y registro. Las licencias de operación y/o registro de los PSP y PSAV tendrán una vigencia indefinida.

Artículo 9. De la cesión, enajenación o transferibilidad de la licencia y/o registro. Los PSP y PSAV, no podrán ceder, transferir, enajenar u otorgar en garantía su autorización para operar.

CAPÍTULO III
PLAN DE NEGOCIO Y PLATAFORMA TECNOLÓGICA

Artículo 10. Contenido mínimo del plan de negocio. El plan de negocio al que hace referencia el literal "i" del artículo 2 del presente reglamento deberá contener de forma clara, coherente y detallada, como mínimo, los siguientes apartados:

a. **Resumen ejecutivo:** síntesis y objetivos del proyecto, descripción de los servicios que se prestarán (PSP, PSAV o ambos), mercado meta identificado y exposición de los principales indicadores financieros proyectados a cinco años.
b. **Descripción de la estructura organizativa:** organigrama de la entidad, con una explicación de las principales áreas funcionales (operaciones, tecnología, riesgos, cumplimiento, atención al cliente u otras pertinentes) y las responsabilidades generales asignadas a cada una.
c. **Modelo de negocio y servicios:** descripción precisa de cada servicio PSP o actividad PSAV solicitada, detallando el flujo operativo de las transacciones (on-boarding, autenticación reforzada, procesamiento, liquidación y conciliación), los instrumentos de pago o activos virtuales involucrados, los canales de prestación (aplicación móvil, web, POS, agencias, entre otros). Cuando se trate del servicio de aceptación de pagos para comercios, deberá describirse el proceso de liquidación de fondos al comercio y los plazos previstos; y, cuando se incluya la emisión y administración de dinero electrónico, se explicará el mecanismo de emisión, la salvaguarda de fondos en CMDE, los procedimientos de redención y los límites operativos aplicables.
d. **Análisis de mercado:** identificación del segmento de mercado objetivo, estimación de su tamaño y potencial, análisis de la competencia existente, estrategia de precios y tarifas, y plan de marketing y adquisición de clientes.
e. **Plan operativo:** detalle de los procesos operativos esenciales (verificación de clientes, procesamiento de transacciones, conciliación y gestión de reclamaciones), especificación de los

recursos humanos requeridos (perfiles y dotación mínima) y ubicación de la oficina principal y, cuando proceda, de los centros de respaldo, tomando como referencia la estructura organizativa descrita en el literal b. del presente artículo.

f. **Plan tecnológico:** documentación detallada de la arquitectura tecnológica propuesta –que incluya sistemas, bases de datos y redes de comunicación, indicando cómo se integrarán y gestionarán los servicios provistos por terceros o aquellos desplegados en la nube si forman parte de la solución tecnológica–; la especificación del software principal (indicando si es desarrollo propio, licenciado, de otra modalidad de adquisición, o consumido como un servicio en la nube); las medidas específicas de seguridad de la información y ciberseguridad que abarquen de manera integral tanto los componentes gestionados internamente como los servicios externalizados; las políticas de gestión de datos que contemplen el tratamiento y la protección de la información en entornos de terceros o en la nube; y los datos de proveedores tecnológicos clave. Si la entidad depende de manera significativa de proveedores de servicios en la nube o de terceros para funciones críticas, el plan deberá describir adicionalmente la estrategia general para la selección y debida diligencia de dichos proveedores. En el caso de los PSAV, el plan debe incorporar adicionalmente, cuando proceda, los mecanismos de creación y distribución de activos virtuales, la arquitectura de custodia (hot y cold wallets y su gestión de claves), los procesos para transacciones en blockchain, los protocolos de interoperabilidad con otras plataformas, y los mecanismos establecidos para la conversión a moneda fiduciaria.

g. **Plan financiero:** detalle de la inversión inicial requerida, fuentes de financiamiento, proyecciones financieras realistas para un mínimo de cinco (5) años, presentadas en formato de hoja de cálculo editable, que incluyan:
   i. Estados financieros proforma (estado de resultados, balance general, flujo de caja).
   ii. Una descripción explícita y detallada de todos los supuestos clave utilizados para la elaboración de las proyecciones de ingresos, costos y gastos.
   iii. Cálculo y análisis de indicadores de viabilidad financiera del proyecto, tales como Valor Actual Neto (VAN), Tasa Interna de Retorno (TIR) y Período de Recuperación de la Inversión, especificando la tasa de descuento utilizada y su justificación.
   iv. Estructura tarifaria detallada y justificada para todos los servicios a ofrecer.

h. **Políticas y procedimientos clave:** incluir en anexos, como mínimo, los borradores de: i) política de atención al cliente (incluyendo gestión de quejas y reclamos), ii) política de seguridad de la información y ciberseguridad, iii) política de privacidad y protección de datos personales, y iv) procedimiento para gestión de incidentes de seguridad, v) plan de continuidad del negocio y de recuperación ante desastres, con objetivos de tiempo y punto de recuperación (RTO/RPO) definidos para servicios críticos y vi) plan de respaldo y recuperación de información.

i. **Cronograma de implementación:** plan detallado con fases, actividades clave y plazos estimados para alcanzar la autorización de inicio de operaciones.

Artículo 11. Requisitos mínimos de la plataforma tecnológica. La plataforma tecnológica de todo PSP o PSAV— ya sea propia, arrendada o desplegada íntegramente en servicios de computación en la nube—deberá ser robusta, escalable, segura y resiliente, para asegurar la confidencialidad, integridad, disponibilidad de las operaciones y los datos; y trazabilidad completa mediante registros inalterables. Adicionalmente deberá cumplir, como mínimo, con los siguientes requisitos:

a. **Infraestructura segura:** tanto en su componente físico como lógico —incluyendo servidores, redes, bases de datos, sistemas operativos y soluciones de seguridad informática— deberá estar configurada de forma segura (hardening), contar con redundancia en sus componentes críticos, y disponer de planes de capacidad actualizados, elaborados con base en el análisis de la demanda y las proyecciones de crecimiento.
   Cuando esta infraestructura sea gestionada directamente por el PSP o PSAV, y no esté alojada en la nube ni en centros de datos de terceros, deberá complementarse con controles ambientales adecuados (como climatización, detección y extinción de incendios) y mecanismos estrictos de control de acceso físico que garanticen la protección de los equipos y la información almacenada.
   En los casos en que se utilicen servicios de centros de datos externos o proveedores de servicios en la nube, el PSP o PSAV deberá asegurarse de contratar únicamente a empresas con trayectoria, solvencia y especialización reconocidas. Además, deberá verificar y conservar evidencia de que estos proveedores cuentan con certificaciones vigentes en estándares internacionales de seguridad, como ISO 27001, SOC 2, PCI DSS, u otros equivalentes aplicables a los servicios contratados.
b. **Seguridad lógica y de aplicaciones:** implementar controles de acceso basado en roles y mínimo privilegio, con las debidas autenticaciones; contar con mecanismos de seguridad de información y protección de datos. Cuando se utilice software propio, seguir prácticas de desarrollo seguro de software reconocidas, y ejecutar análisis de vulnerabilidades periódicos, cuya frecuencia y profundidad se basen en un análisis de riesgos.
c. **Seguridad de red:** segmentar las redes internas para aislar sistemas críticos; monitorear el tráfico de red para detectar anomalías; implementar medidas de protección contra amenazas cibernéticas.
d. **Gestión de vulnerabilidades y actualizaciones:** contar con mecanismos adecuados para identificar, evaluar y mitigar vulnerabilidades en sistemas y aplicaciones; y aplicar de forma oportuna parches y actualizaciones de seguridad.

Seguridad específica para PSAV, según el tipo de actividad:

i. **Custodia segura de activos virtuales:** aquellos PSAV que ofrezcan custodia deben implementar controles técnicos y operativos de alto nivel, incluyendo el uso predominante de almacenamiento en frío (cold storage), gestión segura y distribuida de claves privadas (por ejemplo, multi-firma, HSM si aplica), segregación de activos de clientes, y auditorías de seguridad específicas para los sistemas de custodia.

ii. **Capacidad tecnológica para regla de viaje:** disponer de los sistemas y protocolos necesarios para capturar, almacenar y transmitir de forma segura la información requerida por la regla de viaje en las transferencias de activos virtuales.

iii. **Monitoreo de blockchain:** utilizar herramientas o servicios para el análisis de transacciones en blockchain, identificación de direcciones y evaluación de riesgos asociados, como soporte a la gestión de riesgos operativos y de LA/FT/FP.

iv. **Infraestructura blockchain y puntos de integración:** deberán documentar y asegurar los puntos de integración entre su infraestructura tecnológica y las redes blockchain utilizadas (por ejemplo, nodos propios, proveedores externos, APIs de monitoreo y contratos inteligentes desplegados). Estos puntos deberán contar con mecanismos de verificación de disponibilidad, alertas ante fallos, y monitoreo continuo de la actividad en la red.

v. **Trazabilidad técnica de operaciones on-chain:** deberán implementar mecanismos de trazabilidad técnica que permitan vincular, de forma verificable y auditable, cada operación realizada en su plataforma con su correspondiente transacción en la blockchain pública. Estos registros deberán mantenerse por un mínimo de cinco (5) años.

vi. **Gestión de código y despliegue seguro:** los proveedores que desarrollen o mantengan código propio (como contratos inteligentes, monederos, o lógica backend de operaciones con activos virtuales) deberán implementar controles de gestión de versiones, pruebas en testnet u otros entornos de prueba antes del despliegue, así como auditorías periódicas del código crítico.

e. **Registro de auditoría (logging) y monitoreo:** habilitar registros (logs) detallados, inalterables y sincronizados en tiempo para todos los eventos relevantes (tales como accesos, transacciones, cambios de configuración, eventos de seguridad), de los sistemas críticos. Conservar estos registros de forma segura por un mínimo de cinco (5) años.

f. **Personal técnico:** El PSP o PSAV deberá disponer de personal técnico idóneo, ya sea empleado interno o contratado a través de terceros especializados, en número suficiente para cubrir sus necesidades operativas y de seguridad. Este personal debe contar con formación, experiencia y, cuando corresponda, certificaciones en informática, gestión de sistemas y ciberseguridad. Aunque se puedan subcontratar funciones específicas, el PSP mantendrá siempre la responsabilidad final e indelegable sobre la gobernanza tecnológica, la gestión de riesgos y la seguridad de la plataforma.

Para los PSAV, además de lo anterior, el personal directamente encargado de la gestión de activos virtuales o de la infraestructura asociada deberá poseer conocimientos avanzados y actualizados en tecnologías de registro distribuido (blockchain), criptografía aplicada y seguridad de activos virtuales.

g. **Servicios en la nube o infraestructura subcontratada:** cuando la plataforma —total o parcialmente— se ejecute sobre proveedores externos de computación en la nube o de hosting gestionado, el PSP o PSAV deberá, como mínimo:
   a. Realizar debida diligencia del proveedor antes de la contratación. Esta diligencia deberá evaluar la capacidad técnica, controles de seguridad, certificaciones, reputación, incluyendo un análisis sobre la ubicación física y la jurisdicción legal bajo la cual se almacenarán y procesarán los datos.
   b. Establecer contratos formales que especifiquen el alcance de los servicios, los niveles de servicio (SLAs) medibles y exigibles (incluyendo disponibilidad, rendimiento, y tiempos de respuesta ante incidentes), las responsabilidades de cada parte en materia de seguridad y protección de datos, la confidencialidad, las obligaciones de notificación de brechas o incidentes por parte del proveedor.
   c. Elaborar y mantener actualizada una matriz de responsabilidad compartida que delimite claramente cuáles controles de seguridad y cumplimiento normativo (particularmente los referidos en este artículo) son responsabilidad del proveedor de servicios y cuáles son responsabilidad del PSP o PSAV.
   d. Conservar y revisar periódicamente la evidencia actualizada de las certificaciones de seguridad relevantes del proveedor (por ejemplo, ISO 27001, SOC 2), informes de auditoría externa, así como los registros de incidentes de seguridad relevantes notificados por el proveedor o detectados por la entidad, y las acciones correctivas correspondientes.

El BCN, previa solicitud formal y debidamente justificada por el PSP o PSAV, podrá autorizar la adopción de configuraciones tecnológicas, arquitecturas, medidas compensatorias o formas de evidencia alternativas a las especificadas en este artículo, o excepcionalmente, eximir del cumplimiento de algún requisito particular. Para tal fin, el solicitante deberá sustentar de forma suficiente que la alternativa propuesta permite alcanzar un nivel de seguridad y control de riesgos que el BCN considere adecuado.

El BCN podrá emitir normas técnicas específicas detallando requerimientos adicionales y podrá realizar verificaciones in situ o remotas para constatar el cumplimiento.

CAPÍTULO IV
GESTIÓN DE RIESGOS Y CONTROL INTERNO

Artículo 12. Gestión integral de riesgos. Los PSP y PSAV implementarán un sistema formal y documentado de gestión integral de riesgos, que deberá incluir, como mínimo:

a. Una metodología para identificar, evaluar, medir, monitorear, controlar y reportar periódicamente todos los riesgos materiales a los que está expuesta la entidad, incluyendo de manera destacada los riesgos: operacional (fallos en procesos, personas, entre otros), tecnológico (tales como fallos de infraestructura tecnológica, software), de ciberseguridad (ataques externos/internos, robo de datos/activos), financiero (liquidez, crédito -si aplican-, mercado -para PSAV-), y de cumplimiento (incluyendo LA/FT/FP).
b. Políticas y/o procedimientos específicos para la gestión de cada riesgo material identificado, estableciendo límites de tolerancia al riesgo aprobados por la Junta Directiva.
c. Para PSAV, la gestión de riesgos deberá incluir análisis específicos y controles para los riesgos inherentes a los activos virtuales, según el tipo de actividad realizada, tales como: alta volatilidad de precios, seguridad en la custodia (riesgo de hackeo, pérdida de claves), complejidad tecnológica (errores en smart contracts, fallos de blockchain, entre otros), riesgo de contraparte con otros PSAV o plataformas, riesgo de fraude y estafas específicas del ecosistema, y riesgo regulatorio cambiante.
d. Procesos continuos de monitoreo de la exposición al riesgo y generación de informes para la autoridad respectiva.

Artículo 13. Control interno. Los PSP y PSAV deberán diseñar, implementar y mantener un sistema de control interno robusto y efectivo, integrado en sus procesos operativos, tecnológicos y administrativos, y documentado en manuales de procedimientos. Este sistema debe asegurar el cumplimiento de objetivos, la salvaguarda de activos (propios y de clientes), la fiabilidad de la información financiera y operativa, y el cumplimiento de regulaciones.

CAPÍTULO V
NOMBRAMIENTO DE GERENTE GENERAL

Artículo 14. Requisitos del Gerente General (o ejecutivo principal). El Gerente General (o ejecutivo principal) de los PSP o PSAV distintos a bancos e instituciones de microfinanzas, debe cumplir con los siguientes requisitos:

a. Contar con un mínimo de tres (3) años de experiencia relevante, adquirida en puestos de responsabilidad, en uno o varios de los siguientes campos:
    i. el sector bancario, la industria de medios de pago, o el sector tecnológico con enfoque en servicios financieros;
    ii. el diseño, desarrollo, seguridad, operación o gestión de plataformas de activos virtuales, haber tenido un rol en proyectos o redes que usan blockchain , o la aplicación práctica de criptografía en soluciones financieras o de seguridad, entre otras.

La experiencia descrita en el numeral ii) será de especial consideración y valoración para los candidatos a Gerente General de un PSAV. Adicionalmente, se podrá considerar la experiencia en otros sectores o roles, siempre que estos sean de una magnitud y complejidad equivalentes y directamente pertinentes a las responsabilidades inherentes al cargo.

b. Tener formación y conocimientos en economía, finanzas, tecnología de la información, ingeniería, administración o áreas afines; considerándose para los Gerentes Generales de PSAV como particularmente relevante la demostración adicional de certificaciones técnicas o experiencia práctica sustancial en entornos descentralizados, tecnología blockchain, criptografía aplicada o ecosistemas Web3, entre otros similares.
c. No ser deudor moroso de créditos de cualquier entidad bancaria o financiera, ni haber sido declarado en estado de suspensión de pagos, quiebra o concurso.
d. No haber sido condenado mediante sentencia firme por delitos comunes, ni registrar antecedentes penales en los últimos 5 años.

Artículo 15. Solicitud de no objeción de nombramiento de Gerente General (o ejecutivo principal). Dentro de los cinco (5) días hábiles siguientes a la fecha de nombramiento del Gerente General (o ejecutivo principal), el Presidente o Secretario de la Junta Directiva del PSP o PSAV deberá solicitar formalmente al Presidente del BCN la no objeción a dicho nombramiento, mediante comunicación que incluya, como mínimo, la certificación del acta de la sesión en la que se adoptó la decisión.

Adicionalmente, el PSP o PSAV deberá remitir la documentación completa requerida para su evaluación, en un plazo máximo de quince (15) días hábiles contados a partir de la fecha del nombramiento. El BCN podrá otorgar una prórroga para la presentación de la documentación, previa solicitud debidamente justificada por la entidad.

La documentación a presentar deberá incluir:

a. Currículum vitae documentado, conforme al Anexo 2 del presente Reglamento, acompañado de copias certificadas notarialmente de títulos de educación superior, posgrados, maestrías y/o doctorados, según corresponda.
b. Documento de identificación, debidamente certificado por notario público:
   - Para nacionales: copia de la cédula de identidad (ambos lados).
   - Para residentes: copia de la cédula de residencia.
   - Para extranjeros: copia del pasaporte.
c. Certificado de antecedentes judiciales y policiales, en los que conste que no posee antecedentes penales o policiales en los cinco (5) años previos a dicha solicitud. Estos certificados deben tener como máximo sesenta (60) días de haber sido emitidos con respecto a la fecha de la notificación al Presidente del BCN. Cuando se trate de personas que en los últimos cinco (5) años hayan sido residentes en el exterior, el certificado de antecedentes

judiciales y/o policiales deberá ser expedido por las instancias y/o por los organismos competentes extranjeros, del país o países en que haya residido, con la correspondiente autenticación o apostilla.

d. Mínimo dos (2) referencias personales emitidas por profesionales afines al sector financiero, tecnológico o de medios de pago.
e. Consulta del historial crediticio emitido por al menos dos centrales de riesgos privadas autorizadas por SIBOIF.

Recibida la documentación completa, la Administración Superior del BCN evaluará la solicitud y, dentro de un plazo máximo de quince (15) días hábiles, emitirá una resolución razonada en la que se apruebe o se objete el nombramiento del Gerente General (o ejecutivo principal).

CAPÍTULO VI
REQUERIMIENTOS OPERATIVOS ESPECÍFICOS PARA PSP

Artículo 16. Emisión y administración de dinero electrónico. Los PSP autorizados para emitir dinero electrónico, deberán cumplir con las siguientes disposiciones:

a. **Emisión y respaldo:** emitir dinero electrónico únicamente contra la recepción previa de fondos en moneda fíat por un valor nominal idéntico. El monto total de dinero electrónico en circulación deberá estar permanentemente respaldado, como mínimo, por un monto equivalente de fondos líquidos y seguros.
b. **Salvaguarda en CMDE:** mantener la totalidad de los fondos recibidos por la emisión de dinero electrónico en CMDE abiertas exclusivamente para este fin en bancos supervisados por la SIBOIF. Estas cuentas deberán estar claramente identificadas como tales y separadas de las cuentas operativas propias del PSP. El PSP deberá poder demostrar al BCN, en todo momento, que el saldo agregado de las CMDE cubre el total del dinero electrónico emitido y pendiente de redención, para lo cual deberá cumplir con lo siguiente:
    i. Gestión de fondos en tránsito: asegurar que los fondos recibidos por el PSP o por sus agencias autorizadas, particularmente aquellos ingresados después de la hora de corte del banco custodio, sean abonados en la CMDE a más tardar al día hábil bancario siguiente.
    ii. Conciliación diaria de saldos: verificar diariamente que el total del dinero electrónico emitido y pendiente de redención coincida con el saldo agregado de las CMDE, considerando los depósitos de fondos en tránsito gestionados conforme al literal anterior.
    iii. Registro y control de montos en tránsito: llevar un registro detallado y actualizado de los montos recibidos que se encuentren en tránsito pendientes de abono en las CMDE.

Dicho registro deberá mantenerse disponible y ser entregado al BCN cuando este lo requiera.

c. **Convertibilidad:** garantizar a los clientes convertir su saldo de dinero electrónico a dinero en efectivo o mediante transferencia a una cuenta bancaria, a la par (uno a uno respecto a la moneda fíat de emisión), en cualquier momento durante la vigencia de la relación contractual, sujeto a los límites operativos y de seguridad razonables y a las condiciones contractuales informadas. Los procedimientos de redención deben ser claros, accesibles y ejecutarse sin demoras injustificadas.
d. **Prohibición de intereses:** no pagar ni ofrecer intereses ni ninguna otra forma de rendimiento financiero sobre los saldos de dinero electrónico mantenidos por los clientes.
e. **Registro contable:** reflejar el valor total del dinero electrónico emitido y pendiente de redención como un pasivo exigible en sus estados financieros.
f. **Límites operativos:** establecer límites máximos de saldo por cliente y límites transaccionales (por operación, diarios, mensuales) acordes con el perfil de riesgo del cliente. Estos límites deben ser informados claramente a los usuarios.
g. **Circuito de Transacciones Móviles (CTM):** definir y documentar claramente el funcionamiento de su CTM, incluyendo los instrumentos de pago aceptados, la red de aceptación (comercios, agencias) y las reglas operativas.
h. **Gestión de agencias:** si un PSP utiliza agencias, deberá asegurarse de lo siguiente:
    i. **Contrato y registro.** Formalizar la relación mediante contrato previo y llevar un registro actualizado de cada agencia. El contrato debe detallar, como mínimo: los servicios que la agencia puede ofrecer, sus límites de operación, las medidas de seguridad, las tarifas, las responsabilidades de cada parte (especialmente ante fraudes) y cómo la agencia debe reportar su actividad. Asimismo, deberá mantener una lista actualizada de todas las agencias con las que trabaja.
    ii. **Debida diligencia.** Verificar a cada agencia antes de contratarla. Esto significa confirmar que es confiable para el negocio y que cumple las normas contra el lavado de activos y financiamiento al terrorismo (LA/FT/FP). Asimismo, deberá establecer reglas claras para saber cuándo suspender o dar de baja a una agencia si no cumple o si hay actividades sospechosas.
    iii. **Monitoreo.** Implementar un programa de monitoreo de las agencias con indicadores de desempeño y alertas tempranas de fraude o incumplimiento.
    iv. **Responsabilidad.** El PSP responderá siempre ante el BCN y los clientes por lo que hagan o no hagan sus agencias.
    v. **Capacitación.** Brindar capacitación al personal de la agencia al momento de su incorporación y, de ser posible, de manera periódica. La capacitación debe incluir, al menos, contenidos sobre la prevención del LA/FT/FP, y se debe conservar evidencia documental de su realización.

Artículo 17. Servicios de aceptación de pagos para comercios (Adquirencia y Agregación). Los PSP que actúen como adquirentes o agregadores/subadquirentes deberán realizar:

a. **Contratos con comercios:** suscribir contratos claros y completos con cada comercio afiliado, los cuales deberán precisar, al menos: i) servicios prestados; ii) derechos y obligaciones de las partes; iii) comisiones y demás tarifas aplicables; iv) responsabilidades frente a fraudes y contracargos; v) plazos y modalidad de liquidación de fondos; vi) causales de terminación; y vii) mecanismos de solución de controversias.
b. **Tecnología de aceptación segura:** proveer, instalar o habilitar terminales de punto de venta —fijas o móviles (POS, mPOS, entre otros) — y pasarelas de pago en línea que cumplan las normas vigentes de seguridad de la industria de pagos, en lo que corresponda. El PSP garantizará el mantenimiento y la actualización permanente de dichos equipos y plataformas.
c. **Procesamiento eficiente:** garantizar el procesamiento seguro, eficiente y oportuno de las transacciones autorizadas, incluyendo la captura de datos, solicitud de autorización, y la compensación de fondos a través de los sistemas de pago pertinentes.
d. **Liquidación a comercios:** liquidar los fondos netos correspondientes a las ventas de los comercios afiliados en los plazos contractualmente acordados, utilizando cuentas bancarias en entidades supervisadas. Proveer a los comercios información detallada y periódica sobre las transacciones procesadas y las liquidaciones realizadas.
e. **Relación adquirente-agregador:** el agregador deberá mantener un contrato vigente con uno o más PSP autorizados como adquirentes y respetar las reglas operativas y de riesgo fijadas por éstos y, cuando corresponda, por las marcas de pago internacionales. El PSP que suscriba el contrato directo con el comercio, ya sea como adquirente o como agregador, conservará la responsabilidad principal ante el comercio y ante el BCN.
f. **Gestión de riesgo de comercios:** aplicar procedimientos de debida diligencia del comercio ("Conoce a tu Comercio") antes de su afiliación y efectuar monitoreo continuo de su actividad transaccional, a fin de prevenir operaciones fraudulentas o vinculadas al LA/FT/FP. Establecer criterios objetivos para la suspensión o desafiliación de comercios cuando se detecten incumplimientos o actividades sospechosas.

Artículo 18. Otros servicios PSP.

a. **Ejecución de órdenes de pago (transferencias y débitos directos):** los PSP garantizarán la ejecución exacta, completa y oportuna de las órdenes iniciadas por el ordenante o autorizadas previamente por este (débitos directos). Deberán aplicar autenticación reforzada y controles que verifiquen la legitimidad de la instrucción y eviten alteraciones no autorizadas.

b. **Emisión de instrumentos de pago electrónicos:** para la emisión de tarjetas de débito, crédito, prepago u otros instrumentos electrónicos, el PSP cumplirá los estándares de seguridad física y lógica vigentes —por ejemplo, tecnología de chip EMV y tokenización—, protegerá los datos sensibles del titular y mantendrá al día las certificaciones requeridas por las marcas y la industria de pagos, según corresponda. Los usuarios recibirán información clara sobre costos, límites, medidas de seguridad y el procedimiento para impugnar cargos no reconocidos.
c. **Administración de redes de cajeros automáticos (ATM):** los PSP que operen redes de cajeros asegurarán la disponibilidad operativa de los equipos, la seguridad física de los dispositivos, así como la seguridad lógica del software y de las comunicaciones, la correcta dispensación de efectivo y el registro fiable de las transacciones. Deberán contar con monitoreo permanente para prevenir fraudes —por ejemplo, clonación o malware—, realizar conciliaciones diarias del efectivo y disponer de un canal de atención que resuelva los reclamos relacionados con dispensaciones erróneas o retención de tarjetas.

CAPÍTULO VII
REQUERIMIENTOS OPERATIVOS ESPECÍFICOS PARA PSAV Y PROHIBICIONES

Artículo 19. Intercambio de activos virtuales. Los PSAV autorizados para el intercambio entre activos virtuales y moneda fíat o entre distintas formas de activos virtuales deberán:

a. **Transparencia de precios y detalle de la operación:** antes de que el cliente confirme la operación de intercambio (compra o venta de un activo virtual), el PSAV deberá mostrar de forma fácilmente comprensible, preferiblemente en una sola vista, la información relevante para la transacción, incluyendo:
    i. El precio del activo virtual al momento de la operación.
    ii. Cualquier ajuste al precio base o spread que se aplique sobre el precio del mercado del PSAV para determinar el precio de ejecución final de la orden.
    iii. La comisión fija o porcentual que cobrará el PSAV por ejecutar la transacción.
    iv. La cantidad estimada o exacta de activo virtual que el cliente comprará o venderá como resultado de la operación.
    v. El saldo disponible del cliente en la moneda fíat o en el activo virtual que se utilizará para la operación.
    vi. Un resumen claro de la orden propuesta, detallando al menos el tipo de operación (compra/venta), el precio de ejecución o límite, la cantidad de activo virtual, la comisión total estimada y el impacto en el saldo del cliente.
    vii. El precio efectivo que el cliente pagará o recibirá resultará de la combinación del precio de ejecución de la orden (que puede incluir un ajuste o spread) y la comisión

total aplicable, todo lo cual debe estar claramente presentado antes de que el cliente finalice la operación.

Adicionalmente, el PSAV deberá mantener publicada y actualizada en su plataforma, la metodología general empleada para determinar los spreads aplicados, así como los factores que puedan afectar la variación de las comisiones, permitiendo a los usuarios comprender el impacto económico de sus operaciones.

b. **Ejecución y liquidación eficiente:** ejecutar las órdenes de compraventa de los clientes de manera rápida y en los términos acordados. La liquidación del contravalor de la operación, ya sea mediante la entrega de moneda fíat o de los activos virtuales correspondientes, se procesará sin dilación injustificada y a la mayor brevedad posible que la tecnología y los sistemas de pago permitan. El PSAV deberá informar de forma clara y accesible al cliente sobre los plazos estimados para la ejecución y la liquidación de sus operaciones.
c. **Salvaguarda de fondos fíat:** cuando el PSAV reciba o custodie fondos en moneda fíat pertenecientes a sus clientes, ya sea dinero entregado por el cliente para la adquisición de activos virtuales, o dinero resultante de la venta de activos virtuales del cliente que el PSAV mantiene bajo su custodia temporalmente hasta que el cliente disponga de él (por ejemplo, retirándolo o utilizándolo en otra operación), dichos fondos deberán ser segregados. Para tal efecto, el PSAV deberá depositar y mantener estos fondos en CMAV, las cuales deberán estar clara y efectivamente separadas de los fondos propios del PSAV. Estas CMAV deberán ser mantenidas en bancos supervisados por la SIBOIF. Los fondos depositados en las CMAV solo podrán ser utilizados para ejecutar las instrucciones específicas de compra de activos virtuales del cliente o para su devolución directa al cliente que sea el titular de los fondos.

Artículo 20. Transferencia de activos virtuales. Los PSAV autorizados para realizar transferencias de activos virtuales deberán cumplir con lo siguiente:

a. **Capacidad tecnológica y operativa para la regla de viaje:** implementar y mantener la infraestructura tecnológica, los procesos internos y los protocolos de seguridad necesarios para cumplir plenamente con las obligaciones derivadas de la "Regla de Viaje" en las transferencias de activos virtuales que se realicen entre PSAVs. Esto incluye la capacidad de:
    i. Obtener, verificar y registrar la información del originador de la transferencia, y, cuando aplique, la información del PSAV originador.
    ii. Obtener y registrar la información requerida del beneficiario y, cuando aplique, la información del PSAV beneficiario.
    iii. Transmitir de forma segura, precisa y oportuna la información requerida a la contraparte (el PSAV beneficiario o intermediario) al momento de ordenar o ejecutar la transferencia.

iv. Recibir, procesar, verificar y almacenar de forma segura la información asociada proveniente de transferencias entrantes iniciadas desde otros PSAVs.

b. **Monitoreo de transacciones y direcciones:** utilizar herramientas y soluciones tecnológicas especializadas en el análisis de transacciones y direcciones de blockchain, complementadas con otras fuentes de información relevante. El PSAV deberá monitorear las transferencias de activos virtuales, tanto entrantes como salientes, y analizar las direcciones de origen y destino, con el fin de identificar posibles vínculos con actividades ilícitas, direcciones o entidades sujetas a sanciones, o cualquier otro factor de alto riesgo, como parte integral de su sistema de gestión de riesgos de LA/FP/FT.

c. **Debida diligencia reforzada para transferencias con monederos sin custodia:** cuando las transferencias de activos virtuales, recibidas por el PSAV desde un monedero externo, o enviadas por el PSAV hacia un monedero externo, involucren un monedero sin custodia, se deberán aplicar procedimientos de debida diligencia reforzada si el valor de la transacción supera los umbrales establecidos por la UAF o normativa interna del PSAV. Dichos procedimientos de debida diligencia reforzada deberán incluir la implementación de medidas razonables y verificables por parte del PSAV para confirmar que su cliente es efectivamente el propietario o ejerce control sobre el monedero sin custodia involucrado en la transferencia.

   Las medidas de verificación podrán incluir: solicitud de captura de pantalla del monedero, transacción de verificación previa (micro-transferencia), análisis de comportamiento histórico del cliente, o cualquier otro medio técnico razonable que permita establecer con un grado aceptable de certeza la titularidad del monedero externo.

Artículo 21. Custodia y administración segura de activos virtuales. Los PSAV autorizados para prestar servicios de custodia y/o administración de activos virtuales en nombre de terceros deberán implementar y mantener un marco de seguridad integral y robusto, diseñado específicamente para la protección de dichos activos, que incluya, como mínimo, lo siguiente:

a. **Infraestructura de custodia segura:** implementar y utilizar una estrategia de almacenamiento combinada que priorice el uso de almacenamiento en frío (cold storage), manteniendo fuera de línea la gran mayoría de los activos virtuales custodiados. El almacenamiento en caliente (hot wallets) solo se empleará para cubrir las necesidades operativas inmediatas y de liquidez necesaria para el procesamiento ágil de transacciones, minimizando en todo momento la exposición de los activos en línea.

b. **Gestión segura de claves privadas:** establecer y cumplir políticas y procedimientos estrictos que cubran todo el ciclo de vida de las claves privadas que controlan los activos custodiados, incluyendo su generación segura, métodos de almacenamiento protegidos (considerando el uso de Módulos de Seguridad de Hardware - HSMs, si aplica, u otras soluciones equivalentes de alta seguridad), protocolos definidos para su uso autorizado,

procedimientos robustos para su respaldo (backup) y planes claros para su destrucción segura cuando dejen de ser necesarias. Se deberán emplear tecnologías como la multi-firma para requerir la concurrencia de múltiples autorizaciones para la ejecución de transacciones críticas o de alto valor desde los monederos de custodia.

c. **Segregación de activos:** asegurar que los activos virtuales custodiados en nombre de cada cliente estén clara y efectivamente segregados, tanto a nivel contable en los registros internos del PSAV como, preferiblemente, a nivel criptográfico (mediante el uso de direcciones de monedero únicas para cada cliente o mecanismos equivalentes que permitan distinguir inequívocamente los activos de un cliente de los de otro). Esta segregación debe garantizar una separación completa respecto de los activos virtuales propios del PSAV.
d. **Controles de acceso estrictos:** implementar controles de acceso físico y lógico rigurosos a las instalaciones, sistemas y procesos involucrados en la custodia y administración de activos virtuales. Dichos controles deberán basarse en el principio de mínimo privilegio (otorgar solo los permisos estrictamente necesarios para cada función) y requerir autenticación multifactorial (MFA) para todo el personal con acceso a sistemas críticos.
e. **Procedimientos de retiro seguros:** establecer y aplicar procesos internos rigurosos y con múltiples niveles de control para la autorización y ejecución de las solicitudes de retiro de activos virtuales iniciadas por los clientes. Esto incluye implementar mecanismos efectivos para verificar la legitimidad de la solicitud de retiro y aplicar límites de retiro basados en perfiles de riesgo o verificaciones adicionales.
f. **Conciliaciones y pruebas de reservas:** realizar conciliaciones frecuentes y documentadas entre los saldos de activos virtuales registrados en las cuentas individuales de los clientes en los sistemas internos del PSAV y la cantidad total de activos virtuales efectivamente mantenidos en custodia (tanto on-chain en la blockchain como off-chain, si aplica).

   Adicionalmente, el PSAV deberá realizar, al menos una vez al año, una prueba de reservas (proof of reserves) que sea verificable y técnicamente auditable. Esta prueba deberá:

   - Confirmar que los activos custodiados por el PSAV respaldan íntegramente los saldos registrados en favor de los clientes;
   - Ser ejecutada bajo estándares técnicos reconocidos, preferiblemente por terceros independientes o con herramientas verificables por el BCN;
   - Estar documentada y disponible para la revisión del BCN;
   - No comprometer la identidad del cliente, permitiendo validación criptográfica sin exposición de datos personales.

   El BCN podrá requerir pruebas adicionales en cualquier momento, especialmente en caso de incidentes operativos, reclamos generalizados de usuarios o señales de debilidad financiera.

Artículo 22. Participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual. Los PSAV que, de acuerdo con su autorización, participen en la oferta inicial o secundaria de un activo virtual, o provean servicios financieros relacionados con su promoción, distribución o faciliten la venta o adquisición de dicho activo en nombre de un emisor o tercero a través de su plataforma, deberán asegurar el cumplimiento de lo siguiente:

a. **Debida diligencia del emisor y proyecto:** realizar una evaluación exhaustiva y documentada de la legitimidad y seriedad del activo virtual, incluyendo (cuando aplique): la debida diligencia sobre el emisor o equipo de desarrollo, la revisión del documento técnico oficial (whitepaper), verificación técnica del contrato inteligente (smart contract), la viabilidad técnica y económica del proyecto subyacente, la solidez de la tecnología empleada y los riesgos inherentes asociados al propio activo. Esta evaluación deberá llevarse a cabo como parte del proceso de decisión para participar en su oferta, promoción, distribución, o para listar y facilitar su negociación o venta en la plataforma del PSAV.
b. **Transparencia informativa y advertencia de riesgos asociados al activo:** asegurar que la información relevante sobre el activo virtual, el proyecto (cuando sea pertinente y verificable) y los riesgos inherentes asociados a su adquisición o negociación, sea en todo momento clara, precisa, completa y no contenga elementos engañosos. Dicha información deberá estar disponible de forma accesible para los potenciales adquirentes en la plataforma del PSAV. Adicionalmente, se deberá incluir una advertencia prominente y de fácil comprensión sobre los altos riesgos de pérdida de capital, volatilidad y otras contingencias asociadas a la inversión o adquisición de activos virtuales en general y, si aplica, riesgos específicos del activo en particular.
c. **Controles de prevención de LA/FT/FP aplicados a la adquisición:** aplicar controles robustos de Debida Diligencia del Cliente (DDC), que deberán incluir medidas reforzadas dependiendo del nivel de riesgo identificado, y un monitoreo continuo sobre la identidad de los clientes que adquieran o vendan el activo virtual a través de la plataforma, así como sobre los flujos de fondos (fiduciarios o virtuales) asociados a estas operaciones, como parte integral de su programa de prevención de LA/FT/FP.

Artículo 23. Prohibiciones operativas específicas para PSAV. Los PSAV tienen estrictamente prohibido:

a. Ofrecer, integrar o facilitar el uso de servicios diseñados para ofuscar transacciones u ocultar la identidad de las partes, tales como Mezcladores (Mixers), Volteadores (Tumblers), o servicios similares.
b. Soportar o permitir transacciones con criptomonedas diseñadas específicamente para mejorar el anonimato (Anonymity-Enhanced Cryptocurrencies - AECs) o que utilicen protocolos de privacidad que impidan la trazabilidad requerida por la regla de viaje.

c. Permitir el uso, la conexión o la integración dentro de su propia plataforma (incluyendo monederos internos del PSAV o funcionalidades de interacción) de monederos de privacidad (privacy wallets) o la aplicación de tecnologías que, al ser utilizadas dentro del entorno controlado del PSAV, impidan la identificación clara y el registro del origen o destino de los fondos de los clientes.
d. Facilitar o procesar transacciones de activos virtuales que involucren el uso de herramientas de anonimización de red como TOR (The Onion Router) o redes privadas virtuales (VPN) cuando dichas herramientas sean directamente integradas, promovidas o requeridas por el PSAV como medio para ocultar la ubicación geográfica o el origen de la conexión de red del usuario en la realización de transacciones en la plataforma del PSAV. Esto no prohíbe a los usuarios emplear VPNs por su propia cuenta para acceder al servicio del PSAV.
e. Realizar o facilitar operaciones de intercambio o transferencia que constituyan un "salto de cadenas" (chain-hopping) entre diferentes blockchains, cuyo propósito evidente o principal sea dificultar o romper deliberadamente el rastreo del movimiento de los fondos a través de las diferentes redes, como parte de un esquema de ofuscación.
f. Prometer, facilitar, comercializar o listar activos virtuales que ofrezcan, simulen o impliquen rendimientos financieros fijos o garantizados, o que estén estructurados como esquemas de inversión colectiva, a menos que se cuente previamente con una autorización expresa del BCN.

CAPÍTULO VIII
OBLLIGACIONES GENERALES DE PSP Y PSAV

Artículo 24. Requisitos de seguridad de autenticación. Los PSP y PSAV que ofrezcan servicios de dinero electrónico, activos virtuales, acceso a carteras digitales, compraventa e intercambio de divisas de forma electrónica, o transferencias de fondos, deberán implementar y exigir la autenticación reforzada de sus clientes, para todas las interacciones electrónicas o digitales que estos realicen y que se describen a continuación.

1. Para el inicio de sesión del cliente en la plataforma o aplicación, se requerirá, como mínimo:
   a. El identificador único del cliente; y
   b. Un factor de autenticación de alguna de las categorías reconocidas (conocimiento, posesión o inherencia).

2. Se deberá requerir, adicionalmente al inicio de sesión, la aplicación de al menos un factor de autenticación más, preferiblemente de distinta categoría a la utilizada en el factor de autenticación del numeral 1, literal b) de este artículo, para cumplir con el principio de autenticación reforzada, al momento de autorizar o ejecutar cualquiera de las siguientes acciones a través de los canales electrónicos o digitales proporcionados por el PSP o PSAV:

a. Operaciones de pago o transferencias de fondos o de activos virtuales dirigidas a terceros.
b. Acciones que impliquen el acceso, consulta o modificación de datos sensibles del cliente, de la configuración de sus cuentas, o de las características de sus instrumentos de pago o servicios contratados.
c. Configuración o modificación de parámetros de seguridad de la cuenta, de los límites transaccionales, o de los mecanismos de autenticación
d. Cualquier otra acción que, a criterio del proveedor o del BCN, implique un riesgo significativo de fraude, acceso no autorizado a los fondos o activos virtuales, o exposición indebida de datos sensibles del cliente.

Artículo 25. Transparencia y requisitos de información al cliente. Los PSP y PSAV deberán poner a disposición permanente de sus clientes, de forma clara, precisa, completa, fácilmente accesible, sin costo y oportuna, a través de su página web oficial y cualquier otra plataforma o medio principal de prestación de servicios que este considere, como mínimo, la siguiente información:

a. Condiciones y términos contractuales del servicio.
b. Descripción del funcionamiento de los servicios ofrecidos.
c. Horarios de operación y canales de atención al cliente.
d. Lista completa y detallada de tarifas, comisiones y cargos aplicables.
e. Procedimiento para consultas, quejas y reclamos.
f. Los PSAV deberán divulgar de manera sencilla y clara en su página de internet o en cualquier otro medio principal que utilicen para prestar su servicio, una advertencia explícita sobre los riesgos inherentes y significativos asociados a la adquisición, tenencia y operación con activos virtuales. Esta advertencia deberá incluir, entre otros, los riesgos de volatilidad extrema, pérdida total o parcial del capital invertido, riesgos tecnológicos (como fallos en la blockchain o ciberataques), riesgos de contraparte, y la posible falta de mecanismos de protección o seguro equivalentes a los de los productos financieros tradicionales.

Artículo 26. Obligaciones de los PSP y PSAV

a. Informar al BCN, mediante correspondencia escrita, ya sea por correo electrónico o carta física, dentro de los quince (15) días hábiles siguientes a su formalización u ocurrencia, sobre cualquier modificación relevante relacionada con: el representante legal (cuando sea distinto del Gerente General); la composición del capital social o estructura accionaria, incluyendo a los beneficiarios finales en caso de cambios; reformas a la escritura de constitución o a los estatutos sociales; designación o cese de miembros de la junta directiva; cambios significativos en la infraestructura tecnológica crítica o en proveedores tecnológicos estratégicos; apertura o cierre de la oficina principal u otras oficinas operativas en el territorio nacional; así como

cualquier otra información societaria, operativa o de gobernanza que la entidad considere relevante.

b. Permitir y facilitar el acceso inmediato a sus instalaciones físicas, sistemas informáticos (incluyendo bases de datos y registros de transacciones), documentación y cualquier otra fuente de información, al personal del BCN autorizado y designado para realizar labores de vigilancia o supervisión. Asimismo, deberán poner a disposición del BCN, las herramientas de consulta en tiempo real, los reportes específicos y el apoyo técnico necesario que este determine para el cabal cumplimiento de estas labores.

c. Proporcionar al BCN los datos estadísticos y operativos sobre las transacciones efectuadas, y cualquier otra que este estime pertinente, en los formatos, plazos y en los medios que este lo requiera.

d. Formular sus estados financieros correspondientes al período comprendido entre el 1 de enero y el 31 de diciembre de cada año, fecha en la que se procederá al cierre del ejercicio. Dentro de los 150 días posteriores al cierre, la máxima autoridad de la entidad deberá celebrar sesión de Junta Directiva para conocer y resolver sobre los estados financieros auditados. Una vez aprobados, deberá remitirse al BCN, por vía electrónica, una copia de los estados financieros en un plazo no mayor a 10 días hábiles contados a partir de la fecha de su aprobación.

   Las entidades distintas a bancos sujetos a la supervisión de la SIBOIF y de las instituciones de microfinanzas reguladas y supervisadas como tal por la CONAMI, que hayan iniciado operaciones en el segundo semestre del año relacionado al ejercicio, solamente deberán enviar al BCN los estados financieros certificados por contador público autorizado en el año subsiguiente. En el año calendario siguiente a la remisión de los estados financieros certificados, deberán remitir los estados financieros auditados.

e. Notificar interrupciones del servicio conforme lo siguiente:

   i. Interrupciones programadas: en el caso de interrupciones programadas que excedan las seis (6) horas continuas dentro del horario de servicio, originadas por mantenimientos, implementación de mejoras tecnológicas u otras circunstancias controladas, notificar a los clientes afectados y al BCN con una antelación mínima de dos (2) días hábiles respecto al inicio de la interrupción, y especificar el motivo, la fecha, la hora de inicio y la duración estimada de la misma. Se exceptúan de esta obligación los eventos catalogados como fuerza mayor o caso fortuito.

   ii. Interrupciones no programadas (por fallas o incidencias operativas, tecnológicas o de seguridad o de otra índole), se deberá proceder de la siguiente manera:

      - Notificación inicial: en caso de una interrupción grave (por generar un impacto negativo significativo en el servicio o afectar el sistema de pagos), o cuando la interrupción continua de los servicios a los clientes supere las seis (6) horas dentro de un mismo día de servicio, el proveedor deberá notificar de inmediato al BCN a través de correo electrónico. Esta notificación deberá contener la información esencial disponible en el momento sobre la incidencia.

- Informe detallado del incidente: adicionalmente a la notificación inicial, se deberá remitir un informe escrito detallado del incidente. Este informe deberá enviarse por correo electrónico en un plazo no mayor a dos (2) días hábiles a partir de la ocurrencia del evento, utilizando el formato de reporte de incidentes dispuesto por el BCN.

f. Conservar los registros de cada operación o transacción por un período mínimo de cinco (5) años, contados a partir de la fecha de su ejecución.
g. Definir y comunicar los requisitos técnicos, de infraestructura, de recursos humanos, de seguridad y otros aplicables que deberán cumplir las agencias autorizadas, en caso de operar a través de estas.
h. Suscribir y mantener vigentes los contratos de servicios que formalicen la relación con las agencias autorizadas, en caso de operar a través de estas.
i. Contar con las siguientes políticas y procedimientos, los cuales deberán estar formalmente aprobados por su Junta Directiva, debidamente documentados, efectivamente implementados, difundidos internamente entre el personal relevante, y ser revisados y actualizados periódicamente, como mínimo una vez cada dos (2) años o cuando ocurran cambios significativos en el entorno operativo o regulatorio:
    i. Plan de continuidad del negocio y de recuperación ante desastres, con RTO y RPO definidos para los servicios críticos.
    ii. Plan de respaldo y recuperación de información.
    iii. Política de atención al cliente (incluye gestión de quejas y reclamos).
    iv. Política de seguridad de la información y ciberseguridad.
    v. Política de privacidad y protección de datos personales.
    vi. Procedimiento para gestión de incidentes de seguridad.
j. Garantizar a sus clientes el acceso y uso de todos los servicios para los cuales la entidad obtuvo autorización del BCN, prestándolos en condiciones equitativas, transparentes y no discriminatorias, sin perjuicio de la aplicación de criterios de segmentación de clientes basados en perfiles de riesgo u otros factores objetivos, siempre que dichos criterios sean previamente definidos y documentados.
k. Acreditar íntegramente a sus clientes los fondos derivados de las operaciones, dentro de los plazos establecidos por el proveedor para cada uno de los servicios.
l. Asegurar la prestación de los servicios en los días y horario establecido por cada entidad.
m. Los PSP y PSAV, con excepción de los bancos sujetos a la supervisión de la SIBOIF y las instituciones de microfinanzas reguladas y supervisadas como tal por la CONAMI, deberán solicitar y obtener la no objeción previa y por escrito del BCN para realizar las siguientes actuaciones:
    i. Nombramiento y/o sustitución del Gerente General o ejecutivo que ejerza la máxima responsabilidad administrativa, conforme al procedimiento y requisitos establecidos en el Capítulo V de este Reglamento.

ii. Cambios de domicilio
iii. Traspasos de titularidad de acciones cuyo valor nominal iguale o supere el 25% (veinte y cinco por ciento) del capital pagado de la entidad, fusión con otras entidades o escisión de su patrimonio.
iv. Suspensión temporal voluntaria de la totalidad de sus operaciones o de una o más líneas de servicio previamente autorizadas, por un período continuo o acumulado superior a treinta (30) días calendario dentro de un año, cuando dicha suspensión no esté directamente ocasionada por la imposición de medidas precautorias o sancionatorias por parte de una autoridad competente, ni por los incidentes operativos imprevistos referidos en el literal e) de este artículo.

Artículo 27. Suministro de información al BCN. Los PSP y PSAV están obligados a suministrar al BCN, cuando este lo requiera, información tecnológica, administrativa, financiera, estadística, legal, normativa, y cualquier otra, tal como procedimientos, manuales, políticas, contratos suscritos con proveedores de servicios y/o clientes, y cualquier otra documentación que el BCN considere pertinente, en el ámbito de su labor de vigilancia y supervisión de los sistemas de pago.

CAPÍTULO IX
CANCELACIÓN DE LA LICENCIA Y REGISTRO A SOLICITUD DEL PROVEEDOR Y CESE DE SERVICIOS

Artículo 28. Cancelación de la licencia y registro a solicitud del proveedor. Los PSP o PSAV podrán solicitar voluntariamente al BCN la cancelación de sus licencias y/o registros cuando decidan cesar de forma definitiva sus operaciones o la prestación de los servicios autorizados.
Para tal efecto, el proveedor deberá cumplir con el siguiente procedimiento:

1. **Solicitud Formal:** presentar una solicitud formal y motivada al Presidente del BCN, suscrita por el Representante Legal, expresando la decisión de cesar operaciones y solicitar la cancelación de la licencia o registro. Dicha solicitud deberá ir acompañada, como mínimo, de la siguiente documentación e información:
   a. Acta del órgano societario competente (Junta Directiva o Junta General de Accionistas, según corresponda) donde se apruebe la decisión de cesar operaciones y solicitar la cancelación de la licencia y/o registro.
   b. Un plan detallado de cese de operaciones (Plan de Cese), que deberá incluir, como mínimo:
      i. El cronograma para la finalización progresiva de los servicios.
      ii. El procedimiento y plazos para la comunicación a todos los clientes afectados sobre el cese de operaciones, con una antelación razonable que no podrá ser inferior a (30) días calendario antes de la fecha prevista para el cese efectivo de los servicios.

iii. Las medidas específicas para la liquidación de todas las obligaciones pendientes con los clientes, incluyendo la devolución de fondos, la transferencia de dinero electrónico o activos virtuales a otros proveedores o cuentas indicadas por los clientes, según corresponda.
iv. Procedimientos para la atención y resolución de consultas y reclamos de los clientes durante el proceso de cese y por un período posterior razonable.
v. Un plan para la conservación y resguardo seguro de los registros de transacciones y documentación de clientes por el período mínimo legal establecido en el artículo 26, literal f), del presente Reglamento, y la forma en que el BCN podrá acceder a ellos si fuese necesario.

c. Estados financieros aprobados por su Junta Directiva, con corte al mes anterior a la presentación de la solicitud de cancelación.
d. Cualquier otra información o documentación que el BCN considere necesaria para evaluar el impacto del cese de operaciones y la protección de los intereses de los usuarios.

2. **Evaluación por parte del BCN:** recibida la solicitud y la documentación completa, el BCN evaluará el Plan de Cese y la situación del proveedor. El BCN podrá requerir al solicitante información adicional, aclaraciones o modificaciones al Plan de Cese para asegurar un cierre ordenado y la protección de los usuarios. El plazo para resolver la solicitud se suspenderá mientras el solicitante atienda dichos requerimientos.
3. **Obligaciones del proveedor durante el proceso:** durante el proceso de evaluación y hasta la efectiva cancelación de la licencia o registro, el proveedor deberá:
   a. Abstenerse de iniciar nuevas operaciones o captar nuevos clientes para los servicios que se pretenden cesar, desde el momento de la notificación a clientes de su Plan de Cese.
   b. Continuar cumpliendo con todas sus obligaciones regulatorias, incluyendo la remisión de información al BCN, salvo dispensa expresa por parte de este último.
   c. Ejecutar el Plan de Cese conforme a lo presentado al BCN, o según las modificaciones que este hubiere instruido.
   d. Informar periódicamente al BCN sobre el avance en la ejecución del Plan de Cese.
4. **Resolución y efectos de la cancelación:**
   a. Una vez que el BCN considere que se ha completado la ejecución del Plan de Cese y que el proveedor ha cumplido con todas sus obligaciones frente a los clientes, la Administración Superior del BCN emitirá la resolución de cancelación de la licencia y/o registro en un plazo no mayor a quince (15) días hábiles.
   b. El BCN comunicará la cancelación a la UAF, SIBOIF y a la CONAMI, según corresponda.
   c. La resolución de cancelación será publicada en La Gaceta, Diario Oficial, a costa del interesado, y en el sitio web del BCN.
   d. La cancelación de la licencia o registro inhabilita al proveedor para continuar prestando los servicios que le fueron autorizados.

Artículo 29. Cese voluntario de servicios específicos autorizados. Los PSP o PSAV que cuenten con una licencia o registro vigente y decidan cesar de forma definitiva la prestación de uno o más de los servicios específicos que les fueron autorizados, manteniendo la autorización para otros, deberán solicitarlo al BCN. Para tal efecto, el proveedor deberá cumplir con el siguiente procedimiento:

1. **Solicitud formal al BCN:** el proveedor debe presentar una solicitud formal a la División de Operaciones Financieras del BCN. Esta solicitud debe:
   a. Identificar claramente el servicio o servicios a discontinuar.
   b. Justificar las razones del cese.
   c. Adjuntar el acta del órgano societario competente (Junta Directiva o Junta General de Accionistas, según corresponda) donde se apruebe la decisión.
   d. Adjuntar un Plan de Cese del servicio específico.

2. **Contenido del Plan de Cese:** deberá detallar como mínimo:
   a. Un cronograma claro, incluyendo la fecha propuesta para el cese efectivo del servicio.
   b. Las principales actividades para el cierre ordenado del servicio.
   c. El procedimiento de comunicación a los clientes afectados, con al menos treinta (30) días calendario de antelación a la fecha de cese.
   d. Las medidas específicas para liquidar todas las obligaciones pendientes con los clientes, particularmente cómo se gestionará la devolución de saldos o fondos no utilizados que correspondan exclusivamente al servicio que se discontinúa, cuando aplique.
   e. Los canales de atención que se mantendrán disponibles para consultas y reclamos de los clientes afectados durante el proceso de cese y por un tiempo razonable después.

3. **Resolución y efectos de la cancelación:**
   a. Una vez que el BCN considere que se ha completado la ejecución del Plan de Cese y que el proveedor ha cumplido con todas sus obligaciones frente a los clientes, la Administración Superior del BCN emitirá la resolución de cancelación de la licencia y/o registro en un plazo no mayor a quince (15) días hábiles.
   b. El BCN comunicará el cese del servicio a la UAF, SIBOIF y a la CONAMI, según corresponda y actualizará la lista de servicios en la página web.

CAPÍTULO X
INFRACCIONES, SANCIONES, SUSPENSIÓN Y REVOCACIÓN DE REGISTROS Y LICENCIAS

Artículo 30. Clasificación de infracciones y sanciones. Se establecen las siguientes clasificaciones de infracciones al incumplir la Norma de los Proveedores de Tecnología Financiera

de Servicios de Pago y de los Proveedores de Servicios de Activos Virtuales (Resolución CDMF-XIII-2-25) y las obligaciones detalladas en el presente Reglamento:

1. **Infracciones Leves:** se consideran infracciones leves, entre otras de similar naturaleza, las siguientes:
   a. No notificar al BCN la fecha efectiva de publicación de la licencia en La Gaceta, Diario Oficial, dentro del plazo de diez (10) días hábiles siguientes a dicha publicación, conforme al artículo 5.
   b. Remitir de forma extemporánea e injustificada la información o documentación requerida por el BCN en el ejercicio de sus facultades, de acuerdo con el artículo 27.
   c. Remitir de forma extemporánea el certificado de registro ante la UAF, conforme el artículo 2, literal h).
   d. Incumplir con la obligación de poner a disposición permanente de los clientes la información mínima requerida en el artículo 25, de forma incompleta, imprecisa, o de manera que dificulte su acceso o comprensión, especialmente en lo referente a tarifas, comisiones, riesgos y términos contractuales, o no mantener actualizada dicha información.
   e. Incumplir con las notificaciones al BCN sobre interrupciones del servicio, conforme al artículo 26, literal e).
   f. Omitir la notificación al BCN de modificaciones relevantes no sujetas a autorización previa, dentro de los quince (15) días hábiles siguientes a su formalización u ocurrencia, según lo dispuesto en el artículo 26, literal a).
   g. No remitir al BCN los estados financieros aprobados por la Junta Directiva en el plazo de diez (10) días hábiles posteriores a su aprobación, conforme al artículo 26, literal d), siempre que el retraso no sea excesivo o reiterado.
   h. Otros incumplimientos de igual o similar gravedad que infrinjan a las disposiciones legales, normativas y otras que le sean aplicables.

2. **Infracciones Moderadas:** se consideran infracciones moderadas, entre otras de similar naturaleza, las siguientes:
   a. No presentar la solicitud de autorización de inicio de operaciones para servicios adicionales dentro del plazo de doscientos cincuenta (250) días desde su aprobación, conforme al artículo 7, numeral 3.
   b. La falta de remisión de la información (estadística, operativa o de otra índole) requerida por el BCN, o la remisión de la misma con errores u omisiones significativos, cuando cualquiera de estas situaciones ocurra de forma reiterada, conforme a lo establecido en los artículos 26, literal c), y 27.
   c. No contar con alguna de las políticas o planes requeridos en el artículo 26, literal i), o que estos no estén formalmente aprobados por la Junta Directiva, no se encuentren

debidamente documentados, o no sean revisados y actualizados periódicamente según lo establecido.

d. No implementar la autenticación reforzada de clientes en los supuestos obligatorios establecidos en el artículo 11, literal c), y en el artículo 24.
e. No conservar los registros de cada operación o transacción por el período mínimo de cinco (5) años, o no asegurar su integridad o disponibilidad para el BCN, en contravención al artículo 26, literal f).
f. Para los PSP emisores de dinero electrónico, incumplir con la debida diligencia, supervisión continua o capacitación de sus agencias, conforme al Artículo 16, literal h).
g. Para los PSP que ofrecen servicios de aceptación de pagos, no aplicar procedimientos de debida diligencia del comercio ("Conoce a tu Comercio") o no efectuar monitoreo continuo de su actividad, conforme al Artículo 17, literal f).
h. Para los PSAV, no mostrar la información relevante de la transacción de intercambio de activos virtuales de forma clara antes de la confirmación del cliente, conforme al artículo 19, literal a).
i. Para los PSAV, no implementar la infraestructura tecnológica, procesos o protocolos para cumplir con la "Regla de Viaje", conforme al artículo 20, literal a).
j. Para los PSAV que custodian activos virtuales, no implementar una estrategia de almacenamiento que priorice el uso de almacenamiento en frío, o no gestionar de forma segura las claves privadas, o no asegurar la segregación de activos de clientes, conforme al artículo 21, literales a), b) y c).
k. Para los PSAV, no realizar la debida diligencia del emisor y proyecto en la oferta de activos virtuales, o no proveer transparencia informativa y advertencia de riesgos, conforme al artículo 22, literales a) y b).
l. Obstaculizar o dificultar las labores de vigilancia o supervisión del BCN, impidiendo el acceso a instalaciones, sistemas o documentación, conforme al artículo 26, literal b).
m. No implementar un sistema formal y documentado de gestión integral de riesgos, o un sistema de control interno robusto y efectivo, conforme a los artículos 12 y 13, cuando dicha omisión ponga en riesgo la estabilidad de la entidad o los intereses de los clientes.
n. La reincidencia en la comisión de tres o más infracciones leves en un lapso de doce (12) meses continuos.
o. Otros incumplimientos de igual o similar gravedad que infrinjan a las disposiciones legales, normativas y otras que le sean aplicables.

3. **Infracciones Graves:** se consideran infracciones graves, entre otras de similar naturaleza, las siguientes:

a. Operar servicios o actividades no comprendidas en la licencia o registro otorgado por el BCN, o iniciar operaciones de servicios adicionales sin la autorización de inicio de operaciones del BCN, en contravención a los artículos 4 y 7.
b. No solicitar la no objeción previa del BCN para el nombramiento y/o sustitución del Gerente General, cambios de domicilio, traspasos de titularidad de acciones significativos, fusión, escisión, o suspensión temporal voluntaria de operaciones, conforme a lo dispuesto en el artículo 15 y artículo 26, literal m).
c. Ceder, transferir, enajenar u otorgar en garantía la autorización para operar, en contravención al artículo 9.
d. Incumplir con los requisitos mínimos de la plataforma tecnológica establecidos en el artículo 11, de forma que se comprometa gravemente la confidencialidad, integridad, disponibilidad o trazabilidad de las operaciones o datos, o la seguridad de los fondos o activos de los clientes.
e. Para los PSP emisores de dinero electrónico, incumplir con el artículo 16, literales a) y b).
f. Para los PSP emisores de dinero electrónico, pagar u ofrecer intereses o cualquier forma de rendimiento financiero sobre los saldos de dinero electrónico, en contravención al artículo 16, literal d).
g. Para los PSAV, no salvaguardar los fondos en moneda fiduciaria de los clientes en CMAV segregadas, conforme al artículo 19, literal c).
h. Para los PSAV, incumplir cualquiera de las prohibiciones operativas específicas establecidas en el artículo 23, tales como ofrecer servicios de mezcladores, soportar criptomonedas de anonimato mejorado, o facilitar el "salto de cadenas" con fines de ofuscación.
i. Presentar al BCN información o documentación falsa o sustancialmente inexacta en el proceso de solicitud de licencia, registro, autorización de inicio de operaciones, o en respuesta a requerimientos de supervisión.
j. Incumplir con la obligación de mantener el capital social mínimo requerido por la Norma.
k. Realizar actos que pongan en grave riesgo la seguridad y la eficiencia del Sistema de Pagos Nacional o la estabilidad del Sistema Financiero Nacional, a criterio del BCN.
l. La reincidencia en la comisión de tres o más infracciones graves en un período de un (1) año.
m. Operar como PSP o PSAV sin contar con la licencia o registro del BCN, o continuar operando tras la suspensión o revocación de la misma.

La Administración Superior del BCN impondrá la multa correspondiente a la infracción cometida, dentro del rango establecido para cada categoría (Leve, Moderada, Grave) con base en lo establecido en el artículo 147 de la Ley 1232, considerando las circunstancias atenuantes y agravantes previstas en el artículo 10 de la Norma.

Las multas se calcularán sobre el valor absoluto del patrimonio del PSP o PSAV registrado en el último estado financiero disponible. Asimismo, estas deberán depositarse en la cuenta en el BCN a favor de la TGR, en un plazo no mayor de cinco (5) días hábiles una vez se encuentren firmes.

El plazo para subsanar o solventar las indicaciones del BCN derivadas de la comisión de infracciones no deberá ser mayor a seis (6) meses. Se exceptúan los casos que, a solicitud debidamente fundamentada por la entidad, requieran una ampliación de plazo. El BCN decidirá con total independencia si se acepta o no dicha solicitud.

Artículo 31. Suspensión temporal y revocación de la licencia. La Administración Superior del BCN suspenderá temporalmente o revocará la licencia o registro otorgado a un PSP o PSAV cuando se presenten las siguientes causales:

Causas de suspensión temporal:

a. No mantener el capital social mínimo establecido en el artículo 6 de la Norma, otorgándose un plazo para su adecuación. Si transcurrido dicho plazo no se regulariza la situación, se procederá con la revocación.
b. Cuando una autoridad judicial competente lo ordene, conforme sentencia firme.
c. Cuando el PSP o PSAV incumpla reiteradamente las instrucciones o requerimientos del BCN emitidos en el ejercicio de sus funciones de vigilancia y supervisión.
d. Cuando el PSP o PSAV ponga en riesgo la seguridad y la eficiencia del Sistema de Pagos Nacional o del Sistema Financiero Nacional a criterio del BCN.
e. Por solicitud expresa y justificada del PSP o PSAV para una suspensión voluntaria de operaciones, conforme al artículo 26, literal m), sub-literal iv), siempre que no afecte los derechos de los usuarios o la estabilidad del sistema, y por el plazo que el BCN determine.
f. Cuando por alguna circunstancia, así lo determine el BCN.

Causas de revocación:

a. Si el PSP o PSAV no solicita la autorización de inicio de operaciones dentro del plazo de doscientos cincuenta (250) días contados desde la entrada en vigencia de la licencia, o si, habiéndola solicitado, no cumple con los requisitos o no subsana las omisiones en el plazo concedido.
b. Si, habiendo obtenido la aprobación para un servicio adicional, no solicita la autorización de inicio de operaciones para dicho servicio dentro del plazo de doscientos cincuenta (250) días. En este caso se le revocará el registro del servicio específico.
c. Cuando se les otorgue licencia o registro de operación como PSP o PSAV y no inicien operaciones en un lapso de un (1) año posterior a la entrada en vigencia de la licencia y/o registro.

d. Cuando se les otorgue la aprobación para un servicio adicional, y no inicien operaciones en un lapso de un (1) año posterior a dicha autorización. En este caso se le revocará el registro del servicio específico.
e. Por la interrupción de la totalidad de sus operaciones autorizadas o de los principales servicios esenciales autorizados, por un período superior a un (1) año.
f. Por la disolución y liquidación de la sociedad titular de la licencia o registro, o por la declaración de quiebra.
g. Cuando se compruebe que la licencia o registro fue obtenido mediante la presentación de información o documentación falsa o sustancialmente inexacta.
h. Por la comisión de infracciones graves que, por su naturaleza, reincidencia, o el grave perjuicio causado a los usuarios, al sistema de pagos o a la confianza pública, así lo ameriten, a criterio del BCN.
i. Si, habiendo sido suspendida temporalmente la licencia o registro, el PSP o PSAV no subsana las causas que motivaron la suspensión dentro del plazo otorgado por el BCN, o si durante el período de suspensión incumple las directrices impartidas.
j. Por realizar actividades ilícitas o fraudulentas comprobadas mediante sentencia judicial firme, o por facilitar de manera sistemática y dolosa la comisión de dichas actividades a través de sus servicios.
k. Cuando, a criterio del BCN, el PSP o PSAV haya perdido las condiciones de idoneidad técnica, financiera o de gobernanza que fueron determinantes para el otorgamiento de la licencia o registro, y dicha pérdida ponga en grave riesgo la continuidad del servicio o los intereses de los usuarios.

La resolución de suspensión o revocación deberá ser notificada formalmente al PSP o PSAV afectado y, en caso de revocación, se gestionará su publicación en La Gaceta, Diario Oficial. El BCN comunicará dichas resoluciones a la UAF, SIBOIF y CONAMI, según corresponda, conforme al artículo 6. Las licencias o registros suspendidos o revocados se publicarán en la web del BCN.

CAPÍTULO XI
DISPOSICIONES TRANSITORIAS Y FINALES

Artículo 32. Plazo de adecuación para proveedores existentes. Los PSP que se encuentren operando a la fecha de entrada en vigencia de la Norma, en virtud de autorización otorgada bajo la Resolución CD-BCN-XXV-1-22 y sus reformas, dispondrán de los siguientes plazos para adecuarse a las disposiciones de la Norma y del presente Reglamento:

a. Hasta el 18 de diciembre de 2026, para ajustar su capital social mínimo al requerido en el artículo 6 de la Norma. Deberán presentar al BCN la evidencia del cumplimiento de dicha adecuación dentro de este plazo.
b. Hasta el 29 de mayo de 2026, para adecuar su plataforma tecnológica a los requisitos establecidos en el Capítulo III y otras disposiciones tecnológicas aplicables de este Reglamento.
c. Hasta el 29 de mayo de 2026, para implementar los ajustes necesarios para cumplir con los requisitos de gestión de riesgos, control interno, operativos específicos y obligaciones generales establecidos en los Capítulos IV, VI, VII y VIII de este Reglamento, así como con las demás obligaciones contenidas en la Norma.
d. Los Gerentes Generales de los PSP existentes que se encuentren en funciones a la fecha de entrada en vigencia de la Norma no requerirán someterse nuevamente al proceso de no objeción previsto en el Capítulo V (artículo 15) de este Reglamento, mientras continúen ininterrumpidamente en dicho cargo dentro de la misma entidad autorizada.

Artículo 33. Reclasificación de servicios y actualización de licencias y registros[2]**.** La División de Operaciones Financieras del BCN, procederá a reclasificar los servicios y actividades autorizados a los PSP existentes bajo la Resolución CD-BCN-XXV-1-22, con el propósito de ajustarlos a las categorías de servicios definidas en el artículo 4 de la Norma. Asimismo, propondrá a la Administración Superior del BCN la incorporación en las respectivas licencias y constancias de registro de aquellos servicios contemplados en dicho artículo 4 que, sin haber sido autorizados previamente por el BCN, los proveedores ya ofrezcan.

Como parte del proceso, el BCN verificará la reclasificación de los servicios de cada proveedor y, de ser necesario, dispondrá los ajustes pertinentes. La emisión de las nuevas licencias y constancias de registro resultantes de la reclasificación e incorporación señaladas, se realizará sin costo alguno. Dicho proceso de actualización y la correspondiente notificación a cada proveedor deberán completarse a más tardar el doce de septiembre de dos mil veinticinco. Las licencias y constancias de registro surtirán efectos desde su notificación. En el caso de las licencias, su efecto será válido sin perjuicio de su posterior publicación en La Gaceta, Diario Oficial, por parte del proveedor.

Artículo 34. Vigencia. El presente Reglamento entrará en vigencia a partir de su aprobación, sin perjuicio de su posterior publicación.

(Hasta acá el texto de la Resolución)

[2] Artículo 33, reformado el 23 de julio de 2025 - Resolución Administrativa GG-13-JULIO-2025-LASMF-DO.

ANEXO 1

Banco Central de Nicaragua
Emitiendo confianza y estabilidad

FORMATO DE SOLICITUD DE LICENCIA Y/O REGISTRO DE OPERACIÓN DE LOS PROVEEDORES DE TECNOLOGÍA FINANCIERA DE SERVICIOS DE PAGO Y DE LOS PROVEEDORES DE SERVICIO DE ACTIVOS VIRTUALES

I. DATOS DE LA ENTIDAD

Nombre de la empresa:
Nombre comercial:
Objeto social:
Número RUC:
Dirección:
Ciudad:
Teléfono:
Correo electrónico:
Descripción de la actividad de la entidad:

Años de antigüedad del negocio:
Apartado postal:
Sitio web:
Coordenadas de geolocalización de empresa:

CONSTITUCION Y REGISTRO
Fecha de constitución:
No. Escritura de constitución:

Datos de Inscripción
Fecha de inscripción en Registro Público:
Tomo/Folio/Asiento
Número único de folio personal:
Registro Público de la ciudad de:

REFORMAS A CONSTITUCION Y REGISTRO (EN CASO DE APLICAR)
Fecha de reforma:
No. Escritura:

Fecha de inscripción en Registro Público:
Tomo/Folio/Asiento
Número único de folio personal:
Registro Público de la ciudad de:

II. DATOS DEL REPRESENTANTE LEGAL O APODERADO

REPRESENTANTE LEGAL O APODERADO
Primer nombre:
Primer apellido:
Estado civil:

Segundo nombre:
Segundo apellido:
Sexo:
Masculino: ☐
Femenino: ☐

Fecha de nacimiento:
Nacional — No. Cédula:
Extranjero residente — No. Cédula residencia:
Extranjero no residente — No. Pasaporte:
País de nacionalidad:
Dirección actual donde reside:
Ciudad/País de nacionalidad
No. Teléfono oficina:
No. Celular:

País de nacimiento:
Fecha de expiración:
Fecha de expiración:
Fecha de expiración:

Correo electrónico institucional:
Correo electrónico personal:

ACTIVIDAD QUE DESEMPEÑA EL REPRESENTANTE LEGAL O APODERADO
Cargo o puesto que desempeña:
Profesión u Oficio:
Antigüedad en el Puesto:

Datos de Inscripción del Poder
Fecha de escritura:
No. Escritura:
Fecha de inscripción en Registro Público:
Tomo/Folio/Asiento
Número único de folio personal:
Registro Público de la ciudad de:

III. JUNTA DIRECTIVA (Conforme certificación del Órgano Societario correspondiente, que refiera a los integrantes de la Junta Directiva Vigente)

Nombres y apellidos	Cargo	N° de identificación	Nacionalidad

IV. LISTA DE ACCIONISTAS Y DE LOS BENEFICIARIOS FINALES (BENEFICIARIO FINAL: Persona Natural)

Nombres y Apellidos	Nacionalidad	N° de identificación	Nombres y Apellidos del Representante legal	Nacionalidad del Representante legal	N° de identificación de representante legal	Participación (%)

(Continúa)

Banco Central de Nicaragua
Emitiendo confianza y estabilidad

FORMATO DE SOLICITUD DE LICENCIA Y/O REGISTRO DE OPERACIÓN DE LOS PROVEEDORES DE TECNOLOGÍA FINANCIERA DE SERVICIOS DE PAGO Y DE LOS PROVEEDORES DE SERVICIO DE ACTIVOS VIRTUALES

V. FUNCIONARIOS PRINCIPALES

Nombres y apellidos	Cargo	N° de identificación	Nacionalidad

VI. DATOS FINANCIEROS DE LA INSTITUCIÓN

Información del último Estado de Resultados disponible (en córdobas)

Período:	
Ingresos anuales:	C$
Egresos anuales:	C$
Total (Ingresos-Egresos):	C$

Información del último Balance General disponible (en córdobas)

Al corte del:	
Activos:	C$
Pasivos:	C$
Patrimonio:	C$

VII. SERVICIOS PARA LOS QUE SOLICITA LICENCIA O REGISTRO

Servicios de tecnología financiera de servicios de pago para los que se solicita Licencia o Registro:

Servicios de ejecución de órdenes de pago ☐ Servicios de aceptación de pagos para comercios ☐ Emisión y administración de dinero electrónico ☐ Emisión de instrumentos de pago ☐

Administración de redes de cajeros automáticos ☐ Servicios de compraventa e intercambio de divisas de forma electrónic ☐ Otros servicios de pago relacionados ☐

Servicios de activos virtuales para los que se solicita Licencia o Registro:

Intercambio entre activos virtuales y monedas fia ☐ Intercambio entre una o más formas de activos virtuale ☐ Transferencia de activos virtuales ☐ Custodia y/o administración de activos virtuales ☐

Participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo vir ☐ Otros servicios de activos virtuales ☐

Descripción de los servicios y operaciones a ofrecer:

VIII. INSTITUCIONES FINANCIERAS NACIONALES O EXTRANJERAS EN LAS QUE LA ENTIDAD MANTIENE DEPÓSITOS

Nombre de la institución financiera	Moneda de la cuenta (córdoba / dólar/ euro)

IX. PARIENTES QUE LABORAN EN EL BCN O FORMAN PARTE DE LA DIRECCIÓN SUPERIOR (de los socios, miembros de la junta directiva y del representante legal, si aplica)

Nombre y apellidos	Grado de parentesco	Área o dependencia en el BCN en la que labora

Declaro que los datos que anteceden son verídicos, sometiéndome a las sanciones que la ley determina por cualquier inexactitud de los mismos.

Llenado en la ciudad de _____ a los _____ días del mes de _____ del año _____

_____
Representante legal

ANEXO 2
Formato de Currículum

I. DATOS GENERALES

Nombre completo:	
Nacionalidad:	
Profesión u oficio:	
Lugar y fecha de nacimiento:	
Número de Cédula de Identidad:	
Cédula de Residencia (en el caso de extranjeros residentes en el país):	
Número de Pasaporte (en el caso de extranjeros no residentes en el país):	
Domicilio:	
Condición migratoria:	
¿Tiene autorización para trabajar en el país?	
Sí ( ) No ( )	
Número de autorización:	
Fecha de autorización:	
Vigencia de la autorización:	

II. FORMACIÓN ACADÉMICA Y CONOCIMIENTOS

A. Educación superior formal. (Indique sus títulos universitarios, maestrías, doctorados, etc. Adjunte copias certificadas).

Nombre de la Institución Educativa	Título Obtenido	Período (Mes/Año Inicio – Mes/Año Fin)	Observaciones (Opcional)

B. Capacitación especializada, certificaciones y conocimientos adicionales relevantes. (Detalle cursos, certificaciones, diplomados y otros conocimientos significativos en economía, finanzas, tecnología de la información, ingeniería, administración, cumplimiento normativo, gestión de riesgos. Para Gerentes Generales de PSAV, es crucial detallar cualquier formación, certificación o experiencia demostrable en ecosistemas blockchain, criptografía aplicada, desarrollo o gestión de plataformas de activos virtuales, y tecnologías Web3, conforme al artículo 14 literal b) del Reglamento).

Descripción del Curso/Certificación/Conocimiento	Institución Emisora / Modalidad (si aplica)	Período o Fecha de Obtención	Observaciones (Opcional)

III. EXPERIENCIA PROFESIONAL

(Detalle su experiencia laboral, con énfasis en aquella relevante para el cargo y el sector. Se requiere un mínimo de tres (3) años de experiencia relevante en puestos de responsabilidad, según artículo 14 literal a) del Reglamento. Para cada puesto, describa las principales funciones, responsabilidades y logros, destacando la experiencia en: sector bancario, sector tecnológico, medios de pago, y/o específicamente en ecosistemas blockchain, criptografía aplicada, o plataformas de activos virtuales, u otros sectores de magnitud y complejidad equivalentes.)

Nombre de la Entidad/Empresa	Cargo(s) Desempeñado(s)	Período (Mes/Año Inicio – Mes/Año Fin)	Principales Funciones Desempeñadas y Logros Relevantes

Declaro que los datos que anteceden son verídicos, sometiéndome a las sanciones que la ley determina por cualquier inexactitud de los mismos.

Lugar y fecha:

Firma:

Nombre completo: