LIBRO I.- NORMAS DE CONTROL PARA LAS ENTIDADES DE LOS SECTORES FINANCIEROS PÚBLICO Y PRIVADO

TÍTULO XXI.- DE LA SUPERVISIÓN Y CONTROL DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS (Creado con Resolución No. SB-2025-02325 de 25 de septiembre de 2025)

CAPÍTULO I.- NORMA PARA LA SUPERVISIÓN Y CONTROL DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS; Y, DE LAS ACTIVIDADES FINTECH DE LAS SOCIEDADES ESPECIALIZADAS DE DEPÓSITOS Y PAGOS ELECTRÓNICOS (Expedido con Resolución No. SB-2025-02325 de 25 de septiembre de 2025)

SECCIÓN I.- GENERALIDADES

ARTÍCULO 1.- Objetivo y ámbito. La presente norma de control tiene como objetivo establecer los requisitos, políticas, procesos, procedimientos de supervisión y control aplicables para las entidades de servicios financieros tecnológicos; y, a las Sociedades Especializadas de Depósitos y Pagos Electrónicos, según corresponda.

ARTÍCULO 2.- Principios. La regulación, supervisión y control se basará en los siguientes principios:

a) **Inclusión Financiera:** Acceso y uso de productos y servicios financieros regulados y de calidad por parte de personas y empresas capaces de elegir de manera informada. Los productos y servicios financieros deben ofrecerse de forma transparente, responsable y sostenible, y deben responder a las necesidades de la población.

b) **Transparencia:** Provisión de información veraz, clara, comprensible y oportuna a usuarios, inversionistas y reguladores, respecto de la procedencia, licitud, destino y uso de fondos o activos que se vean involucrados en las operaciones, políticas y condiciones de los servicios financieros tecnológicos.

c) **Protección del Consumidor:** Garantizar la protección de los derechos de los consumidores, incluyendo la privacidad de los datos y la seguridad de la información.

d) **Estabilidad y solvencia Financiera:** Precautelar la estabilidad del sistema financiero y la solidez financiera de las entidades que lo conforman.

e) **Proporcionalidad:** Aplicación de estructuras y controles en función del tamaño, complejidad y riesgo y naturaleza de las operaciones de la entidad.

SECCIÓN II.- DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS DE CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 3.- Prohibición de intermediación. Según lo dispuesto en el numeral 1 del artículo 439.1 del Código Orgánico Monetario y Financiero, los productos de crédito que se ofrezcan a través de plataformas electrónicas no implican la captación de recursos del público con finalidad de intermediación.

ARTÍCULO 4.- Productos. Las entidades de concesión digital de créditos solamente podrán otorgar los productos de: concesión de crédito directo y emisión de tarjeta de crédito.

Conforme al segmento de crédito deberán constituirse las garantías establecidas por la Junta de Política y Regulación Financiera y Monetaria.

ARTÍCULO 5.- Operación de tarjetas de crédito. Para operar con el producto de tarjetas de crédito, se deberá cumplir con lo dispuesto en el Capítulo de la "Norma que regula las operaciones de las tarjetas de crédito, débito y de pago emitidas y/u operadas por las entidades financieras bajo el control de la Superintendencia de Bancos", Título II "Sistema Financiero Nacional", Libro I "Sistema Monetario y Financiero" de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros.

ARTÍCULO 6.- Segmento de crédito. Las entidades de concesión digital de créditos operarán en los segmentos de crédito que contemple la normativa vigente, en función de la tecnología crediticia evaluada por la Superintendencia de Bancos en el estudio de factibilidad presentado para la calificación.

SUBSECCIÓN I.- POLÍTICAS Y PROCESOS INTERNOS DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS DE CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 7.- Políticas para el otorgamiento de créditos. Las entidades, para prestar los servicios, deben establecer políticas de otorgamiento de créditos digitales que definan los criterios y procesos utilizados para evaluar la solvencia y el riesgo crediticio de los solicitantes, de conformidad con las disposiciones del Código Orgánico Monetario y Financiero, así como, de la Junta de Política y Regulación Financiera y Monetaria aplicables para tales efectos.

Estas políticas deben garantizar que la toma de decisiones de crédito sea objetiva, basada en datos precisos y no discriminatorios. Deben incluir, entre otros aspectos, los criterios de elegibilidad, los límites de crédito y las tasas de interés aplicables de conformidad a los criterios emitidos por la Junta de Política y Regulación Financiera y Monetaria.

ARTÍCULO 8.- Políticas, procesos y procedimientos de gestión de riesgos. Las entidades calificadas, para prestar los servicios, deben contar con políticas de gestión de riesgos que incluyan la identificación, medición, control y monitoreo de los riesgos asociados a la concesión de créditos digitales, tales como, riesgo de crédito, de mercado, operativo y de liquidez.

ARTÍCULO 9.- Procesos de evaluación y aprobación de solicitudes de crédito. Las entidades calificadas, para prestar los servicios, deben definir procesos para la evaluación y aprobación de solicitudes de crédito. Estos procesos deben ser claros y eficientes, garantizando una respuesta rápida a los solicitantes de conformidad con lo determinado por la Junta de Política y Regulación Financiera y Monetaria aplicable para tales efectos.

Deberán definir procedimientos para la verificación de la identidad de los usuarios y solvencia de los solicitantes, así como para la validación de la información proporcionada a través de una adecuada infraestructura tecnológica, de seguridad de la información y de protección de datos personales, conforme lo detallado en la norma de control expedida para el efecto.

ARTÍCULO 10.- Procesos de originación y desembolso de créditos. Las entidades de concesión digital de créditos, para su calificación, deberán contar con procesos de

originación y desembolso de créditos que aseguren la correcta documentación de las transacciones y la seguridad en el desembolso de los fondos.

Estos procesos deben incluir mecanismos de validación de la información del solicitante, así como controles para evitar fraudes y errores en la originación y desembolso de créditos.

ARTÍCULO 11.- Procesos de monitoreo y seguimiento de cartera. Las entidades deben establecer procesos de monitoreo y seguimiento de la cartera de créditos digitales, incluyendo el seguimiento de pagos, la gestión de morosidad y la toma de medidas correctivas.

Deben llevar un registro actualizado de la calidad de la cartera y establecer procedimientos para la recuperación de créditos en caso de incumplimiento por parte de los deudores.

ARTÍCULO 12.- Procesos de recuperación. Las entidades calificadas, para prestar servicios financieros tecnológicos de concesión digital de créditos, deben establecer procedimientos de recuperación de cartera efectivos éticos y ajustados a lo que la normativa vigente establece sobre los derechos del consumidor y usuario en los procesos de cobranza, para gestionar los préstamos y garantizar la recuperación oportuna de los fondos pendientes.

Los procesos de recuperación de cartera deben incluir, al menos:

1. Estrategias de comunicación y notificación a los deudores en mora con el propósito de recordarles sus obligaciones y establecer acuerdos de pago.
2. La asignación de recursos y personal capacitado para la gestión de morosidad.
3. La evaluación de alternativas de recuperación, que pueden incluir, por ejemplo, acuerdos de reestructuración de deudas, planes de pago escalonados o la recuperación de garantías en caso de préstamos garantizados.
4. Un seguimiento minucioso de los pagos y el mantenimiento de registros precisos de las acciones tomadas en el proceso de recuperación de cartera.
5. Las entidades deben asegurarse de que todas las prácticas de recuperación de cartera respeten los derechos de los usuarios financieros y se realicen de conformidad con las leyes y regulaciones aplicables, evitando prácticas abusivas o coercitivas hacia los deudores.

SUBSECCIÓN II.- PROCEDIMIENTOS PARA LA CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 13.- Procedimientos de identificación y autenticación del cliente. Para la concesión digital de créditos, las entidades deben implementar mecanismos de seguridad en sus plataformas, de acuerdo con lo establecido en la norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos expedida para el efecto, así como las normas de protección de datos personales vigente.

ARTÍCULO 14.- Procedimientos de scoring y modelización de riesgos. Las entidades de concesión digital de créditos deberán implementar sistemas de scoring y modelización de riesgos para evaluar la solvencia y el riesgo crediticio de los solicitantes; así como, el seguimiento de los créditos desembolsados para estimar las pérdidas esperadas. Estos sistemas deben ser objetivos y basados en datos precisos y podrán ser propios o proporcionados por un tercero.

ARTÍCULO 15.- Procedimientos de gestión de cobranzas. Las entidades de concesión digital de créditos deberán establecer procedimientos de gestión de cobranzas para el seguimiento de los pagos de los deudores y la gestión de la morosidad.

ARTÍCULO 16.- Procedimientos de informes y reportes. Las entidades de concesión digital de créditos deberán mantener procedimientos para la generación de informes o reportes contables, financieros y de riesgos.

Los informes deben contener datos relevantes sobre las operaciones de la cartera de créditos, la solidez financiera y demás información que el organismo de control lo requiera.

SUBSECCIÓN III.- DEL GOBIERNO CORPORATIVO DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS DE CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 17.- Estructura de gobierno corporativo. Las entidades deberán aplicar los principios de buen gobierno corporativo, incorporando en sus estatutos y reglamentos, manuales de políticas internas y en la estructura organizacional, lo previsto en los "Principios de un Buen Gobierno Corporativo" contenidos en la Codificación de las Normas de la Superintendencia de Bancos", promoviendo la toma de decisiones, la supervisión y la rendición de cuentas en la organización.

Como parte de la estructura de gobierno corporativo se deberá incluir, al menos, un Comité de Administración integral de riesgos, un Comité de Auditoría, un Comité de Tecnología y Seguridad de la Información, así como, otros comités que consideren necesarios, según su modelo de negocio.

ARTÍCULO 18.- Unidad de Riesgos. Las entidades establecerán una Unidad de Riesgos que deberá contar de manera permanente con los recursos humanos, materiales y tecnológicos necesarios y suficientes para ejecutar sus funciones. La unidad estará compuesta por personal capacitado que demuestre un sólido conocimiento y experiencia en el manejo y control de riesgos y que sea capaz de comprender las metodologías y procedimientos de la entidad para identificar, medir, controlar, mitigar y supervisar los riesgos presentes y futuros.

ARTÍCULO 19.- Funciones de los comités y la unidad de riesgos. Las funciones de los comités previamente señalados y de la Unidad de Riesgos corresponden a las establecidas por la Junta de Política y Regulación Financiera y Monetaria y por la Superintendencia de Bancos, en las normas de regulación y control emitidas.

ARTÍCULO 20.- Divulgación de información financiera y operativa. Las entidades tecnológicas deben mantener la transparencia en la divulgación de información financiera y operativa. Esto incluye la publicación de informes financieros, así como la comunicación clara de las políticas, condiciones y términos de sus servicios.

La entidad debe proporcionar información adecuada para que los clientes comprendan los costos, los riesgos y los términos asociados al servicio contratado.

SUBSECCIÓN IV.- ADMINISTRACIÓN INTEGRAL DE RIESGOS DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS DE CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 21.- Administración de riesgos. Las entidades deben llevar a cabo una administración integral de los riesgos asociados a los servicios financieros tecnológicos, incluyendo los riesgos crediticios, de liquidez, de mercado, de tasa de interés, riesgo de tipo de cambio, riesgo operativo, legal, reputacional, sistémico, y de lavado de activos y la financiación de otros delitos, conforme lo detallado en la norma definida para el efecto.

Deben clasificar los riesgos identificados y mantener un registro actualizado de estos, con la finalidad de implementar medidas de mitigación apropiadas.

ARTÍCULO 22.- Evaluación y clasificación de riesgos. Las entidades que soliciten la calificación deben llevar a cabo una evaluación integral de los riesgos asociados a los servicios financieros tecnológicos, incluyendo los riesgos crediticios, de liquidez, de mercado, de tasa de interés, riesgo de tipo de cambio, riesgo operativo, de lavado de activos y del financiamiento de delitos, legal, reputacional y sistémico.

Deben clasificar los riesgos identificados y mantener un registro actualizado de estos, con la finalidad de implementar medidas de mitigación apropiadas.

Las entidades de servicios financieros tecnológicos para el servicio ofertado deben implementar lo pertinente para la administración de riesgos operativos en sus plataformas, conforme con lo establecido en el Capítulo “Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos”, Título IX “De la gestión y administración de riesgos”, Libro I “Normas de Control para las entidades de los sectores financieros público y privado”, y la Norma de Administración Integral de Riesgos.

ARTÍCULO 23.- Evaluación de riesgos de ciberseguridad y seguridad de la información. Las entidades tecnológicas para el servicio ofertado deben implementar mecanismos de monitoreo a sus plataformas, conforme lo detallado en la norma expedida para el efecto.

ARTÍCULO 24.- Monitoreo y control de riesgos operativos. Las entidades de servicios financieros tecnológicos deben implementar mecanismos de monitoreo y control a sus plataformas, conforme con lo establecido en la “Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos”, Título “De la gestión y administración de riesgos”, Libro I “Normas de Control para las entidades de los sectores financiero público y privado” de la Codificación de las Normas de la Superintendencia de Bancos.

ARTÍCULO 25.- Riesgo de lavado de activos. Las entidades de concesión digital de créditos deben implementar los mecanismos, procesos y procedimientos conforme lo estipula el Capítulo de la “Norma de control para la prevención y administración del riesgo de lavado de activos y la financiación de otros delitos (PARLAFD)”, Título “De la gestión y administración de riesgos”, Libro I “Normas de Control para las entidades de los sectores financieros público y privado”, de la Codificación de las Normas de la Superintendencia de Bancos.

SUBSECCIÓN V.- CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS DE CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 26.- Las entidades que ejerzan las actividades de Servicios Financieros Tecnológicos, así como las Sociedades Especializadas de Depósitos y Pagos Electrónicos y las Administradoras de Sistemas Auxiliares de Pago (ASAP), deberán cumplir con lo establecido en la Sección de “Seguridad de la Información”, del Capítulo de la “Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos”, Título IX “De la gestión y administración de riesgos”, Libro I “Normas de control para las entidades de los sectores financieros público y privado”, de la Codificación de las Normas de la Superintendencia de Bancos.

ARTÍCULO 27.- Políticas y procedimientos de seguridad de la información. Estas entidades deben implementar políticas y procedimientos de seguridad de datos que garanticen la confidencialidad, integridad y disponibilidad de la información sensible.

Estas políticas y procedimientos deben abordar la gestión de contraseñas, el cifrado de datos, el control de acceso y otras prácticas de seguridad.

ARTÍCULO 28.- Protección contra amenazas cibernéticas. Estas entidades deben establecer medidas de protección contra amenazas cibernéticas, incluyendo la detección y prevención de intrusiones, así como la mitigación de ataques maliciosos.

Deben contar con sistemas de monitoreo de seguridad que alerten sobre actividades inusuales o potenciales amenazas.

ARTÍCULO 29.- Plan de respuesta a incidentes de seguridad. Estas entidades deben desarrollar un plan de respuesta a incidentes de seguridad que establezca procedimientos claros para la identificación, notificación, contención y recuperación de incidentes de seguridad.

Deben designar un equipo de respuesta a incidentes y capacitar a su personal en la ejecución de este plan.

ARTÍCULO 30.- Capacitación en ciberseguridad. Estas entidades deben proporcionar capacitación continua en ciberseguridad a su personal para garantizar una comprensión adecuada de las amenazas y las mejores prácticas de seguridad.

Deben promover la conciencia de seguridad entre los empleados y usuarios.

ARTÍCULO 31.- Auditorías y pruebas de seguridad. Estas entidades deben realizar auditorías periódicas de seguridad de la información y pruebas de vulnerabilidad para evaluar la efectividad de las medidas de seguridad implementadas, al menos, una vez al año.

Deben corregir las vulnerabilidades identificadas y mantener registros de las auditorías y pruebas realizadas.

SUBSECCIÓN VI.- RÉGIMEN CONTABLE DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS DE CONCESIÓN DIGITAL DE CRÉDITOS

ARTÍCULO 32.- Las entidades de concesión digital de créditos aplicarán el régimen contable expedido por la Superintendencia de Bancos.

SECCIÓN III.- DE LA SUPERVISIÓN Y CONTROL DE LAS ENTIDADES DE ADMINISTRACIÓN DE FINANZAS PERSONALES

SUBSECCIÓN I.- POLÍTICAS Y PROCESOS INTERNOS DE LAS ENTIDADES DE ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 33.- Políticas para la administración de finanzas personales. Las entidades, para prestar los servicios de administración de finanzas personales, deben establecer políticas que definan los criterios y procesos utilizados para evaluar la situación financiera de los usuarios y sus expectativas, objetivos y metas financieras, así como las alternativas de administración financiera disponibles, de ser el caso, de conformidad con las disposiciones del Código Orgánico Monetario y Financiero, así como, de la Junta de Política y Regulación Financiera y Monetaria aplicables para tales efectos.

Estas políticas deben garantizar que la toma de decisiones por parte de los usuarios sea objetiva, basada en datos precisos y no discriminatorios.

ARTÍCULO 34.- Políticas, procesos y procedimientos de gestión de riesgos. Las entidades, para prestar los servicios de administración de finanzas personales, deben contar con políticas de gestión de riesgos que incluyan la identificación, medición, control y monitoreo de los riesgos asociados, para lo cual deberán tomar en cuenta al menos lo detallado en la normativa vigente.

SUBSECCIÓN II.- PROCEDIMIENTOS PARA LAS ENTIDADES DE ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 35.- Procedimientos de identificación y autenticación del usuario. Para la administración de finanzas personales, las entidades deben implementar mecanismos de seguridad en sus plataformas, así como, las normas de protección de datos personales vigentes.

ARTÍCULO 36.- Procedimientos de modelización de riesgos. Las entidades de administración de finanzas personales deberán implementar sistemas de modelización de riesgos para evaluar la situación financiera de los usuarios; así como, las diferentes alternativas de administración financiera disponibles. Estos sistemas deben ser objetivos y basados en datos precisos y podrán ser propios o proporcionados por un tercero.

Las entidades de administración de finanzas personales podrán implementar modelos, algoritmos o herramientas automatizadas, con la finalidad de robustecer la precisión del análisis, los cuales deberán contar con una fundamentación técnica y metodológica que garantice su validez y fiabilidad. De la misma forma, estos deberán cumplir con lo establecido en la norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos.

ARTÍCULO 37.- Procedimientos de limitación de pérdidas para los usuarios financieros. Las entidades de administración de finanzas personales implementarán procedimientos operativos y/o tecnológicos, para la determinación de niveles de tolerancia a pérdidas predefinidos que permitan proteger los recursos dispuestos por el usuario en los productos financieros administrados o recomendados por la entidad, para lo cual deberá tomar las siguientes acciones:

1. Cierre automático de posiciones ante riesgos de pérdidas superiores al recurso gestionado del usuario;
2. Alertas tempranas y notificaciones sobre fluctuaciones en el valor de las inversiones;
3. Otros que determine la Superintendencia de Bancos.

ARTÍCULO 38.- Procedimientos de informes y reportes. Las entidades de administración de finanzas personales mantendrán procedimientos para la generación de informes necesarios para su gestión, los mismos que deberán ser contables, financieros y de riesgos.

Los informes deben contener datos relevantes sobre las operaciones de la entidad, su solidez financiera y demás información requerida por el Organismo de Control, y deberán ser remitidos en la forma y periodicidad que para el efecto determine la Superintendencia de Bancos.

SUBSECCIÓN III.- DEL GOBIERNO CORPORATIVO DE LAS ENTIDADES DE ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 39.- Principios del gobierno corporativo. Las entidades sujetas a esta norma deberán regirse, como mínimo, por los siguientes principios:

a) **Transparencia:** Provisión de información veraz, clara, comprensible y oportuna a usuarios, inversionistas y reguladores.

b) **Responsabilidad:** Actuación diligente y cumplimiento de deberes fiduciarios por parte de sus órganos de administración.

c) **Equidad:** Trato justo y no discriminatorio entre socios, usuarios y demás partes interesadas.

d) **Gestión de riesgos:** Identificación, evaluación y mitigación de riesgos estratégicos, operacionales, tecnológicos y financieros.

e) **Proporcionalidad:** Aplicación de estructuras y controles en función del tamaño, complejidad y riesgo operativo de la entidad.

SUBSECCIÓN IV.- ESTRUCTURA DEL GOBIERNO CORPORATIVO DE LAS ENTIDADES DE ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 40.- Órgano de administración. Toda entidad de administración de finanzas personales deberá contar con una Junta Directiva u órgano equivalente responsable de la dirección estratégica y supervisión de la gestión. La composición mínima será de tres (3) y máxima de cinco (5) miembros, conforme a los siguientes umbrales:

Factor	Umbral	Aplicación
Volumen de activos	> USD 2 millones	Requiere cinco miembros
Número de clientes activos	> 10.000 usuarios	Requiere cinco miembros

Se considerará la naturaleza emergente de las entidades administración de finanzas personales para aplicar estructuras proporcionales.

ARTÍCULO 41.- Funciones del órgano de administración. Corresponde a la Junta Directiva u órgano equivalente:

- Aprobar políticas internas y de gestión de riesgos.
- Nombrar y supervisar al gerente general.
- Designar al auditor interno.
- Conocer y resolver los informes de auditoría.
- Asegurar la sostenibilidad, transparencia y cumplimiento normativo de la entidad.
- Aprobar el plan estratégico .

ARTÍCULO 42.- Gerencia general. La ejecución de la operación estará a cargo del Gerente General, en apego a las directrices estratégicas del órgano de administración y en cumplimiento de las políticas internas y normativas aplicables.

SUBSECCIÓN V.- DE LOS COMÍTES DE APOYO DE LAS ENTIDADES ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 43.- Comités mínimos requeridos. Las entidades deberán contar con al menos los siguientes comités:

a) Comité de Administración Integral de Riesgos, conforme al Capítulo "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos";

b) Comité de Auditoría, conforme al Capítulo "Del comité de auditoría", Título "Del control interno", Libro I "Normas de control para las entidades de los sectores financieros público y privado" de la Codificación de Normas de la Superintendencia de Bancos; y,

c) Comité de Ética, conforme al artículo respecto de la conformación establecido en la Sección del "Ámbito y objetivo", Capítulo de los "Principios de un buen gobierno corporativo", Título "De los usuarios financieros", Libro I "Normas de control para las entidades de los sectores financieros público y privado" de la Codificación de Normas de la Superintendencia de Bancos.

ARTÍCULO 44.- Integración. Cada comité deberá incluir, como mínimo:

- El responsable del área correspondiente, quien lo presidirá;
- El auditor interno; y,
- Un delegado de los accionistas.

Los integrantes de los comités deberán acreditar criterios de idoneidad técnica, académica, ética y de experiencia, conforme a lo siguiente:

a) Comité de Auditoría:

- Incluir, al menos, un miembro independiente sin vínculos con la administración o accionistas;
- Poseer título universitario en finanzas, contabilidad, auditoría o carreras afines, registrado en la SENESCYT; y,
- Demostrar un mínimo de dos (2) años de experiencia en auditoría, control interno o cumplimiento.

b) Comité de Ética:

- Contar con un miembro independiente sin participación accionaria ni conflictos de interés;
- Poseer formación en derecho, administración o carreras afines, registrada en la SENESCYT;
- Acreditar experiencia mínima de tres (3) años en funciones de cumplimiento, control o ética; y,
- Presentar suscrito el compromiso de integridad, confidencialidad y aceptación del código de ética.

c) Comité de Administración Integral de Riesgos:

- Contar con profesionales con un perfil adecuado en materia de administración de riesgos financieros, operativos y tecnológicos, acreditando formación académica o experiencia equivalente que garantice el cumplimiento de sus funciones.
- La conformación y funcionamiento de este comité se encuentra determinado en el Capítulo de la "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos", del Título **"**De la gestión y administración de riesgos", Libro I "Normas de control para las entidades de los sectores financieros público y privado" de la Codificación de las Normas de la Superintendencia de Bancos.

ARTÍCULO 45.- Verificación de requisitos. La documentación que acredite lo señalado en el artículo anterior deberá presentarse ante la Superintendencia de Bancos de la siguiente manera:

a) La independencia y ausencia de conflictos de interés se comprobará mediante declaración juramentada otorgada ante notario público;
b) Los títulos académicos se verificarán mediante certificados de registro emitidos por la SENESCYT; en caso de títulos obtenidos en el extranjero estos deberán estar certificados y apostillados;
c) La experiencia profesional se comprobará con documentos originales o copias certificadas que respalden el ejercicio de las funciones señaladas; y,
d) El compromiso de integridad, confidencialidad y aceptación del código de ética será presentado en formato suscrito por el miembro designado.

La Superintendencia de Bancos podrá confirmar la veracidad de la documentación y declaraciones presentadas, mediante certificaciones a los organismos de control competentes.

ARTÍCULO 46.- Código de Ética. Las entidades deberán contar con un código de ética que incorpore valores de transparencia, legalidad, respeto a los grupos de interés, rendición de cuentas y responsabilidad social, conforme al artículo sobre los requisitos establecido en la Sección de “Estructura”, Capítulo sobre los “Principios de un buen gobierno corporativo”, Título “De los usuarios financieros”, Libro I “Normas de control para las entidades de los sectores financieros público y privado” de la Codificación de Normas de la Superintendencia de Bancos.

SUBSECCIÓN VI.- DE LOS ESTÁNDARES DE GOBIERNO CORPORATIVO DE LAS ENTIDADES ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 47.- Sistema de control interno. Las entidades administración de finanzas personales deberán implementar un sistema integral de control interno sustentado en los siguientes pilares:

a) Ambiente de control ético y supervisión activa;
b) Evaluación periódica de riesgos;
c) Actividades de control verificables;
d) Información y comunicación efectiva.; y,
e) Monitoreo continuo de efectividad y acciones correctivas.

ARTÍCULO 48.- Transparencia de la información. Se deberá garantizar la revelación clara, suficiente y oportuna de información a usuarios, inversionistas y reguladores, diferenciando los contenidos por grupo de interés y asegurando su validación interna.

ARTÍCULO 49.- Indicadores de gobierno corporativo. Las entidades deberán contar con indicadores de gobierno corporativo que serán establecidos en base a los lineamientos dictados por este organismo de control.

SUBSECCION VII.- DE LAS AUDITORÍAS PERIÓDICAS DE LAS ENTIDADES ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 50.- Función de auditoría interna. Las entidades administración de finanzas personales que cumplan con los criterios establecidos por la Superintendencia de Bancos deberán implementar una función de auditoría interna formalmente constituida, con

independencia operativa y con acceso directo al órgano de gobierno o al comité designado para supervisar dicha función.

ARTÍCULO 51.- Plan de auditoría interna. El auditor interno deberá elaborar anualmente un plan de trabajo basado en riesgos, que contemple la evaluación de procesos críticos, controles tecnológicos, cumplimiento normativo y protección de los intereses de los usuarios y terceros vinculados. Este plan deberá ser aprobado por el órgano de gobierno correspondiente.

ARTÍCULO 52.- Reportes y seguimiento. Los informes de auditoría interna deberán:

a) Documentar los hallazgos identificados en los procesos examinados;
b) Asignar responsables y establecer fechas de implementación de acciones correctivas; y,
c) Ser objeto de seguimiento periódico por parte del órgano de control interno o comité correspondiente.

SUBSECCIÓN VIII.- DE LA CONSERVACIÓN Y DISPONIBILIDAD DE DOCUMENTOS DE LAS ENTIDADES ADMINISTRACIÓN DE FINANZAS PERSONALES

ARTÍCULO 53.- Lineamientos. Establecer los lineamientos mínimos que deberán observar las empresas Fintech cuya actividad se centre en la administración de finanzas personales, respecto de la conservación, integridad, disponibilidad y acceso a la documentación generada en el marco de sus operaciones, contratos, servicios y obligaciones legales.

ARTÍCULO 54.- Tipología documental. Las entidades de administración de finanzas personales deberán conservar, al menos, los siguientes registros y documentos:

a) Datos de identificación del usuario: Nombre completo, número de cédula o RUC, información de contacto, perfil transaccional o de riesgo (en caso de aplicar);
b) Documentación contractual: Contratos firmados, consentimientos informados, aceptación de términos y condiciones (T&C), modificaciones contractuales y cualquier documento accesorio suscrito entre las partes;
c) Historial de operaciones: Registros de transacciones con detalle de fechas, montos, tipo de operación, canales utilizados, contrapartes involucradas y niveles de validación;
d) Comprobantes y transacciones: Confirmaciones de operaciones, facturas electrónicas, recibos generados, mensajes de validación o autenticación;
e) Bitácora de comunicaciones: Interacciones con los usuarios relativas a reclamos, requerimientos, respuestas emitidas y notificaciones relevantes; y,
f) Consentimientos y autorizaciones: Registros que evidencien la aceptación del tratamiento de datos personales, decisiones automatizadas, suscripción a comunicaciones comerciales o marketing.

ARTÍCULO 55.- Plazo mínimo de conservación. Las entidades de administración de finanzas personales deberán conservar los documentos señalados en la presente norma conforme a los siguientes criterios:

a) Documentos contables o financieros: Deberán conservarse por un período no menor a diez (10) años desde la fecha de su generación o desde la última operación o cierre de la relación comercial;
b) Documentos en formato digital: Deberán conservarse por un período mínimo de quince (15) años, garantizando su integridad y trazabilidad; y,

c) Documentación sujeta a procedimientos pendientes: En caso de que existan procedimientos judiciales, administrativos o regulatorios en curso, la documentación deberá mantenerse hasta su resolución definitiva.

ARTÍCULO 56.- Formato y accesibilidad. Los registros deberán conservarse en formato digital, estructurado y auditable, organizado mediante código único de usuario o identificador equivalente. La información deberá mantenerse disponible para fines de control y supervisión, debiendo ser entregada dentro del plazo máximo de cinco (5) días hábiles contados desde el requerimiento efectuado por la Superintendencia de Bancos, de conformidad con lo dispuesto en el artículo 63 del Código Orgánico Monetario y Financiero.

ARTÍCULO 57.- Responsabilidades del proveedor del servicio. Las entidades administración de finanzas personales deberán:

a) Designar responsables internos para la custodia, disponibilidad y seguridad de la documentación;
b) Implementar mecanismos que garanticen la integridad, inalterabilidad y confidencialidad de los registros digitales, conforme a la infraestructura tecnológica de la entidad; y,
c) Establecer políticas claras de respaldo, recuperación y continuidad operativa ante fallos o ataques cibernéticos.

SUBSECCIÓN IX.- DE LA ENTREGA DE INFORMACIÓN Y REPORTES AL ÓRGANO DE CONTROL

ARTÍCULO 58.- Obligación de reporte. Las entidades de administración de finanzas personales deberán remitir a la Superintendencia de Bancos, de manera periódica o cuando ésta lo requiera, información financiera, patrimonial, operativa, tecnológica y de gestión de riesgos, conforme a los formatos, frecuencia, canales y demás lineamientos técnicos e instructivos que emita el órgano de control para el efecto.

ARTÍCULO 59.- Reporte de patrimonio mínimo. La entidad deberá presentar información que permita evaluar la capacidad de absorción de pérdidas inesperadas, en función de su naturaleza, volumen y complejidad operativa. Este reporte deberá incluir como mínimo la base patrimonial constituida, composición del capital y cobertura patrimonial frente a riesgos asumidos.

ARTÍCULO 60.- Estados Financieros. Las entidades de administración de finanzas personales deberán remitir sus Estados Financieros suscritos por el Representante Legal y el Contador, junto con la información adicional relacionada con la gestión financiera que sea requerida por esta Superintendencia.

ARTÍCULO 61.- Información financiera y de desempeño. La presentación de la información financiera deberá alinearse al modelo de negocio y contemplar análisis sobre sostenibilidad, eficiencia, rentabilidad, patrimonio, liquidez, calidad de activos, calidad de pasivos y riesgos.

La Superintendencia de Bancos podrá establecer los formatos, indicadores, y periodicidad para la entrega de información.

ARTÍCULO 62.- Facultades de verificación. La Superintendencia de Bancos podrá verificar, validar y solicitar explicaciones adicionales sobre los reportes presentados por las entidades de administración de finanzas personales, sin perjuicio de requerir información complementaria, realizar auditorías o ejercer mecanismos de supervisión continua.

SUBSECCIÓN X.- DEL RIESGO DE LAVADO DE ACTIVOS

ARTÍCULO 63.- Riesgo de lavado de activos. Las entidades de Administración de finanzas personales deben implementar los mecanismos, procesos y procedimientos conforme lo estipula el Capítulo de la "Norma de control para la prevención y administración del riesgo de lavado de activos y la financiación de otros delitos (PARLAFD)", Título "De la gestión y administración de riesgos", Libro I "Normas de Control para las entidades de los sectores financieros público y privado", de la Codificación de las Normas de la Superintendencia de Bancos.

SECCIÓN IV.- DE LAS SOCIEDADES ESPECIALIZADAS DE DEPÓSITOS Y PAGOS ELECTRÓNICOS

ARTÍCULO 64.- Estructura de gobierno corporativo. Las sociedades especializadas de depósitos y pagos electrónicos que soliciten la licencia deberán aplicar los principios de buen gobierno corporativo, incorporando en sus estatutos y reglamentos, manuales de políticas internas y en la estructura organizacional, lo previsto en los "Principios de un Buen Gobierno Corporativo" contenidos en la Codificación de las Normas de la Superintendencia de Bancos", promoviendo la toma de decisiones, la supervisión y la rendición de cuentas en la organización.

Como parte de la estructura de gobierno corporativo se deberá incluir, al menos, un Comité de Administración Integral de Riesgos, un Comité de Auditoría, un Comité de Tecnología y Seguridad de la Información, así como, otros comités que consideren necesarios, según su modelo de negocio.

ARTÍCULO 65.- Unidad de Riesgos. Las sociedades especializadas de depósitos y pagos electrónicos establecerán una Unidad de Riesgo que deberá contar de manera permanente con los recursos humanos, materiales y tecnológicos necesarios y suficientes para ejecutar sus funciones. La unidad estará compuesta por personal capacitado que demuestre un sólido conocimiento y experiencia en el manejo y control de riesgos y que sea capaz de comprender las metodologías y procedimientos de la entidad para identificar, medir, controlar, mitigar y supervisar los riesgos presentes y futuros.

ARTÍCULO 66.- Funciones de los comités y la unidad de riesgos. Las funciones de los comités previamente señalados y de la Unidad de Riesgos corresponden a las establecidas por la Junta de Política y Regulación Financiera y Monetaria y por la Superintendencia de Bancos, en las normas de regulación y control emitidas.

ARTÍCULO 67.- Divulgación de información financiera y operativa. Las sociedades especializadas de depósitos y pagos electrónicos deben mantener la transparencia en la divulgación de información financiera y operativa. Esto incluye la publicación de informes financieros, así como la comunicación clara de las políticas, condiciones y términos de sus servicios.

La entidad debe proporcionar información adecuada para que los clientes comprendan los costos, riesgos y términos asociados al servicio contratado.

SUBSECCIÓN I.- DE LA GESTIÓN Y ADMINISTRACIÓN DE RIESGOS DE LAS SOCIEDADES ESPECIALIZADAS DE DEPÓSITOS Y PAGOS ELECTRÓNICOS

ARTÍCULO 68.- Evaluación y clasificación de riesgos. Las sociedades especializadas de depósitos y pagos electrónicos que soliciten la licencia deben llevar a cabo una evaluación

integral de los riesgos asociados a los servicios financieros tecnológicos, incluyendo los riesgos crediticios, de liquidez, de mercado, de tasa de interés, riesgo de tipo de cambio, riesgo operativo, de lavado de activos y del financiamiento de delitos, legal, reputacional y sistémico.

Deben clasificar los riesgos identificados y mantener un registro actualizado de estos, con la finalidad de implementar medidas de mitigación apropiadas.

Las sociedades especializadas de depósitos y pagos electrónicos para el servicio ofertado deben implementar lo pertinente para la administración de riesgos operativos en sus plataformas, conforme con lo establecido en el Capítulo de la "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos", del Título "De la gestión y administración de riesgos", Libro I "Normas de Control para las entidades de los sectores financieros público y privado" de la Codificación de las Normas de la Superintendencia de Bancos.".

ARTÍCULO 69.- Evaluación de riesgos de ciberseguridad y seguridad de la información. Las sociedades especializadas de depósitos y pagos electrónicos para el servicio ofertado deben implementar mecanismos de monitoreo a sus plataformas.

La gestión de riesgos de seguridad de la información incluidos los de ciberseguridad, se debe realizar mediante una metodología que le permita identificar, medir, controlar/mitigar y monitorear los riesgos asociados a los activos de información para preservar su confidencialidad, integridad y disponibilidad; esta metodología debe estar alineada a la metodología de gestión del riesgo operativo de la entidad.

ARTÍCULO 70.- Monitoreo y control de riesgos operativos. Las sociedades especializadas de depósitos y pagos electrónicos deben implementar mecanismos de monitoreo y control a sus plataformas, conforme con lo establecido en el Capítulo de la "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos", del Título "De la gestión y administración de riesgos", Libro I "Normas de Control para las entidades de los sectores financieros público y privado" de la Codificación de las Normas de la Superintendencia de Bancos.".

SUBSECCIÓN II.- CIBERSEGURIDAD Y SEGURIDAD DE LA INFORMACIÓN DE LAS SOCIEDADES ESPECIALIZADAS DE DEPÓSITOS Y PAGOS ELECTRÓNICOS

ARTÍCULO 71.- Las Sociedades Especializadas de Depósitos y Pagos Electrónicos y las Administradoras de Sistemas Auxiliares de Pago (ASAP), deberán cumplir con lo establecido en el Capítulo de la "Norma de control para la gestión integral y administración de riesgos de las entidades de servicios financieros tecnológicos", del Título "De la gestión y administración de riesgos", Libro I "Normas de Control para las entidades de los sectores financieros público y privado" de la Codificación de las Normas de la Superintendencia de Bancos.".

ARTÍCULO 72.- Políticas y procedimientos de seguridad de la información. Las Sociedades Especializadas de Depósitos y Pagos Electrónicos deben implementar políticas y procedimientos de seguridad de datos que garanticen la confidencialidad, integridad y disponibilidad de la información sensible.

Estas políticas y procedimientos deben abordar la gestión de contraseñas, el cifrado de datos, el control de acceso y otras prácticas de seguridad.

ARTÍCULO 73.- Protección contra amenazas cibernéticas. Las Sociedades Especializadas de Depósitos y Pagos Electrónicos deben establecer medidas de protección contra amenazas cibernéticas, incluyendo la detección y prevención de intrusiones, así como la mitigación de ataques maliciosos.

Deben contar con sistemas de monitoreo de seguridad que alerten sobre actividades inusuales o potenciales amenazas.

ARTÍCULO 74.- Plan de respuesta a incidentes de seguridad. Las Sociedades Especializadas de Depósitos y Pagos Electrónicos deben desarrollar un plan de respuesta a incidentes de seguridad que establezca procedimientos claros para la identificación, notificación, contención y recuperación de incidentes de seguridad.

Deben designar un equipo de respuesta a incidentes y capacitar a su personal en la ejecución de este plan.

ARTÍCULO 75.- Capacitación en ciberseguridad. Las Sociedades Especializadas de Depósitos y Pagos Electrónicos deben proporcionar capacitación continua en ciberseguridad a su personal para garantizar una comprensión adecuada de las amenazas y las mejores prácticas de seguridad.
Deben promover la conciencia de seguridad entre los empleados y usuarios.

ARTÍCULO 76.- Auditorías y pruebas de seguridad. Las Sociedades Especializadas de Depósitos y Pagos Electrónicos deben realizar auditorías periódicas de seguridad de la información y pruebas de vulnerabilidad para evaluar la efectividad de las medidas de seguridad implementadas, al menos, una vez al año.

Deben corregir las vulnerabilidades identificadas y mantener registros de las auditorías y pruebas realizadas.

DISPOSICIONES GENERALES

PRIMERA. - Las entidades sujetas a esta norma deberán dar cumplimiento a lo dispuesto en el Código Orgánico Monetario y Financiero; la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley FINTECH), las resoluciones emitidas por la Junta de Política y Regulación Financiera y Monetaria; y, las Normas de Control emitidas por la Superintendencia de Bancos.

SEGUNDA.- Los casos de duda en la aplicación de la presente norma serán resueltos por la Superintendencia de Bancos.