Resolución No. JPRF-F-2023-076

LA JUNTA DE POLÍTICA Y REGULACIÓN FINANCIERA

CONSIDERANDO:

Que, el Artículo 132, número 6 de la Constitución de la República del Ecuador, determina que se requerirá de ley para *"6. Otorgar a los organismos públicos de control y regulación la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales.";*

Que, el Artículo 226 de la Carta Magna manda que las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley;

Que, el Artículo 227 *ibidem* establece que la Administración Pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, coordinación, participación, y entre otros;

Que, el Artículo 308 de la Ley Fundamental prescribe que las actividades financieras son un servicio de orden público. Además, señala que el Estado fomentará el acceso a los servicios financieros y a la democratización del crédito;

Que, el Artículo 309 de la Norma Suprema indica que "*el Sistema Financiero Nacional se compone de los sectores público, privado, y del popular y solidario (…)"* Cada uno de estos sectores contará con normas y entidades de control específicas y diferenciadas, que se encargarán de preservar su seguridad, estabilidad, transparencia y solidez;

Que, el Artículo 13 del Código Orgánico Monetario y Financiero, Libro I, creó a la Junta de Política y Regulación Financiera, parte de la Función Ejecutiva y como persona jurídica de derecho público, responsable de la formulación de la política y regulación crediticia, financiera, de valores, seguros, y servicios de atención integral de salud prepagada;

Que, el Artículo 14, número 2 *ibidem*, preceptúa que le corresponde a la Junta de Política y Regulación Financiera *"2. Emitir las regulaciones que permitan mantener la integralidad, solidez, sostenibilidad y estabilidad de los sistemas financiero nacional, de valores, seguros y servicios de atención integral de salud prepagada en atención a lo previsto en el artículo 309 de la Constitución de la República del Ecuador (…)";*

Que, el Artículo 14.1 del referido Código Orgánico, ordena a la Junta de Política y Regulación Financiera a cumplir las siguientes facultades, entre las cuales se encuentran: *"1. Regular la creación, constitución, organización, actividades, operación y liquidación de las entidades financieras (…); 7. Emitir el marco regulatorio prudencial al que deben sujetarse las entidades financieras (…), marco que deberá ser coherente, no dar lugar a arbitraje regulatorio (…)"; 15. Establecer, en el marco de sus competencias, cualquier medida que coadyuve a: a. Prevenir y procurar erradicar prácticas fraudulentas y prohíbidas, incluidos el lavado de activos y el financiamiento de delitos como el terrorismo, considerando los estándares internacionales vigentes y aplicables; b. Proteger la privacidad de los individuos en relación con la difusión de su información personal, así como la información de seguridad nacional (…); d. Fomentar la inclusión financiera, promoviendo la participación de las entidades financieras (…); 27. Ejercer las demás funciones, deberes y facultades que le asigne este Código y la ley.";*

Que, el Artículo 5 de la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech), publicada el 22 de diciembre de 2022 en el Segundo Suplemento Nro. 215 del Registro Oficial, enumera las Actividades Fintech, entre las cuales se encuentran los Servicios Financieros Tecnológicos;

Que, el Artículo 6 *ibidem* establece los siguientes principios por los cuales se rige la mencionada Ley: autonomía de la voluntad, regulación basada en riesgos, transparencia, especialidad, lealtad, confiencialidad y protección de datos, seguridad, e incidentes/vulnerabilidades;

Que, el Artículo 8 de la referida Ley Orgánica prescribe que *"las compañías fintech estarán reguladas por la Junta de Política y Regulación Monetaria y Junta de Política y Regulación Financiera, según corresponda (…)";*

Que, el Artículo 11 de la Ley Fintech reformó el artículo 162 del Código Orgánico Monetario y Financiero, Libro I, Capítulo 2 "Integración del Sistema Financiero Nacional", del Título II "Sistema Financiero Nacional", incorporando en los números 4 y 5, como entidades del sector financiero privado a las de Servicios Financieros Tecnológicos y Sociedades Especializadas de Depósitos y Pagos Electrónicos;

Que, el Artículo 12 de la precitada Ley Orgánica reformó Código Orgánico Monetario y Financiero, Libro I, incorporando los artículos 439.1, 439.2, 439.3, 439.4, 439.5 y 439.6 en la Sección 12 "De los servicios financieros tecnológicos", Capítulo 5 "Sector Financiero Privado", del Título II "Sistema Financiero Nacional";

Que, el Artículo 439.1 del precitado cuerpo normativo establece que entre las entidades de servicios financieros tecnológicos se encuentra la concesión digital de créditos, la que es definida como *"empresas que ofrecen productos de crédito a través de plataformas electrónicas, sin que esto implique captación de recursos del público con finalidad de intermediación (…)";*

Que, el Artículo 439.4 *ibidem* manda a la Junta de Política y Regulación Financiera a regular sobre los expertos en economía y seguridad de la información que determinarán los criterios diferenciados según los riesgos financieros y tecnológicos de las entidades de servicios finanacieros tecnológicos;

Que, el Artículo 439.5 del Código Orgánico *ut supra* ordena a la Junta de Política y Regulación Financiera y a la Junta de Política y Regulación Monetaria, según corresponda, a regular la definición y las acciones que comprenden las operaciones a cargo de las entidades de servicios financieros tecnológicos;

Que, el Artículo 439.6 del Código Orgánico Monetario y Financiero, Libro I, establece que las actividades financieras basadas en tecnología que representen un alto riesgos serán determinadas por la Junta de Política y Regulación Financiera;

Que, la Disposición Transitoria Primera de la referida Ley otorga a la Junta de Política y Regulación Financiera y a la Junta de Política y Regulación Monetaria el periodo de tiempo ciento ochenta (180) días contados a partir de su publicación en el Registro Oficial, para desarrollar normativa secundaria que permita la aplicación de lo dispuesto en la misma;

Que, la Secretaria Técnica de la Junta de Política y Regulación Financiera, a través de Memorando Nro. JPRF-ST-2023-0069-M de 09 de septiembre de 2023, remite a la Presidente de la Junta los siguientes informes:

i. El Informe Técnico Nro. JPRF-CTSF-2023-014 de 09 de septiembre de 2023 concluye que, sobre la base de la revisión de norma comparada, de los talleres de trabajo efectuados con actores públicos y privados, consultores especializados en regulación de fintech de países de la región, organismos internacionales y de la revisión de fuentes bibliográficas relacionadas a la materia, se estima pertinente que la propuesta de norma de aplicación de las entidades de concesión digital de crédito incluya, en el marco de los aspectos dispuestos por la Ley Fintech a esta Junta, elementos referentes a las operaciones, capital mínimo para su funcionamiento, gestión de los riesgos que implicarían afectación a los clientes, como la gestión del riesgo operativo, de riesgo tecnológico y de seguridad de la información, además del riesgo de lavado de activos y financiamiento de delitos como el terrorismo, y

disposiciones relativas a la protección de los derechos de los usuarios financieros, reconociendo en dichas disposiciones la naturaleza y características propias de este tipo de entidades, conforme las definiciones contenidas en la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (LEY FINTECH).

ii. El Informe Jurídico Nro. JPRF-CJF-2023-040 de 09 de septiembre de 2023 concluye que:

- La Junta de Política y Regulación Financiera, de conformidad con los artículos 13, 14, 14.1, 439.2, 439.4, 439.5 y 439.6 del Código Orgánico Monetario y Financiero, Libro I, y el artículo 8 la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech), es competente para emitir la normativa secundaria para la aplicación de Ley Fintech.

- Los artículos 11 y 12 de la referida Ley reformaron al Código Orgánico Monetario y Financiero, Libro I, incorporando en el número 4 del artículo 162 del Capítulo 2 "Integración del Sistema Financiero Nacional", del Título II "Sistema Financiero Nacional", a las entidades de servicios financieros tecnológicos como parte del Sector Financiero Privado e incluyendo los artículos 439.1, 439.2, 439.3, 439.4, 439.5 y 439.6 en la Sección 12 "De los servicios financieros tecnológicos", Capítulo 5 "Sector Financiero Privado", Título II "Sistema Financiero Nacional", respectivamente.

- La Junta de Política y Regulación Financiera debe observar la Disposición Transitoria Primera de la Ley Fintech, misma que otorga a la misma un periodo de tiempo de ciento ochenta (180) días contados a partir de su publicación en el Registro Oficial, para desarrollar la normativa secundaria que permita la aplicación de la misma. Dicho periodo de tiempo debe computarse como término, de conformidad a lo previsto en los artículos 58 y 59 del Código Orgánico Administrativo.;

Que, la Junta de Política y Regulación Financiera, en sesión ordinaria realizada por medios tecnológicos, convocada el 09 de septiembre de 2023 y llevada a cabo a través de video conferencia el 11 de septiembre de 2023, conoció el Memorando Nro. JPRF-ST-2023-0069-M de 09 de septiembre de 2023, emitido por la Secretaria Técnica de la Junta; así como el Informe Técnico Nro. JPRF-CTSF-2023-014 y el Informe Jurídico Nro. JPRF-CJF-2023-040 de 09 de septiembre de 2023, emitidos por la Coordinación Técnica de Política y Regulación del Sistema Financiero y por la Coordinación Jurídica de Política y Normas Financieras, y el proyecto de resolución correspondiente;

Que, la Junta de Política y Regulación Financiera, en sesión ordinaria realizada por medios tecnológicos, convocada el 09 de septiembre de 2023 y llevada a cabo a través de video conferencia el 11 de septiembre de 2023, conoció y aprobó la siguiente Resolución; y,

En ejercicio de sus funciones,

RESUELVE:

ARTÍCULO ÚNICO.- Incorpórese el Capítulo LXII "Norma que Regula las Entidades de Servicios Financieros Tecnológicos", a continuación del Capítulo LXI "Mecanismo Extraordinario y Temporal de Alivio Financiero Aplicable al Sector Financiero de la Economía Popular y Solidaria", del Título II "Sistema Financiero Nacional", Libro I "Sistema Monetario y Financiero", de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros, con el siguiente texto:

"CAPITULO LXII.- NORMA QUE REGULA LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS

SECCIÓN I.- DEFINICIONES, CALIFICACIÓN Y OPERACIONES DE LAS ENTIDADES DE SERVICIOS FINANCIEROS TECNOLÓGICOS

SUBSECCIÓN I.- DEFINICIONES

Art.1.- Definiciones.- *Para efectos de la presente norma se consideran las siguientes definiciones:*

a. ***Análisis de datos (Data analytics):*** *Es el procesamiento, depuración, transformación y modelamiento de datos con el objetivo de descubrir patrones, tendencias, correlaciones e información estadísticamente significativa. El análisis de datos permite tomar decisiones informadas, identificar oportunidades de negocio, mejorar la eficiencia y obtener conocimientos de grandes volúmenes de datos.*

b. ***Asesores automatizados:*** *Son plataformas digitales que ofrecen asesoramiento financiero automatizado en inversiones y gestión de cartera e intermediación de contratos.*

c. ***Big data:*** *Se refiere a conjuntos grandes y complejos de datos que requieren métodos de procesamiento especializados para tareas como captura, almacenamiento, análisis y visualización. Se caracteriza por su alto volumen, velocidad, variedad, y el requerimiento de tecnología innovadora para recopilar y analizar los datos.*

d. ***Blockchain:*** *Tecnología de registro de la información que recoge y almacena data en bloques, así como detalles de transacciones, creando un registro único en una cadena preexistente, de criptografía avanzada.*

e. ***Ciberseguridad:*** *Es el conjunto de medidas de protección de la infraestructura tecnológica y de la información, a través del tratamiento de las amenazas que ponen en riesgo la información procesada por los diferentes componentes tecnológicos interconectados.*

f. ***Cliente:*** *Persona natural o jurídica, interna o externa a la organización, con la que una entidad del sistema financiero establece, de manera directa o indirecta, ocasional o permanente, una relación contractual de carácter financiero, económico o comercial.*

g. ***Computación en la nube (Cloud Computing):*** *Modelo de servicios de tecnología de la información que proporciona acceso a recursos informáticos, como almacenamiento, servidores y software, a través de internet.*

h. ***Concesión digital de créditos:*** *Es el proceso relacionado al otorgamiento de créditos que implica al menos la promoción, evaluación del perfil de riesgo del cliente, aprobación y desembolso, automatizados en gran medida por el uso de tecnologías digitales, a través de plataformas electrónicas. Se excluye todo lo referente a financiamiento colectivo.*

i. ***Confidencialidad:*** *Es el atributo de que solo el personal autorizado de la entidad accede a la información preestablecida.*

j. ***Contrato inteligente:*** *Algoritmo electrónico que se configura sobre una cadena de bloques (blockchain) para cumplir con un acuerdo previamente establecido entre dos o más partes. Una vez que las condiciones se cumplen, se ejecuta una tarea digital o transacción automática. Las transacciones realizadas son rastreables, transparentes e irreversibles.*

k. ***Datos abiertos:*** *Son aquellos datos no restringidos y fácilmente disponibles para el público en sitios web y conjuntos de datos públicos abiertos.*

l. ***Datos biométricos:*** *Datos personales únicos, relativos a las características físicas, fisiológicas o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.*

m. ***Datos confidenciales:*** *Datos protegidos contra la divulgación y que sean altamente sensibles o estén legal, reglamentaria o contractualmente restringidos de su divulgación.*

n. ***Datos crediticios:*** *Datos que integran el comportamiento económico de personas, para analizar su capacidad financiera.*

o. ***Entidades de concesión digital de créditos:*** *Son entidades de servicios financieros tecnológicos que ofertan productos de crédito exclusivamente a través de plataformas electrónicas, mediante procesos automatizados, en gran medida por el uso de tecnologías digitales, que implican al menos la promoción, evaluación del perfil de riesgo del cliente, aprobación y desembolso, sin que pueda captar recursos del público con finalidad de intermediación.*

p. ***Fintech (Tecnología Financiera):*** *Innovaciones financieras propiciadas por la tecnología que podrían dar lugar a nuevos modelos de negocio, aplicaciones, procesos o productos con un efecto sustancial sobre los mercados, las instituciones financieras y la prestación de servicios financieros.*

q. ***Infraestructura tecnológica****: Conjunto de elementos tecnológicos agrupados y organizados cuya función es soportar las operaciones de una entidad.*

r. ***Inteligencia de negocios (Business Intelligence, BI):*** *Proceso de recopilación, análisis y presentación de datos, que utiliza herramientas tecnológicas para la generación de información y optimización del análisis para la toma de decisiones.*

s. ***Protección de datos:*** *Son las medidas técnicas, organizativas, legales y de cualquier otra índole, que sean necesarias, para que el tratamiento de los datos sea utilizado exclusivamente para el propósito con el que fueron solicitados y/o autorizados, de conformidad con la ley vigente para el efecto.*

t. ***Proveedor:*** *Es toda persona natural o jurídica de carácter público o privado que desarrolle actividades de producción, fabricación, importación, construcción, distribución, alquiler o comercialización de bienes, así como prestación de servicios a consumidores.*

u. ***Servicios financieros tecnológicos:*** *Son actividades financieras centradas en la tecnología digital y electrónica prestadas por las entidades reconocidas en la ley. Entre las entidades que prestan servicios financieros tecnológicos se encuentran las siguientes:*

   a. *Las de Concesión digital de créditos;*
   b. *Neobancos;*
   c. *Las de Finanzas personales y asesoría financiera; y,*
   d. *Otras que determine la Junta de Política y Regulación Financiera.*

v. ***Sistema de gestión de información (SGI)****: Es un conjunto de procesos, procedimientos, políticas, tecnologías y herramientas diseñadas para gestionar eficientemente la información dentro de una entidad.*

w. ***Tecnología digital:*** *Se refiere al uso de tecnologías de información, tales como Internet, plataformas electrónicas, tecnologías móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones.*

x. ***Tecnología electrónica:*** *Hace referencia al uso de dispositivos y sistemas electrónicos para llevar a cabo procesos y actividades. En el contexto de las soluciones Fintech, esto implica el uso de dispositivos como teléfonos inteligentes (smartphones), ordenadores, tabletas (tablets), entre otros.*

y. ***Transferencia electrónica de información:*** *Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros.*

z. ***Verificación de identidades:*** *Proceso que permite autenticar, de manera objetiva y mediante cualquier sistema, que la identidad del solicitante coincide con la persona que obtendrá el producto o servicio.*

SUBSECCIÓN II.- DE LA ADMINISTRACIÓN DEL RIESGO DE LAVADO DE ACTIVOS Y FINANCIAMIENTO DE DELITOS, COMO EL TERRORISMO (ARLAFDT)

Art. 2.- Normas aplicables.- *Las entidades de servicios financieros tecnológicos deberán sujetarse a las regulaciones sobre la ARLAFDT emitidas por la Junta de Política y Regulación Financiera, y las establecidas por la Superintendencia de Bancos, en lo que corresponda al objeto social y operaciones de las mismas.*

Art. 3.- Del Oficial de Cumplimiento.- *Las entidades de servicios financieros tecnológicos deberán contar con un oficial de cumplimiento titular y un suplente. En caso de ausencia temporal o definitiva del oficial de cumplimiento titular, lo reemplazará el oficial de cumplimiento suplente. A falta del suplente, la función de cumplimiento será ejercida temporalmente por el representante legal.*

Los oficiales de cumplimiento titular y suplente ejercerán sus funciones para la prevención del riesgo de lavado de activos y del financiamiento de delitos, al menos a tiempo parcial, es decir, podrán realizar otras actividades siempre que no estén relacionadas con otras áreas que puedan generar conflicto de interés.

DISPOSICIÓN TRANSITORIA ÚNICA.- *Las entidades descritas en esta subsección implementarán las normas para la Administración del Riesgo de Lavado de Activos y Financiamiento de Delitos, como el Terrorismo en un plazo máximo de seis (6) meses, a partir de su calificación ante la Superintendencia de Bancos.*

SUBSECCIÓN III.- ENTIDADES DE CONCESIÓN DIGITAL DE CRÉDITOS

PARÁGRAFO I.- ÁMBITO

Art. 4.- Ámbito.- *Las disposiciones de esta subsección se aplicarán a las entidades de concesión digital de créditos, mismas que observarán lo dispuesto en el Código Orgánico Monetario y Financiero, Libro I, la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech), y cualquier otra normativa que le sea aplicable.*

PARÁGRAFO II.- DEL CAPITAL Y DE LA CALIFICACIÓN

Art. 5.- Cápital mínimo.- *El capital de las entidades de concesión digital de créditos estará dividido en acciones nominativas. El capital suscrito y pagado mínimo para la constitución de estas entidades será de USD 200.000.00 (doscientos mil dólares de los Estados Unidos de América).*

Art. 6.- Calificación.- *Los requisitos para la calificación de estas entidades serán establecidos por la Superintendencia de Bancos, entre los cuales deberán constar políticas, procesos, procedimientos y metodologías de gobierno corporativo, gestión y administración de riesgos, incluyendo aspectos de ciberseguridad y de seguridad de la información.*

El proceso de calificación que realice la Superintendencia de Bancos para la concesión digital de créditos permitirá a las entidades calificadas operar en todos los segmentos de crédito que contemple la normativa vigente, con el propósito de fomentar la innovación y el desarrollo, adopción y uso de nuevas tecnologías en productos y servicios financieros para mejorar la inclusión financiera, la productividad nacional y contribuir a la reducción de brechas de desigualdad socioeconómica en un contexto de plena competencia y brindar la protección a las y los usuarios y consumidores de los servicios.

PARÁGRAFO III.- POLÍTICAS, PROCEDIMIENTOS, CONTROLES, SUPERVISIÓN Y DEL EXPERTO EN ECONOMÍA Y SEGURIDAD DE LA INFORMACIÓN

Art.7.- Políticas, procedimientos y controles.- *Las entidades deberán diseñar, aprobar e implementar políticas, procedimientos y controles que compatibilicen su viabilidad económica-financiera con su capacidad de contar con respuestas estratégicas idóneas para los riesgos inherentes a sus líneas de negocios, conforme a su tamaño, volumen y naturaleza de sus negocios y riesgos.*

Art.8.- Supervisión y Control.- *La supervisión y control de estas entidades le corresponderá a la Superintendencia de Bancos con un enfoque de gestión de riesgos.*

Art.9.- Experto de Economía y de Seguridad.- *Para efectos del cumplimiento de lo previsto en el artículo 439.4 del Código Orgánico Monetario y Financiero, Libro I, la Superintendencia de Bancos será la encargada de la determinación de los criterios diferenciados que serán considerados en el establecimiento de los requisitos de calificación de estas entidades.*

PARÁGRAFO IV.- DE LAS OPERACIONES

Art.10.- Términos y condiciones.- *Las entidades deberán proporcionar al cliente información completa, clara, veraz y transparente sobre los términos y condiciones de los productos y servicios financieros que ofrezcan, incluyendo al menos lo siguiente:*

a. El costo total y demás condiciones del crédito;
b. Los medios y herramientas que se encuentran a disposición de los clientes para realizar los pagos correspondientes; y,
c. Los canales de comunicación para la tramitación de las reclamaciones.

Art.11.- Simuladores de créditos.- *Las entidades contarán con simuladores de crédito en línea u otros instrumentos que, mediante el ingreso de información relacionada al menos con el monto del préstamo, plazo, tipo de crédito y frecuencia de pago, permita calcular el monto total del crédito y los pagos periódicos requeridos.*

Art.12.- Productos.- *Las entidades de concesión digital de créditos solamente podrán otorgar los siguientes productos: concesión de crédito directo y emisión de tarjetas de crédito.*

Art.13.- Infraestructura tecnológica.- *Las entidades podrán utilizar equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones para otorgar sus servicios y podrán efectuar cualquier forma de verificación reconocida en las normas aplicables a la materia, para dar acceso a sus clientes a su infraestructura tecnológica, contratar sus productos y servicios o realizar operaciones. El funcionamiento y uso de tales equipos, medios y formas de verificación se sujetará a las disposiciones que para tal efecto emita el organismo de control, con un enfoque de neutralidad tecnológica.*

Art.14.- Aceptación expresa del producto.- *Las entidades deberán contar con el respaldo de la aceptación expresa del producto por parte del cliente a través de medios digitales válidos.*

Art.15.- Calificación del cliente.- *Las entidades deberán evaluar la capacidad y carácter de pago del cliente para lo cual tomarán en cuenta la situación económica y financiera, el grado de endeudamiento, la capacidad de generar resultados o flujo de caja, la puntualidad y morosidad en los pagos, el sector de la actividad económica, entre otros. Para su cumplimiento, las entidades de concesión digital de créditos deberán contar con scores de crédito.*

Art.16.- Contrato y otros documentos legales.- *Las entidades deberán poner a diposición del cliente los contratos y demás documentos legales vigentes de los que se deriven sus obligaciones y derechos, ya sea a través de medios físicos o electrónicos.*

Art.17.- Desembolsos del crédito directo.- *Los desembolsos de los créditos otorgados a sus clientes, previa la verificación de su identidad, se efectuarán mediante transferencias desde cuentas abiertas en el sistema financiero nacional a nombre de la entidad, hacia cuentas abiertas en entidades del sistema financiero nacional que se encuentren a nombre del cliente; o, monto fijo no revolvente otorgado a través de tarjetas.*

Art.18.- Protección de los usuarios financieros.- *Con finalidad de velar por la protección de los derechos de los usuarios financieros, las entidades de concesión digital de crédito deberán realizar como mínimo lo siguiente:*

a. Informar de manera completa, clara, veraz y transparente al cliente sobre los beneficios, riesgos y condiciones fundamentales de los productos o servicios ofertados;
b. Garantizar que cualquier información facilitada al cliente, ya sea por escrito, vía electrónica o de manera verbal, sea justa, clara y transparente;
c. Garantizar que la información sobre los productos y servicios ofertados se encuentre actualizada y facilmente accesible para el cliente; y,
d. Divulgar su identidad en los documentos y otros instrumentos emitidos en el ejercicio de su actividad, y al momento de contratar con el usuario financiero.

PARÁGRAFO V.- DE LA CALIFICACIÓN DE CARTERA, PROVISIONES, DE LA NOVACIÓN, REFINANCIAMIENTO, REESTRUCTURACIÓN Y DEL CASTIGO DE LAS OBLIGACIONES

Art.19.- Calificación de cartera.- *Las entidades de concesión digital de créditos calificarán la cartera conforme lo dispuesto en la Sección II "Elementos de la calificación de activos de riesgo y su clasificación", del Capítulo XVIII "Calificación de activos de riesgo y constitución de provisiones por parte de las entidades de los sectores financiero público y privado bajo el control de la Superintendencia de Bancos", del Título II "Sistema Financiero Nacional", Libro I "Sistema Monetario y Financiero" de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros.*

Art.20.- Constitución de provisiones.- *Las entidades de concesión digital de créditos, al no estar facultadas para captar recursos del público con la finalidad de intermediación, a fin de cubrir la desvalorización de su cartera de créditos, pérdidas por ciclo económico y otras relacionadas a su giro del negocio (genéricas), de conformidad con los artículos 205 y 206 del Código Orgánico Monetario y Financiero, Libro I, deberán constituir provisiones en los diferentes segmentos de crédito, en los porcentajes mínimos y máximos que constan en la siguiente tabla:*

	PORCENTAJE DE PROVISIÓN	
CATEGORÍAS	**MIN**	**MAX**
A-1	1,00%	1,99%
A-2	1,00%	2,99%
A-3	1,00%	5,99%
B-1	1,00%	9,99%
B-2	1,00%	19,99%
C-1	1,00%	39,99%
C-2	1,00%	59,99%
D	1,00%	99,99%
E	1,00%	100%

De conformidad con la Ley Reformatoria para la Equidad Tributaria del Ecuador, las provisiones requeridas para cubrir riesgos de incobrabilidad o pérdida del valor de los activos de riesgo de las entidades de concesión digital de créditos, que se hagan con cargo al estado de pérdidas y ganancias de dichas entidades financieras, serán deducibles de la base imponible correspondiente al ejercicio en el cual se constituyan las mencionadas provisiones hasta por el monto máximo establecido en el inciso anterior dentro de los rangos de las subcategorías de riesgo de cada uno de los segmentos de crédito.

El monto de las provisiones por activos de riesgo deberá cargarse a la cuenta de resultados deudora al 31 de diciembre de cada año.

Art.21.- Novación, refinaciamiento y reestructuración.- *Los procesos de novación, refinanciamiento y reestructuración de las operaciones de créditos de las entidades de concesión digital de créditos se sujetarán a lo dispuesto en la Sección V "Créditos novados, refinanciados y reestructurados", del Capítulo XVIII "Calificación de activos de riesgo y constitución de provisiones por parte de las entidades de los sectores financiero público y privado bajo el control de la Superintendencia de Bancos", del Título II "Sistema Financiero Nacional", Libro I "Sistema Monetario y Financiero" de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros.*

Art.22.- Castigo de las obligaciones.- *Con referencia al castigo de las obligaciones, las entidades de concesión digital de créditos se sujetarán a la Sección I "Del castigo", del Capítulo XX "Castigo de préstamos, descuentos y otras obligaciones por parte de las entidades controladas por la Superintendencia de Bancos", del Título II "Sistema Financiero Nacional", del Libro I "Sistema Monetario y Financiero" de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros.*

DISPOSICIONES GENERALES

PRIMERA.- *Las entidades de concesión digital de créditos aplicarán la Sección I "Normas que Regulan las Tasas de Interés", del Capítulo XI "Sistema de Tasas de Interés y Tarifas del Banco Central del Ecuador para las Entidades del Sistema Financiero Nacional", del Título I "Sistema Monetario"; el Capítulo III "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"; el Capítulo IX "Normas que Regulan la Segmentación de la Cartera de Crédito de las Entidades del Sistema Financiero Nacional"; el Capítulo XXV "Servicios Financieros del Sector Financiero Público y Privado", la Sección I "Servicios No Financieros", del Capítulo LIII "Usuarios Financieros"; y, el Capítulo LIV "Norma sobre los Burós de Información Crediticia y las Obligaciones de Pago que deben constar en el Servicio de Referencias Crediticias, del Título II "Sistema Financiero Nacional", del Libro I "Sistema Monetario y Financiero" de la Codificación de Resoluciones Monetarias, Financieras, de Valores y Seguros.*

SEGUNDA.- *Las entidades de concesión digital de créditos aplicarán lo establecido en la norma que determina la relación entre el patrimonio técnico total y los activos y contingentes ponderados por riesgo para las entidades del sistema financiero público y privado, una vez que la Superintendencia de Bancos emita la norma que disponga el régimen contable respectivo.*

TERCERA.- *La Superintendencia de Bancos emitirá las normas de control necesarias para la aplicación de la presente subsección.*

CUARTA.- *La concesión digital de créditos podrá ser efectuada únicamente por las entidades calificadas por la Superintendencia de Bancos.*

DISPOSICIONES TRANSITORIAS

PRIMERA.- *La Superintendencia de Bancos emitirá la norma para la calificación de las entidades de concesión digital de créditos en un plazo de dos (2) meses, a partir de la publicación de la presente Resolución en el Registro Oficial.*

SEGUNDA.- *La Superintendencia de Bancos emitirá el catálogo de cuentas de las entidades de concesión digital de créditos en un plazo de tres (3) meses, a partir de la publicación de la presente Resolución en el Registro Oficial.*

TERCERA.- *Las entidades de concesión digital de créditos, en un plazo de seis (6) meses, a partir de su calificación ante la Superintendencia de Bancos, implementarán las normas de esta subsección.*

SUBSECCIÓN IV.- DE LA GESTIÓN DE RIESGOS DE LAS ENTIDADES DE CONCESIÓN DIGITAL DE CRÉDITOS

Art.23.- Ámbito.- *Las disposiciones de la presente subsección son aplicables a las entidades de concesión digital de créditos, cuyo control le compete a la Superintendencia de Bancos.*

Art.24.- Comité de Gestión de Riesgos.- *Las entidades establecerán un comité responsable de la gestión de riesgos. Este comité estará compuesto al menos por un representante de la Junta General de Accionistas o del Directorio en caso de haberlo, quien lo presidirá; el representante legal; y, el responsable de la Unidad de Riesgos. El presidente del comité tendrá voto dirimente.*

El Comité de Gestión de Riesgos se reunirá ordinariamente al menos una vez al mes, y de manera extraordinaria cuando así lo requiera. El quorum de las reuniones será con la totalidad de sus miembros y sus decisiones serán tomadas por mayoría de votos.

Art.25.- Funciones del Comité de Gestión de Riesgos.- *El Comité de Gestión de Riesgos tiene la responsabilidad de llevar a cabo al menos las siguientes funciones:*

a. *Aprobar y mantener actualizado los manuales de procedimientos, metodologías de gestión de riesgos, plan de continuidad del negocio, cuando exista delegación de la Junta General de Accionistas o del Directorio;*

b. *Administrar los procesos, procedimientos y metodologías que promuevan una eficaz gestión de riesgos;*

c. *Evaluar, proponer y tomar acciones correctivas relacionadas a los sistemas de gestión de riesgos;*

d. *Mantener informada a la Junta General de Accionistas o al Directorio, sobre la evolución de los niveles de exposición para cada riesgo identificado y la probabilidad de afectación ante cambios repentinos en el entorno económico; y,*

e. *Cumplir con otras funciones que la Junta General de Accionistas o el Directorio determine o que sean establecidas por la Superintendencia de Bancos.*

Es obligación del Comité de Gestión de Riesgos mantener registros documentales que respalden el cumplimiento de las disposiciones establecidas en este artículo. Asimismo, es imprescindible que la documentación presentada a la Junta General de Accionistas o al Directorio cuente con la aprobación correspondiente.

Art.26.- 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.*

El número de funcionarios de la Unidad de Riesgos deberá guardar proporción con la naturaleza, complejidad y volumen de los negocios, operaciones y actividades desarrolladas por la entidad.

Art.27.- Funciones de la Unidad de Riesgos*: Las principales funciones de la Unidad de Riesgos son:*

a. *Analizar de forma sistemática las exposiciones por tipo de riesgos respecto de los principales clientes, proveedores, sectores económicos, área geográfica, tecnologías de la información, entre otros;*

b. *Coordinar la preparación e implementación de los planes de contingencia, continuidad del negocio, el Sistema de Gestión de Seguridad de Información SGSI y el Plan Estratégico de Seguridad de la Información PESI;*

c. *Implementar de manera sistemática mecanismos de divulgación que permitan una mayor cultura de riesgos al interior de toda la organización;*

d. *Analizar la incursión de la entidad en operaciones, actividades y servicios acorde con el objeto y estrategias del negocio;*

e. *Analizar el entorno y sus efectos en la posición de riesgos de la entidad y realizar pruebas de estrés y back testing a los modelos de riesgos, incorporando cualquier señal de deterioro provista por los estudios realizados internamente u otras fuentes; y,*

f. *Definir los límites de concentración por sujeto de crédito, en relación al patrimonio de la entidad.*

PARÁGRAFO I.- DE LA GESTIÓN DEL RIESGO OPERATIVO

Art.28.- Definiciones.- *Para efectos de la aplicación de las disposiciones del presente parágrafo, se considerarán las siguientes definiciones:*

a. ***Administración de la continuidad del negocio:*** *Es un proceso permanente que garantiza la continuidad de las operaciones de las entidades, a través del mantenimiento efectivo de un sistema de gestión de continuidad del negocio.*

b. ***Administración de la información:*** *Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes.*

c. ***Evento de riesgo operativo:*** *Es el hecho que deriva en pérdidas para las entidades, originado por fallas o insuficiencias en los factores de riesgo operativo.*

d. ***Factor de riesgo operativo:*** *Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son: procesos, personas, tecnología de la información y eventos externos.*

e. ***Incidente de seguridad de la información:*** *Es el evento asociado a posibles fallas en la seguridad de la información, o una situación con probabilidad de comprometer las operaciones del negocio y amenazar la seguridad de la información.*

f. ***Indicadores claves de riesgo:*** *Es una métrica para determinar qué tan posible es que la probabilidad de un evento, combinada con sus consecuencias, supere el apetito de riesgo operativo, cuantifican el perfil de riesgo operativo de la entidad; y, ayudan a tomar acciones oportunas y corregir las desviaciones de metas, antes de que sucedan.*

g. ***Información crítica:*** *Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones.*

h. ***Línea de negocio:*** *Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo, definido en la planificación estratégica de la entidad.*

i. ***Pista de auditoría:*** *Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos, bases de datos, sistemas operativos y demás elementos tecnológicos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría.*

j. ***Plan de continuidad del negocio:*** *Es el conjunto de procedimientos que orientan a las entidades a mantener su operatividad en el caso de que ocurran interrupciones que afecten sus servicios.*

k. ***Procedimiento:*** *Es la forma específica para llevar a cabo una actividad o un proceso.*

l. ***Proceso:*** *Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente interno o externo utilizando recursos de la entidad.*

m. ***Proceso crítico:*** *Es el conjunto de actividades indispensables para la continuidad del negocio y las operaciones de la entidad controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto negativo.*

n. ***Propietario de la información:*** *Es la persona encargada de cuidar la integridad, confidencialidad y disponibilidad de la información; debe tener autoridad para especificar y exigir las medidas de seguridad necesarias para cumplir con sus responsabilidades.*

o. ***Resiliencia operativa:*** *Capacidad de una entidad para seguir entregando los servicios críticos durante eventos disruptivos; esta capacidad le permite a la entidad identificar y protegerse de amenazas y potenciales fallas, respondiendo y adaptándose a ellas; así como, recuperarse y aprender de los eventos disruptivos con la finalidad de minimizar su impacto hacia el futuro en la entrega de los servicios críticos.*

p. ***Seguridad de la información:*** *Es el conjunto de medidas y técnicas que permite la preservación de la confidencialidad, integridad y disponibilidad de la información; incluyen aspectos relacionados con la seguridad informática y la ciberseguridad.*

q. ***Tarea:*** *Es el conjunto de pasos que conduce a un resultado final visible y mesurable.*

r. ***Tecnología de la información:*** *Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes y comunicaciones, entre otros.*

Art.29.- Gestión del riesgo operativo.- *El riesgo operativo se refiere a la probabilidad de pérdidas derivadas de fallos en procesos, personas, tecnología de la información o eventos externos; incluye además el riesgo legal, que se relaciona con pérdidas por no cumplir adecuadamente con disposiciones legales, normativas o decisiones administrativas. Esta inobservancia puede deberse a errores, negligencia o mala interpretación; también se puede originar por una redacción deficiente en contratos o la incorrecta especificación de derechos entre partes; sin embargo, no abarca riesgos sistémicos, estratégicos ni de reputación.*

Art.30.- Políticas y metodologías.- *Las entidades deben establecer políticas y metodologías claras para la gestión del riesgo operativo, las cuales deberán observar los procesos de identificación, medición, control, y monitoreo del riesgo operativo en todas sus operaciones y negocios; para ello, es esencial realizar evaluaciones continuas del riesgo operativo, incluidos los proyectos actuales y nuevos productos.*

Art.31.- Eventos de riesgo operativo.- *Las entidades tienen la obligación de identificar riesgos operativos basándose en diferentes categorías como línea de negocio, tipo de evento y factor de riesgo. Para ello, deben aplicar una metodología adecuadamente documentada y aprobada, utilizando herramientas como autoevaluaciones, mapas de riesgos, indicadores y tablas de control, entre otras.*

Para los eventos de riesgo operativo se considerarán al menos:

a. Fraude interno;
b. Fraude externo;
c. Prácticas laborales y seguridad del ambiente de trabajo;
d. Prácticas relacionadas con los clientes, los productos y el negocio;
e. Daños a los activos físicos;
f. Interrupción del negocio por fallas en la tecnología de la información; y,
g. Deficiencias en el diseño y/o la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Art.32.- Cuantificación del riesgo operativo.- *La cuantificación de riesgos operativos se determinará sobre la base de su probabilidad de ocurrencia e impacto de los posibles eventos de riesgo operativo. Esta información proporciona a la Junta General de Accionistas o al Directorio y al representante legal una perspectiva precisa de la exposición de la entidad al riesgo operativo, facilitando la toma de decisiones informadas para su gestión.*

Art.33.- Revisiones periódicas de incidencias de riesgo operativo.- *Las entidades deben establecer y revisar periódicamente planes de mitigación, que podrían involucrar ajustes en estrategias, políticas, procesos y procedimientos. Esto también podría requerir la implementación o revisión de límites de riesgo, controles, planes de continuidad de negocio, términos de seguros y servicios de terceros, entre otros. Estos controles deben integrarse plenamente en las operaciones diarias de la entidad, garantizando respuestas rápidas a posibles incidencias de riesgo operativo. Además, las entidades deben establecer mecanismos adicionales para enfrentar las fuentes de riesgos no específicamente mencionados en esta norma, pero que estén relacionados con factores del riesgo operativo.*

Art.34.- Contenido de los reportes de riesgo operativo.- *Las entidades tienen la obligación de monitorear continuamente los riesgos operativos asociados a sus procesos y nivel de exposición. Para asegurar una gestión eficaz, deben contar con un sistema organizado de reportes que proporcione información relevante y oportuna para la toma de decisiones.*

Art.35.- Factor procesos.- *Las entidades deben implementar una gestión basada en procesos para asegurar la optimización y estandarización de las actividades, teniendo como referencia estándares internacionales. Con relación a los procesos se deberá tomar en cuenta, al menos:*

a. *Procesos: Se clasifican en Gobernantes o Estratégicos, Operativos y de Apoyo;*
b. *Metodología de procesos: Definir formalmente una metodología para el diseño, control, actualización, seguimiento y medición de los procesos;*
c. *Registro de procesos: Mantener un inventario actualizado de los procesos existentes; y,*
d. *Indicadores: Definir una metodología para medir la efectividad de procesos.*

Las entidades deben procurar que una sola persona no realice funciones que puedan generar riesgos, para lo cual deberá tomar en cuenta el tamaño, naturaleza, complejidad y volumen del negocio.

Art.36.- Factor personas.- *Las entidades deben asegurarse de gestionar eficazmente los riesgos asociados con su capital humano, siguiendo políticas de personal claras, que cubran las áreas de incorporación, permanencia y desvinculación; manteniendo actualizados los acuerdos de confidencialidad vinculados a los roles y responsabilidades de los empleados; y estableciendo responsabilidades relacionadas con la seguridad de la información que se mantienen después de cualquier cambio en las funciones o término de la relación laboral.*

El enfoque debe ser siempre la optimización de recursos humanos alineados con los objetivos de la entidad y la gestión efectiva de los riesgos asociados.

Art.37.- Factor tecnología de la información.- *Para garantizar una gestión adecuada del riesgo tecnológico, las entidades deberán contar con una Unidad de Tecnología de la Información que se adecúe al tamaño y complejidad de las operaciones de la entidad. La Unidad contará con un plan estratégico tecnológico alineado con el plan institucional, aprobado por la Junta General de Accionistas o Directorio; y, un plan operativo anual que detalle las actividades tecnológicas a realizar.*

Para asegurar que las operaciones tecnológicas cumplan con los requisitos de las entidades, establecerán procedimientos sobre la operación de centros de datos, gestión de incidentes tecnológicos y respaldos de información periódicos.

Las entidades adoptarán una metodología que administre el ciclo de vida del desarrollo y mantenimiento de aplicaciones, considerando las mejores prácticas internacionales. Esta metodología debe tener en cuenta desde los requerimientos funcionales hasta el seguimiento postproducción y controles en caso de migración de información.

Las entidades contarán con una infraestructura tecnológica robusta y documentada. Esta debe considerar desde la redundancia en procesos críticos, administración de bases de datos, análisis de capacidad, hasta ambientes aislados para desarrollo y producción.

Las entidades deberán tener un proceso de control de cambios eficiente que garantice la autorización, documentación, prueba y aprobación de cambios en aplicaciones e infraestructura. Este proceso debe ser acorde con las mejores prácticas nacionales e internacionales, garantizando que cualquier cambio no afecte la integridad del sistema.

Las entidades que utilicen big data y computación basada en la nube, deberán contar con una arquitectura tecnológica escalable y adaptable capaz de gestionar volúmenes significativos de datos y responder a las fluctuantes necesidades operativas de la entidad. Se exige que las entidades implementen las herramientas y tecnologías apropiadas para el procesamiento y análisis efectivo de big data. Estas incluyen, pero no se limitan a:

a. *Bases de datos distribuidas de alta disponibilidad;*
b. *Sistemas de almacenamiento de alto rendimiento; y,*
c. *Procedimientos de mantenimiento y actualización periódica de su infraestructura tecnológica asociada al manejo de big data y computación en la nube, con el fin de garantizar la eficacia continua y la adhesión a las mejores prácticas en esta materia.*

Art.38.- Eventos externos.- *La gestión del riesgo operativo exige que las entidades contemplen pérdidas potenciales por eventos fuera de su dominio, como fallas en servicios públicos, desastres naturales, ataques cibernéticos y actos delictivos que interrumpan sus operaciones normales.*

Se deberá integrar la gestión de estos riesgos en la continuidad del negocio, manteniendo protocolos actualizados para asegurar la operatividad constante y reducir pérdidas ante interrupciones.

Art.39.- Gestión de incidentes.- *Las entidades deberán formular y poner en práctica planes de respuesta y recuperación frente a incidentes alineados a esta norma, para asegurar la continuidad, en particular de sus servicios críticos, respetando su tolerancia al riesgo y acorde a las mejores prácticas internacionales, fomentando así su resiliencia operativa. Para ello, estas entidades deben:*

a. Designar un responsable de incidentes;
b. Emitir procedimientos para gestionar los riesgos operativos, contemplando al menos: ciclo de vida, registro, priorización, análisis, solución y seguimiento, de los incidentes;
c. Realizar pruebas controladas de manejo de incidentes; y,
d. Reportar al órgano de control cualquier incidente que comprometa sus procesos críticos.

Art.40.- Administración de la continuidad del negocio.- *Las entidades deben instaurar y optimizar un sistema de gestión de continuidad del negocio alineado a estándares internacionales. Este sistema debe considerar eventos internos y externos, y las estrategias para garantizar la operatividad, fortaleciendo la resiliencia de la entidad.*

Art.41.- Plan de continuidad del negocio.- *El marco de referencia para gestionar la continuidad del negocio debe incorporar los siguientes elementos, garantizando una operación efectiva y resiliente:*

a. ***Alcance:*** *Define la cobertura del sistema de gestión, priorizando procesos críticos;*

b. ***Documentación:*** *Incorpora políticas, estrategias, objetivos, procesos, metodologías, entre otros, para la continuidad del negocio. Estos deben ser conocidos y avalados por el Comité de Gestión de Riesgos y la Junta General de Accionistas o el Directorio, y comunicados al personal para asegurar su cumplimiento;*

c. ***Funciones y responsabilidades:*** *Especifica quiénes son los encargados de las actividades de continuidad y cómo contribuyen a la resiliencia de la entidad;*

d. ***Análisis de impacto:*** *Estudia las consecuencias de interrupciones en los procesos clave, identificando dependencias y recursos de apoyo. Se deben actualizar con cualquier cambio organizacional;*

e. ***Escenarios de riesgo:*** *Identifica las principales amenazas, especialmente tecnológicas, y evalúa su impacto y probabilidad;*

f. ***Estrategias de continuidad:*** *Establece acciones para garantizar la operatividad de cada proceso crítico considerando diversos aspectos, como la seguridad del personal o la infraestructura alternativa;*

g. ***Plan de continuidad del negocio:*** *Proporciona medidas para asegurar la disponibilidad de servicios esenciales y reducir el impacto de eventos disruptivos.*

El plan de continuidad deberá incluir el análisis del impacto que tendría una interrupción de los procesos que soportan los productos y servicios de la entidad. Además, aplicará los parámetros para la identificación de los procesos críticos, su punto de recuperación objetivo (RPO) y tiempos de recuperación objetivo (RTO) definidos por el negocio. Una vez identificados los procesos críticos, deben determinar las dependencias internas y externas; y, recursos de soporte para estos procesos, incluyendo tecnología, personal, proveedores y otras partes interesadas;

h. ***Pruebas del plan:*** *Establece procedimientos para validar y actualizar el plan de continuidad regularmente y ante cualquier cambio relevante; incluye la supervisión de planes de compañías externas que soportan servicios esenciales;*

i. ***Monitoreo y evaluación:*** *Define cómo se supervisará el desempeño y eficacia del sistema de gestión;*

j. ***Difusión y capacitación:*** *Establece cómo se comunicará, formará y concienciará sobre el plan de continuidad a los usuarios internos y proveedores;*

k. ***Integración con la gestión de riesgos:*** *Asegura que la administración de la continuidad esté alineada con la gestión de riesgos; y,*

l. ***Lecciones aprendidas:*** *Se debe mantener una base de datos con aprendizajes derivados de pruebas y eventos reales para mejorar futuras acciones.*

Art 42.- Riesgo legal.- *Las entidades deben gestionar proactivamente el riesgo legal, identificando, midiendo, controlando, mitigando y monitoreando potenciales eventos que conlleven a pérdidas. Las entidades deben desarrollar planes acordes al ordenamiento jurídico ecuatoriano.*

Art 43.- Servicios provistos por terceros.- *Las entidades deben gestionar y monitorear de manera integral los servicios proporcionados por terceros; esta gestión incluye: selección de proveedores; contratación; gestión de riesgos; computación en la nube; normativa financiera; e, integridad de la información.*

Las entidades están obligadas a seguir estas directrices para asegurar la calidad, seguridad y conformidad de los servicios tercerizados.

PARÁGRAFO II.- DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Art 44.- Seguridad de la información.- *La seguridad de la información engloba las estrategias y medidas diseñadas para resguardar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información ante posibles amenazas y riesgos. Las entidades deberán contar con un Manual de Seguridad de la Información, que contemple las funciones y responsabilidades para gestionar estos riesgos.*

Para gestionar la seguridad de la información, la entidad deberá considerar políticas, objetivos, procesos, procedimientos y metodologías, sobre la base de buenas prácticas internacionales, y cumplir con las disposiciones legales y reglamentarias vigentes.

Art 45.- Responsable.- *La entidad designará un Responsable de la Gestión de la Seguridad de la Información, mismo que tendrá al menos las siguientes funciones:*

a. *Definir y revisar periódicamente las políticas, procesos, procedimientos y metodologías de seguridad de la información;*

b. *Mantener un inventario de activos de información;*

c. *Designar a los propietarios de activos de información y definir sus responsabilidades;*

d. *Implementar una metodología de gestión de riesgos de seguridad de la información;*

e. *Desarrollar un Plan de Seguridad de la Información;*

f. *Verificar el cumplimiento de políticas, procesos, procedimientos y controles de seguridad de la información;*

g. *Monitorear semestralmente el cumplimiento y efectividad de los controles de seguridad de la información;*

h. *Evaluar anualmente el desempeño del sistema de gestión de seguridad de la información; e,*

i. *Implementar procedimientos específicos relacionados con el manejo de activos de información, control de accesos, monitoreo de accesos, pistas de auditoría, uso de llaves criptográficas, cifrado de información, instalación de software, auditorías de seguridad de infraestructura tecnológica, segmentación de la red, definición de requerimientos de seguridad de la información para nuevos sistemas, escaneo automatizado de vulnerabilidades en código fuente, afectación directa a las bases de datos, y difusión, comunicación, entrenamiento y concienciación del sistema de gestión de seguridad de la información.*

DISPOSICIÓN TRANSITORIA ÚNICA.- *Las entidades de concesión digital de créditos, en un plazo de un (1) año, a partir de su calificación ante la Superintendencia de Bancos, implementarán las normas de gestión de riesgos."*

DISPOSICIÓN FINAL.- La presente Resolución entrará en vigor a partir de su publicación en el Registro Oficial. Publíquese la presente Resolución en la página web de la Junta de Política y Regulación Financiera, en el término máximo de dos días desde su expedición.

COMUNÍQUESE.- Dada en el Distrito Metropolitano de Quito, el 11 de septiembre de 2023.

LA PRESIDENTE,

Firmado electrónicamente por:
MARIA LUCRECIA PAULINA VELA ZAMBRANO

Mgs. María Paulina Vela Zambrano

Proveyó y firmó la Resolución que antecede la magíster María Paulina Vela Zambrano, Presidente de la Junta de Política y Regulación Financiera, en el Distrito Metropolitano de Quito, el 11 de septiembre de 2023.- **LO CERTIFICO.**

SECRETARIA TÉCNICA

Firmado electrónicamente por:
NELLY DEL PILAR ARIAS ZAVALA

Mgs. Nelly Arias Zavala