-DESIGNACIÓN-
RESOLUCIÓN JM 251127-04

-FECHA-
2025/11/27

-TÍTULO-
CUARTA RESOLUCIÓN DE FECHA 27 DE NOVIEMBRE DEL 2025 QUE AUTORIZA LA PUBLICACIÓN DEFINITIVA DEL REGLAMENTO SOBRE RIESGO OPERACIONAL

-MODIFICACIÓN-
QUINTA RESOLUCIÓN DE FECHA 2 DE ABRIL DEL 2009

-DESCRIPTORES-
AUTORIZACIÓN PUBLICACIÓN; MODIFICACIÓN INTEGRAL; REGLAMENTO SOBRE RIESGO OPERACIONAL; RIESGO OPERACIONAL; BANCO CENTRAL; SUPERINTENDENCIA DE BANCOS;

-TEXTO-
JUNTA MONETARIA
ADMINISTRACIÓN MONETARIA Y FINANCIERA

AVISO

Para los fines procedentes, la Junta Monetaria ha dictado su **Cuarta Resolución** en fecha **27 de noviembre del 2025**, cuyo texto se transcribe a continuación:

"VISTA la comunicación núm.12902 de fecha 25 de noviembre del 2025, dirigida al Gobernador del Banco Central y Presidente de la Junta Monetaria, mediante la cual el Gerente de dicha Institución remite la solicitud de aprobación definitiva de la propuesta de modificación integral del Reglamento sobre Riesgo Operacional, aprobado para consulta pública por dicho Órgano Superior en su Tercera Resolución de fecha 5 de septiembre del 2024;

VISTA la Constitución de la República Dominicana, proclamada en fecha 27 de octubre del 2024;

VISTA la Ley núm.183-02 Monetaria y Financiera de fecha 21 de noviembre del 2002 y sus modificaciones;

VISTA la Ley núm.92-04 que crea el Programa Excepcional de Prevención del Riesgo para las Entidades de Intermediación Financiera, de fecha 27 de enero del 2004;

VISTA la Ley núm.107-13 sobre los Derechos de las Personas en sus Relaciones con la Administración y el Procedimiento Administrativo, de fecha 6 de agosto del 2013;

VISTA la Ley núm.155-17 contra el Lavado de Activos y el Financiamiento del Terrorismo, de fecha 1º de junio del 2017;

…/

VISTA la Ley núm.122-21 que Transforma el Banco Nacional de las Exportaciones en el Banco de Desarrollo y Exportaciones (BANDEX), de fecha 28 de junio del 2021;

VISTO el Reglamento de Sanciones, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 18 de diciembre del 2003 y sus modificaciones;

VISTO el Reglamento sobre Riesgo Operacional, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 2 de abril del 2009 y sus modificaciones;

VISTO el Reglamento sobre Gobierno Corporativo, aprobado mediante la Primera Resolución dictada por la Junta Monetaria en fecha 2 de julio del 2015 y sus modificaciones;

VISTO el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos, aprobado mediante la Tercera Resolución adoptada por la Junta Monetaria en fecha 16 de marzo del 2017;

VISTO el Reglamento de Seguridad Cibernética y de la Información, aprobado mediante la Segunda Resolución adoptada por la Junta Monetaria en fecha 1º de noviembre del 2018;

VISTO el Reglamento Cambiario aprobado mediante la Primera Resolución dictada por la Junta Monetaria en fecha 11 de septiembre del 2025;

VISTO el Reglamento de Sistemas de Pago aprobado mediante la Segunda Resolución dictada por la Junta Monetaria en fecha 28 de agosto del 2025;

VISTO el Instructivo para la Aplicación del Reglamento sobre Riesgo Operacional, aprobado por la Superintendencia de Bancos mediante la Circular SB: núm.011/10 de fecha 9 de agosto del 2010;

VISTO el Instructivo sobre Tercerización o Subcontratación de Servicios (*Outsourcing*), aprobado por la Superintendencia de Bancos mediante Circular SB: núm.011/12 de fecha 28 de diciembre del 2012;

VISTO el Instructivo para la administración y funcionamiento de la Plataforma Cambiaria BCRD aprobado por el Banco Central en fecha 21 de octubre del 2019 y sus modificaciones;

VISTO el Marco de Supervisión Basada en Riesgos aprobado por la Superintendencia de Bancos mediante la Circular SB: núm.003/13 de fecha 3 de junio del 2013 y sus modificaciones;

VISTO el Manual de Solicitudes de Autorización, No Objeción y Notificaciones de las Entidades Supervisadas por la Superintedencia de Bancos, aprobado mediante la Circular SB: CSB-REG-202500007 de fecha 7 de abril del 2025;

VISTO el Manual de Requerimientos de Información de la Administración Monetaria y Financiera, aprobado por la Superintendencia de Bancos mediante la Circular SB: núm.002/2012 de fecha 14 de marzo del 2012 y sus modificaciones;

VISTA la Tercera Resolución dictada por la Junta Monetaria en fecha 5 de septiembre del 2024, que autorizó la publicación para fines de consulta pública de la propuesta de modificación integral del Reglamento sobre Riesgo Operacional;

…/

VISTA la Sexta Resolución dictada por la Junta Monetaria en fecha 17 de julio del 2025, que autorizó la publicación para fines de consulta pública de la propuesta de modificación al Reglamento Cambiario e incorpora a los agentes de cambio y agentes de remesas y cambio al ámbito de aplicación del Proyecto de Reglamento de Riesgo Operacional;

VISTA la propuesta de modificación integral del Reglamento sobre Riesgo Operacional;

VISTA la Matriz comparativa contentiva de las modificaciones propuestas y observaciones al Reglamento sobre Riesgo Operacional;

VISTOS los demás documentos que integran este expediente;

CONSIDERANDO que la Junta Monetaria, mediante la citada Tercera Resolución, autorizó la publicación para fines de consulta pública de los sectores interesados, de la propuesta de modificación al Reglamento sobre Riesgo Operacional, estableciendo un plazo de 30 días para la recepción de observaciones, con el objeto de actualizar y robustecer el marco regulatorio relativo a la gestión de este riesgo, alineándolo con las mejores prácticas internacionales;

CONSIDERANDO que posteriormente, mediante el Ordinal 2 de la citada Sexta Resolución, la Junta Monetaria dispuso incorporar a los agentes de cambio y agentes de remesas y cambio al ámbito de aplicación de la referida propuesta de modificación del Reglamento de Riesgo Operacional, a fin de que les sean aplicables las disposiciones relativas a la gestión del riesgo operacional, incluyendo lo concerniente al requerimiento de capital, en atención a la naturaleza, volumen y cantidad de las operaciones que estos realizan;

CONSIDERANDO que lo dispuesto en la antes mencionada Sexta Resolución persigue que, el Banco Central y la Superintendencia de Bancos por vía de instructivo, puedan detallar reglas especiales que hagan aplicables a dichos intermediarios cambiarios las disposiciones del citado proyecto de Reglamento de Riesgo Operacional, incluyendo los requerimientos de capital por riesgo operacional. Estas reglas especiales deberán observar, sin que sea limitativo, la naturaleza, volumen y cantidad de las operaciones realizadas por los intermediarios cambiarios, su interconexión con las entidades de intermediación financiera, las contrapartes con las cuales operan, así como otros aspectos que, por su efecto prudencial y de mayor transparencia, puedan fundamentarse para ser aplicables a los intermediarios cambiarios;

CONSIDERANDO que la propuesta de modificación, que se presenta para ponderación y aprobación definitiva por parte de la Junta Monetaria, incorpora las observaciones recibidas de los sectores interesados, tales como la Asociación de Bancos de la República Dominicana, Inc. (ABA), la Liga Dominicana de Asociaciones de Ahorros y Préstamos, Inc. (LIDAAPI) y la Asociación de Bancos de Ahorro y Crédito (ABANCORD); y el Scotiabank República Dominicana, S.A., Banco Múltiple;

CONSIDERANDO que las opiniones recibidas en el plazo previsto fortalecieron la propuesta normativa, aportando perspectivas diversas y especializadas en materia de riesgo operacional, las cuales fueron revisadas y analizadas conjuntamente por los equipos técnicos del Banco Central y de la Superintendencia de Bancos, con miras a obtener un texto consensuado que refleje de manera efectiva las perspectivas y necesidades del sector y preserve la solidez del marco regulatorio;

…/

CONSIDERANDO que mediante la citada comunicación de fecha 25 de noviembre del 2025, la Gerencia del Banco Central indica que, como resultado de la ponderación realizada por los equipos técnicos, fueron acogidas las observaciones siguientes:

a) Modificar en el artículo 4 algunas definiciones para adaptarlas al marco de la ISO 31000, cuyos principios se alinean con los objetivos y recomendaciones de Basilea para la gestión del riesgo operacional;

b) Eliminar la parte in fine del artículo 6 relativa a la evaluación de adecuación de capital y posición de liquidez dentro del marco de gestión de riesgo operacional, por tratarse de procesos ya regulados en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos;

c) Modificar el literal a) del artículo 13 para disponer que los controles de mitigación del riesgo operacional se definan conforme a la metodología establecida por cada entidad;

d) Modificar el literal b) del artículo 13 para que la segunda línea de defensa pueda emitir recomendaciones cuando identifique fallas en la gestión del riesgo operacional de las unidades de negocio;

e) Eliminar el artículo 16, en vista de que no especifica las situaciones de notificación sobre riesgo operacional al Banco Central y a la Superintendencia de Bancos, y en atención a que es un aspecto regulado en otros apartados del Reglamento;

f) Modificar el artículo 20, sobre el 'Comité de Riesgo Operacional', a fin de establecer que la Superintendencia de Bancos y el Banco Central requerirán a las entidades, conforme a criterios de proporcionalidad determinados mediante instructivo, disponer de un Comité interno de la Alta Gerencia para la gestión del riesgo operacional, así como eliminar el párrafo II, con el propósito de evitar incertidumbre respecto de cuáles entidades deben contar con dicho Comité;

g) Modificar el artículo 22 para aclarar que la aplicación de las políticas de riesgo operacional de un grupo financiero corresponde a cada entidad y no al conglomerado, preservando el alcance de la supervisión prudencial;

h) Incorporar un artículo relativo al tratamiento aplicable a sucursales o subsidiarias de bancos extranjeros, en coherencia con lo dispuesto en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos;

i) Incluir en el artículo 23 la responsabilidad del Consejo de asegurar canales de reporte claros y estructurados para la información relacionada con el riesgo operacional;

j) Incorporar disposiciones en el artículo 28 que faculten a la unidad especializada de riesgo operacional a proponer medidas correctivas cuando se identifiquen deficiencias y a utilizar herramientas para el análisis de eventos de riesgo operacional materializados;

k) Modificar el párrafo del artículo 59 para precisar que las entidades deben mantener por separado los registros de eventos con pérdidas no materializadas, incluidos entre otros, aquellos cuyo impacto fue mitigado por controles;

…/

l) Eliminar el artículo 85, relativo a 'Supervisiones Especiales o Temáticas', debido a que este proceso se rige por el Marco de Supervisión Basada en Riesgos de la Superintendencia de Bancos;

m) Eliminar el artículo 86, en vista de que los aspectos señalados se encuentran regulados en el Manual de Solicitudes de Autorización, No Objeción y Notificaciones de la Superintendencia de Bancos; y,

n) Modificar el artículo 90 para disponer que las notificaciones sobre eventos materiales de riesgo operacional se realicen conforme al Manual de Solicitudes de Autorización, No Objeción y Notificaciones de la Superintendencia de Bancos.

CONSIDERANDO que asimismo, entre las opiniones recibidas, se identificaron observaciones que, si bien fueron ponderadas técnicamente, no resulta procedente incorporarlas en la propuesta de modificación normativa, ya que, en su mayoría, buscaban ampliar el nivel de detalle del Reglamento en aspectos metodológicos u operativos que, conforme a las mejores prácticas y al marco regulatorio vigente, corresponden a los instructivos de aplicación o a la gestión interna de cada entidad;

CONSIDERANDO que se recibieron comentarios orientados a modificar disposiciones vinculadas a la cultura de riesgo operacional, los sistemas de incentivos, la alineación de las políticas de compensación con el apetito y tolerancia al riesgo, así como las responsabilidades de la primera línea de defensa en la identificación y autoevaluación de controles. Tras su análisis, se mantuvieron las referidas disposiciones por estar en consonancia con los principios del Comité de Supervisión Bancaria de Basilea y por constituir elementos necesarios para fortalecer la gestión del riesgo operacional en el sistema financiero;

CONSIDERANDO que, entre las observaciones, se plantearon inquietudes relacionadas con la creación del Comité de Riesgo Operacional, la definición de sus responsabilidades y su interacción con el Comité de Gestión Integral de Riesgos. En estos casos, se confirmó que el diseño propuesto responde a criterios de proporcionalidad y que su funcionamiento no genera duplicidades, dado que las funciones asignadas difieren en alcance, jerarquía y naturaleza, por tanto, se mantuvo, el enfoque originalmente planteado;

CONSIDERANDO que otras opiniones se refirieron al alcance de la divulgación del marco de gestión, a la facultad de la autoridad para requerir información adicional, a los criterios de materialidad para la notificación de eventos relevantes y a los plazos para su reporte. Estas disposiciones se mantienen conforme a la propuesta, al estar alineadas con los lineamientos del Pilar 3 de Basilea, con el Reglamento de Gobierno Corporativo, con el Reglamento de Seguridad Cibernética y de la Información y con el Marco de Supervisión Basada en Riesgos. En cuanto a la distinción entre notificaciones y solicitudes de no objeción, la misma ya se encuentra regulada en el Manual de Solicitudes de Autorización, No Objeción y Notificaciones de la Superintendencia de Bancos, razón por la cual no fue necesario introducir ajustes adicionales;

CONSIDERANDO que en lo relativo al requerimiento de patrimonio técnico por riesgo operacional, algunas entidades expresaron preocupación por los costos y el tiempo de adecuación. No obstante, se decidió mantener este componente del Reglamento, al estar respaldado por las mejores prácticas internacionales y por los ejercicios de impacto recientemente realizados por el Banco Central y la Superintendencia de Bancos, los cuales

…/

evidencian que el sector financiero cuenta con la holgura suficiente para implementarlo de manera gradual;

CONSIDERANDO que adicionalmente se analizaron observaciones relativas al tratamiento de subsidiarias de bancos extranjeros y a la inclusión del riesgo operacional en la calificación compuesta establecida por la Superintendencia de Bancos. En ambos casos se mantuvo la redacción prevista, en consistencia con el Marco de Supervisión Basada en Riesgos vigente y con los estándares internacionales aplicables a entidades supervisadas;

CONSIDERANDO que en cumplimiento de lo dispuesto en el Ordinal 2 de la citada Sexta Resolución, se incorpora a la propuesta presentada a los agentes de cambio y a los agentes de remesas y cambio dentro del ámbito de aplicación del Reglamento sobre Riesgo Operacional. Esta ampliación resulta necesaria para fortalecer la resiliencia operacional del ecosistema financiero, dada la creciente participación de estos intermediarios en operaciones cambiarias y su integración al Sistema de Pagos de la República Dominicana (SIPARD) y a la Plataforma Cambiaria del Banco Central. En consecuencia, se requiere que cuenten con marcos de gestión sólidos y mecanismos suficientes para prevenir, detectar y mitigar incidentes que puedan afectar la continuidad de sus operaciones o la integridad de la información que procesan;

CONSIDERANDO que con el propósito anteriormente expuesto, se incorpora a la propuesta un nuevo título orientado exclusivamente a los intermediarios cambiarios, en el cual se establecen los lineamientos generales que deberán observar para gestionar de forma adecuada su riesgo operacional. Este marco comprende, entre otros aspectos, la obligación de contar con una política y estructura de gestión proporcional a su naturaleza y volumen de actividades; mecanismos de control interno independientes; y una función de riesgo operacional con acceso al consejo de administración. Asimismo, se dispone que su gestión de riesgo tecnológico y de seguridad de la información sea coherente con el Reglamento Cambiario y que cumpla con los requisitos técnicos y de control necesarios para su integración al Sistema de Pagos de la República Dominicana (SIPARD) y a la Plataforma Cambiaria del Banco Central, notificando oportunamente cualquier incidente grave que pueda afectar la disponibilidad, integridad o confidencialidad de la información;

CONSIDERANDO que, además, se incorpora un esquema aplicable a la remisión de información y al requerimiento de capital por riesgo operacional para los intermediarios cambiarios, el cual será desarrollado mediante instructivos que definirán los parámetros, umbrales y criterios de proporcionalidad correspondientes. Este enfoque permitirá armonizar sus obligaciones con la realidad operativa del sector, garantizando estándares mínimos de gestión, control y solvencia acordes con su participación en el sistema financiero;

CONSIDERANDO que como resultado de la inclusión de los intermediarios cambiarios en la propuesta de modificación al citado Reglamento sobre Riesgo Operacional se fortalece la coherencia del marco regulatorio y contribuye a asegurar que todos los participantes expuestos a riesgos operacionales relevantes cuenten con estándares mínimos de gobernanza, control y capitalización, conforme las mejores prácticas internacionales;

PONDERADOS los planteamientos de los Miembros de la Junta Monetaria, en el sentido de que esta propuesta de modificación del Reglamento sobre Riesgo Operacional responde a los estándares internacionales y a las mejores prácticas que permiten fortalecer la gestión del riesgo operacional en el sistema financiero. Una vez ponderadas las observaciones presentadas por los

…/

sectores interesados, acogiendo aquellas que enriquecen la iniciativa, esta propuesta se constituye en una pieza normativa que traza los criterios, políticas, sistemas y mecanismos que deberán adoptar las entidades para una adecuada gestión de riesgo operacional;

CONSIDERANDO que en atención a todo lo expuesto precedentemente, la Junta Monetaria decide autorizar la modificación definitiva del Reglamento sobre Riesgo Operacional;

Por tanto, la Junta Monetaria

R E S U E L V E:

1. Aprobar la versión definitiva de la modificación integral al Reglamento sobre Riesgo Operacional, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 2 de abril del 2009 y sus modificaciones, para que, en lo adelante, se lea de la manera siguiente:

'REGLAMENTO SOBRE RIESGO OPERACIONAL

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO, ALCANCE Y ÁMBITO DE APLICACIÓN

Artículo 1. **Objeto.** Este Reglamento tiene por objeto establecer los criterios y lineamientos generales que deberán aplicar las entidades de intermediación financiera y los intermediarios cambiarios, para realizar una adecuada gestión del riesgo operacional, en cumplimiento con las disposiciones contenidas en el literal f) del artículo 46, y los literales a) y b) del artículo 55, de la Ley Monetaria y Financiera.

Artículo 2. Alcance. Este Reglamento comprende las políticas y procedimientos mínimos que deberán implementar las entidades de intermediación financiera y los intermediarios cambiarios para identificar, medir, evaluar, monitorear y controlar el riesgo operacional al que están expuestos, así como las consideraciones de lugar para el desarrollo del plan de continuidad de negocios y resiliencia operativa y la metodología para el cómputo del requerimiento de capital por riesgo operacional.

Artículo 3. Ámbito de Aplicación. Las disposiciones establecidas en este Reglamento son de aplicación para las entidades que se identifican a continuación:

a) Bancos múltiples;

b) Bancos de ahorro y crédito;

c) Corporaciones de crédito;

d) Asociaciones de ahorros y préstamos;

e) Entidades públicas de intermediación financiera;

f) Agentes de cambio; y,

g) Agentes de remesas y cambio.

Párrafo. Las disposiciones de este Reglamento serán aplicables a los intermediarios cambiarios debidamente autorizados por la Junta Monetaria, exclusivamente en lo relativo a la gestión del riesgo operacional previsto en el Título VII, sin perjuicio de lo dispuesto en el Reglamento Cambiario.

CAPÍTULO II
GLOSARIO DE TÉRMINOS

Artículo 4. Definiciones. Para los fines de aplicación de las disposiciones contenidas en este Reglamento, los términos y expresiones que se indican más adelante, tanto en mayúscula como en minúscula y, en singular o en plural, tendrán los significados siguientes:

a) **Alta Gerencia:** La integran los principales ejecutivos u órganos de gestión, responsables de planificar, dirigir y controlar las estrategias y las operaciones generales de la entidad, que han sido previamente aprobadas por el Consejo. La estructura de la Alta Gerencia será acorde al tamaño y la complejidad de la entidad;

b) **Apetito de Riesgo:** Límite agregado en función de los tipos de riesgos que el Consejo y la Alta Gerencia están dispuestos a asumir y gestionar para cumplir sus objetivos de negocios y obligaciones con partes interesadas;

c) **Capacidad de Riesgo:** Umbral máximo de riesgo que la entidad puede asumir dado su nivel actual de recursos y desde la perspectiva de las partes interesadas, sin infringir las restricciones determinadas por el capital y los niveles de liquidez reglamentarios, el ambiente operativo y sus obligaciones;

d) **Comité de Gestión Integral de Riesgos o Comité de Riesgos:** Órgano creado por el Consejo, responsable del diseño de las políticas, sistemas, metodologías, modelos y procedimientos para la gestión integral de los riesgos de la entidad;

e) **Confidencialidad:** Es la preservación de la información o procesos, a fin de que estos no sean divulgados, en todo o en parte, a personas físicas o jurídicas, a menos que estos hayan sido autorizados para acceder a dicha información. Incluye los medios para proteger la privacidad personal y la información esencial;

f) **Consejo:** Órgano máximo de dirección que tiene todas las facultades de administración y representación de la entidad, responsable de velar por el buen desempeño de la Alta Gerencia en la gestión, no pudiendo delegar su responsabilidad. Se refiere al Consejo de Directores, Consejo de Administración o Junta de Directores, según corresponda;

g) **Continuidad de Negocio:** Capacidad de una entidad para continuar con la entrega de productos y la prestación de servicios a niveles predefinidos y aceptables tras una interrupción;

h) **Control:** Cualquier acción, política, procedimiento, práctica o recurso, diseñado por la entidad con la finalidad de gestionar y mitigar el nivel de uno o varios riesgos para asegurar que se mantengan dentro de los límites aceptables que permitan alcanzar los objetivos organizacionales a través de la reducción de la probabilidad y/o el impacto de estos;

i) **Control Dual:** Proceso que consiste en la protección de información confidencial, funciones o actividades críticas, a través de dos o más entidades distintas;

j) **Cultura de Riesgo Operacional:** Conjunto de valores, actitudes, competencias y comportamientos individuales y corporativos, que determinan el compromiso y el estilo de gestión del riesgo operacional de una entidad;

k) **Disponibilidad:** La propiedad de los recursos (información, sistemas, equipos, entre otros), de ser accesibles y utilizables a pedido de un usuario, entidad o proceso, cuando sea necesario y autorizado, en los casos que aplique;

l) **Evento de Riesgo Operacional:** Suceso o serie de sucesos originados por la misma causa, internos o externos a la entidad, que surgen por la materialización de un riesgo debido a fallas en procesos, personas y sistemas internos o por eventos externos que pudieran derivar impactos de pérdidas a las entidades afectadas;

m) **Eventos con Pérdidas no Materializadas:** Suceso o serie de sucesos con la capacidad de provocar pérdidas, económicas o no económicas a la entidad, cuyo impacto no se produjo;

n) **Factores de Riesgo:** Fuentes generadoras de eventos que originan o que pueden aumentar la probabilidad de que ocurra un evento de riesgo operacional o intensificar sus consecuencias, a nivel de la actividad o de la unidad de negocio;

o) **Gestión del Cambio:** Marco para gestionar los efectos de los nuevos procesos de negocios, actividades, productos, servicios, mercados o jurisdicciones desconocidas, así como implementaciones de procesos comerciales o sistemas tecnológicos nuevos o modificados;

p) **Gestión de Riesgos:** Conjunto de políticas y procedimientos mediante el cual se identifican, miden, evalúan, monitorean y controlan los riesgos inherentes al negocio, con el objeto de conocer su grado de exposición en el desarrollo de sus operaciones y definir los mecanismos de cobertura para proteger los recursos propios y de terceros que se encuentran bajo su control y administración;

q) **Gestor de Riesgo Operacional:** Personal designado de cada unidad de negocio para ejecutar las actividades de gestión de riesgo operacional de su respectiva unidad y que sirve como enlace con la unidad especializada de riesgo operacional;

…/

r) **Impacto:** Una o varias consecuencias de un evento de riesgo operacional, expresado en términos cuantitativos o cualitativos. Estos pueden ser pérdidas directas, indirectas, entre otros;

s) **Infraestructura tecnológica:** Equipo y sistemas con que cuenta la entidad para procesar la información, así como las adecuaciones del espacio físico que los aloja;

t) **Integridad:** Propiedad que poseen los datos, que asegura que estos no han sido alterados o destruidos de manera no autorizada, durante su creación, transmisión o almacenamiento;

u) **Línea de Defensa:** Grupo organizacional perteneciente al modelo de 3 líneas (operativa, supervisora y evaluación independiente), que participa activamente en la gestión y monitoreo del riesgo, mediante funciones y responsabilidades debidamente establecidas;

v) **Lucro Cesante:** Ganancia o ingreso económico que deja de percibir la entidad a consecuencia de la ocurrencia de un evento de riesgo operacional, como es el caso de pagos dejados de recibir por fallas en el sistema;

w) **Mapa de Calor de Riesgos:** Representación gráfica, utilizando una escala de colores, que presenta de forma resumida los niveles de los riesgos inherentes o residuales, para ayudar a la entidad a priorizar los riesgos identificados;

x) **Mapeo de Procesos:** Herramienta de gestión que permite identificar y estudiar todos los pasos de un procedimiento o tarea utilizada en la organización, con la finalidad de establecer una relación esquemática, que revela oportunidades de mejoras y posibles desequilibrios en la ejecución y la planificación;

y) **Materialización del Riesgo:** Realización del evento previamente determinado como incierto, convirtiendo el riesgo en un hecho o acontecimiento real, que conlleva generalmente daños o pérdidas para la entidad;

z) **Matriz de Riesgos Operacionales:** Herramienta que permite identificar los riesgos inherentes y residuales de una determinada actividad, proceso, producto o servicio en la entidad, así como evaluar la efectividad de la gestión de los riesgos y la optimización de los controles;

aa) **Medidas de Contingencia:** Acciones que aseguran la disponibilidad de recursos, operaciones y servicios ante la interrupción de las operaciones ordinarias, que no llegan a activar el plan de continuidad que se tenga definido;

bb) **Nuevo Producto, Servicio o Canal:** Aquel que es lanzado por primera vez en la entidad para ser ofrecido a sus clientes y/o usuarios, así como las modificaciones o derivados de productos preexistentes que requieren de nuevas iniciativas gerenciales, como cambios y desarrollo de sistemas, procesos, modelos de negocio, canales y adquisiciones sustanciales, para su diseño, desarrollo e implementación;

…/

cc) **Operación, Proceso o Servicio Crítico:** Elementos indispensables para la continuidad de negocio y cuya falta de identificación o aplicación deficiente puede generar un impacto negativo;

dd) **Pérdida Bruta:** Monto de dinero total que comprende las pérdidas directas e indirectas antes de aplicar recuperaciones de cualquier tipo;

ee) **Pérdida Directa:** Monto de dinero que se pierde directamente por la ocurrencia del evento de pérdida, sea esta recuperable o no, como es el monto del dinero robado de caja, valor del equipo robado, entre otros. Incluye las provisiones realizadas producto del evento;

ff) **Pérdida Económica:** Monto de dinero cuyo impacto negativo es registrado en cuentas de resultados o en la situación patrimonial de la entidad, provocado por un evento de riesgo operacional. Incluye las pérdidas directas e indirectas, pero no el lucro cesante;

gg) **Pérdida Indirecta:** Monto de dinero adicional que se pierde o se gasta por la ocurrencia del evento de pérdida, como es el pago de abogados externos por demanda en contra de la entidad, pago de consultor de tecnología para recuperación de datos, entre otros;

hh) **Pérdida Neta:** Monto de dinero que resulta después de tener en consideración los efectos de las recuperaciones (Pérdida Neta = Pérdida Bruta – Recuperaciones);

ii) **Pérdida No Económica:** Efecto negativo de un evento de riesgo operacional por el cual no se producen pérdidas económicas, debido a una situación fortuita distinta del control;

jj) **Pérdida por Riesgo Operacional:** Efecto negativo ocasionado por eventos de riesgo operacional que pudieran ser de carácter financiero (pérdida económica) o de carácter no financiero, pero con perjuicio de otros aspectos de la organización (pérdida no económica);

kk) **Perfil de Riesgo Operacional:** Resultado de la evaluación en el tiempo de las exposiciones inherentes y residuales, después de tomar en cuenta los mitigantes para cada categoría relevante de riesgo operacional;

ll) **Pista de Auditoría:** Registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

mm) **Plan de Gestión de Continuidad de Negocio:** Conjunto formado por planes de actuación, de emergencia, de comunicación y de contingencia, destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre las actividades de una entidad, con la respuesta, recuperación y reanudación de un nivel predefinido de operación después de una interrupción;

nn) **Procedimiento:** Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de los cuales se asegura el cumplimiento de una función operativa;

…/

oo) **Probabilidad:** Posibilidad de ocurrencia de un evento que usualmente es aproximada mediante una distribución estadística, y que, en ausencia de información suficiente, o donde no resulta posible obtenerla, se puede aproximar mediante métodos cualitativos.

pp) **Recuperación de Pérdidas Económicas:** Hecho independiente relacionado con el evento de riesgo operacional inicial, pero separado en el tiempo, por el que se perciben fondos procedentes de un tercero, ya sea a través de seguros o por otros medios, que restituye de forma parcial o total el impacto monetario de un evento de riesgo operacional con pérdida económica;

qq) **Resiliencia Operativa:** Capacidad de una entidad para realizar operaciones críticas tras la ocurrencia de eventos adversos, permitiendo que esta pueda identificar, protegerse, responder y adaptarse, así como recuperarse y aprender de dichos eventos para minimizar el impacto de las interrupciones en la entrega de operaciones críticas;

rr) **Riesgo:** Posibilidad de que se produzca un hecho o evento con consecuencias negativas para el logro de los objetivos de la entidad;

ss) **Riesgo Inherente:** Riesgo intrínseco relativo al desempeño de las actividades significativas de la entidad y surge de la exposición e incertidumbre de la ocurrencia de probables eventos o cambios futuros en las condiciones del negocio y/o de la economía. Este riesgo se evalúa teniendo en cuenta el grado de probabilidad de ocurrencia de un evento adverso, y su impacto en el capital, utilidades u otros aspectos de la entidad. Es el riesgo propio de cada actividad, y su nivel se mide sin tener en cuenta el efecto de los controles;

tt) **Riesgo Legal:** Probabilidad de que se presenten pérdidas o contingencias negativas como consecuencia de las sanciones, obligaciones de indemnización o medidas correctivas derivadas del incumplimiento, intencional o no, parcial o completo, de las leyes o normas aplicables, así como también de las fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de la entidad, derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de estos;

uu) **Riesgo Operacional:** Probabilidad de sufrir pérdidas debido a la falta de adecuación o a fallos de los procesos internos, personas, infraestructuras o sistemas internos, o bien a causa de acontecimientos externos. Incluye el riesgo legal, riesgo tecnológico y riesgo de seguridad de la información. Excluye el riesgo estratégico y reputacional; sin embargo, como consecuencia de eventos de riesgo operacional puede generarse impacto sobre dichos riesgos;

vv) **Riesgo Residual:** Nivel de riesgo que permanece después de la verificación o estimación de la efectividad de los controles sobre los riesgos inherentes;

ww) **Riesgo Tecnológico:** Posibilidad de que un evento asociado al uso, falla o vulnerabilidad de la tecnología o de la infraestructura tecnológica produzca impactos adversos en la confidencialidad, integridad o disponibilidad de la información en la continuidad de los servicios o en los objetivos del negocio;

…/

xx) **Seguridad de la Información:** Protección de los sistemas de información y de la información en todos sus formatos, durante su almacenamiento, procesamiento o transmisión, contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados, a fin de proporcionar confidencialidad, integridad y disponibilidad de la información;

yy) **Tercerización de Servicios:** Contratación de un proveedor de servicio externo con el objetivo de ceder, parcial o totalmente, la gestión de una función o recurso esencial para los procesos de la entidad, y cuya correcta ejecución dependa del proveedor contratado;

zz) **Tecnología de Información (TI):** Conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software (aplicaciones, sistemas operativos, sistemas de administración de bases de datos, etc.), redes, multimedia, servicios asociados, entre otros;

aaa) **Tolerancia al Riesgo:** Desviación con respecto al apetito de riesgo establecido por la entidad, que está dispuesta a aceptar para el logro de sus objetivos;

bbb) **Unidad de Gestión Integral de Riesgos:** Es la responsable de asegurar la debida identificación, cuantificación, evaluación, control o mitigación sobre todos los riesgos que enfrenta la entidad de intermediación financiera en el desarrollo de sus operaciones e informar a la instancia responsable designada por el Consejo;

ccc) **Unidad Especializada de Gestión de Riesgos:** Es la responsable de ejecutar las disposiciones definidas por la Unidad de Gestión Integral de Riesgos y aprobadas por el Consejo para los riesgos que enfrenta la entidad en el desarrollo de sus operaciones y que se encuentran a su cargo;

ddd) **Unidad de Negocio:** Es la responsable de realizar las funciones operativas, de soporte, corporativas o de servicios compartidos asociados. No incluye a las áreas de control, tales como Gestión de Riesgos y Auditoría interna; y,

eee) **Vulnerabilidad:** Debilidad en el diseño, implementación y/o ejecución de un recurso o proceso que por causa de una amenaza podría permitir la materialización de un riesgo.

TÍTULO II
MARCO Y GESTIÓN DEL RIESGO OPERACIONAL

CAPÍTULO I
MARCO DE GESTIÓN DEL RIESGO OPERACIONAL

Artículo 5. Políticas y Procedimientos de Riesgo Operacional. Las entidades deben contar con adecuados sistemas de identificación, medición, seguimiento, control y prevención de riesgos, así como mecanismos independientes de control interno y establecimiento claro y por escrito de sus políticas y procedimientos administrativos, de conformidad con lo dispuesto en el artículo 55 de la Ley Monetaria y Financiera.

…/

Artículo 6. Marco de Gestión de Riesgo Operacional. Es responsabilidad de cada entidad contar con un marco aprobado por el Consejo, con adecuadas estrategias, políticas, procesos, procedimientos, metodologías, modelos y sistemas para la gestión del riesgo operacional, considerando su tamaño, naturaleza, complejidad, perfil de riesgo, importancia sistémica, situación macroeconómica y de los mercados, y acorde con su apetito y nivel de tolerancia al riesgo.

Párrafo. Los aspectos de buen gobierno corporativo, ambiente de gestión de riesgo operacional, planificación de la continuidad de negocio y divulgación de la información deben estar integrados dentro del marco de gestión de riesgo operacional.

Artículo 7. Alcance del Marco de Gestión. Las entidades deberán asegurar que el marco de gestión de riesgo operacional defina el alcance de las 3 líneas de defensa, de manera que en estas se agrupe la organización en todos sus niveles y la aplicación e integración del marco en los procesos generales de gestión de riesgos de la entidad.

Artículo 8. Cultura de Gestión de Riesgo Operacional. El Consejo deberá instaurar una cultura organizacional guiada por una sólida gestión de riesgo operacional, implementada por la Alta Gerencia, estableciendo estándares, sistema de sensibilización al riesgo operacional e incentivos y garantizando la capacitación adecuada del personal de la entidad en lo relativo a la gestión de riesgos y el código de conducta o política de ética, para un comportamiento responsable y profesional.

Artículo 9. Código de Conducta o Política de Ética. El Consejo deberá establecer dentro de su código de conducta o política de ética lo relacionado con el riesgo asociado a la conducta. A tales fines, establecerá expectativas claras de integridad y valores éticos del más alto nivel, tales como la prohibición e identificación de posibles conflictos de intereses y de la oferta inapropiada de productos y servicios financieros.

Párrafo. El código de conducta o la política de ética deberá ser aprobado y revisado regularmente por el Consejo y debidamente conocido por el personal. Su implementación deberá ser supervisada por un comité de ética de alto nivel u otro comité del Consejo y deberá estar a disposición del público en general.

Artículo 10. Apetito, Tolerancia y Capacidad de Riesgo. El Consejo deberá incorporar en su declaración de apetito y tolerancia al riesgo general, lo relativo al riesgo operacional que articule la naturaleza, los tipos y niveles de riesgo operacional que la entidad esté dispuesta a asumir, vinculándose a su estrategia a corto y largo plazo y considerando los intereses de sus clientes y accionistas. De igual manera, la Alta Gerencia deberá definir la capacidad de riesgo de la entidad para cada tipo de riesgo operacional, la cual deberá ser aprobada por dicho Consejo.

Párrafo I. La entidad deberá definir el marco de apetito por el riesgo alineado a su estrategia, incluyendo las políticas, controles y sistemas mediante los cuales se establece, comunica y monitorea el apetito por el riesgo. Este debe contener la declaración del apetito al riesgo, los límites de tolerancia y capacidad de riesgo, y el esquema de los roles y responsabilidades de los que supervisan la implementación y monitoreo de este marco.

…/

Párrafo II. La declaración del apetito al riesgo operacional debe ser una articulación escrita del nivel agregado de los tipos de riesgo operacional que la entidad está dispuesta a aceptar o evitar para lograr sus objetivos de negocio, incluyendo declaraciones cualitativas y medidas cuantitativas formuladas respecto a ganancias, capital, medidas de riesgo, liquidez y otras medidas relevantes.

Párrafo III. El Comité de Gestión Integral de Riesgos deberá revisar, al menos anualmente, la idoneidad de los límites y la declaración general de apetito y tolerancia al riesgo, incluido el riesgo operacional, considerando los cambios actuales y esperados en el entorno externo, los aumentos continuos o futuros en los volúmenes de negocios o actividades, la calidad del ambiente de control, la efectividad de la gestión de riesgos y las estrategias de mitigación, la experiencia de pérdida y la frecuencia, volumen o naturaleza de las infracciones de límites. Asimismo, deberá monitorear el cumplimiento de la Alta Gerencia con la declaración de apetito y tolerancia al riesgo, proporcionando una detección oportuna y alertando sobre dichas infracciones. El Consejo deberá conocer y aprobar los cambios propuestos producto de estas revisiones.

Artículo 11. Alineación de Políticas de Compensación. Las entidades deberán establecer políticas de compensación para todos los niveles de la organización que estén alineadas con su declaración de apetito y tolerancia al riesgo, y equilibrar adecuadamente el riesgo con la recompensa, evitando promover acciones que generen riesgos mayores a los establecidos.

CAPÍTULO II
GESTIÓN DEL RIESGO OPERACIONAL

Artículo 12. Gestión del Riesgo Operacional. Las entidades establecerán un proceso de gestión del riesgo que les permita identificar, cuantificar, evaluar, vigilar, informar y controlar sus exposiciones al riesgo operacional en el desarrollo de sus negocios y operaciones. En la etapa de control de los riesgos, se deberán considerar los tratamientos al riesgo operacional apropiados según el apetito de riesgo de la entidad, incluyendo evitar, transferir, mitigar y aceptar el riesgo.

Artículo 13. Modelo de Tres Líneas de Defensa. Las entidades deberán implementar el modelo de 3 líneas de defensa para la gestión del riesgo operacional, de acuerdo con su naturaleza, tamaño, complejidad y perfil de riesgo de sus actividades, tomando en consideración la estructura y funciones para cada línea, según se muestra a continuación:

a) **Primera Línea de Defensa:** Corresponde a la línea funcional (Unidades de Negocio), la cual tiene la propiedad del riesgo, por lo que reconoce y gestiona el riesgo en el que incurre al realizar sus actividades. También es responsable de planificar, dirigir y controlar las operaciones diarias de una actividad significativa o proceso, así como de identificar y gestionar los riesgos operacionales en los productos, actividades, procesos y sistemas por los cuales es responsable. En adición, debe implementar controles apropiados para mitigar el riesgo operacional inherente y verificar la efectividad de dichos controles, de acuerdo con la metodología definida por cada entidad;

…/

b) **Segunda Línea de Defensa:** Las entidades deberán contar formalmente con una función de gestión de riesgos en su estructura organizacional que haga la función de segunda línea de defensa. Esta deberá contar con los recursos e independencia adecuada, tener una estructura de reporte que sea independiente de las unidades de negocio que generan riesgo operacional y estar contemplada en la estrategia de gestión de riesgos de la entidad. Esta línea corresponde a las actividades de supervisión del proceso de identificación, medición, monitoreo y reporte objetivo del riesgo operacional; y, representa una recopilación de actividades y procesos de gestión de riesgos operacionales, incluido el diseño y la implementación del marco para la gestión de dichos riesgos. La segunda línea de defensa debe proporcionar recomendaciones y efectuar alertas y revisiones especializadas relacionadas con la Gestión del Riesgo Operacional, así como evaluaciones objetivas de la medición y estimación de riesgos, incluyendo la efectividad de los controles realizados por las unidades de negocio. En adición, en esta línea se establecen herramientas de informes que incluyen alertas y recomendaciones para proporcionar una seguridad razonable de la gestión; y,

c) Tercera Línea de Defensa: Las revisiones de la tercera línea serán realizadas por la auditoría interna y externa de la entidad. El personal de esta función no debe participar en el desarrollo, implementación u operación de los procesos de gestión de riesgos elaborados por las otras 2 líneas de defensa. El alcance y la frecuencia de las revisiones deberán ser suficientes para cubrir todas las actividades de la entidad, verificar que el marco de gestión del riesgo operacional se haya implementado según lo previsto y funcione de manera efectiva, así como dar seguimiento a los informes del ente supervisor.

Párrafo I. Las entidades deberán asegurarse de que el enfoque de las 3 líneas de defensa funcione satisfactoriamente, debiendo el Consejo, la auditoría independiente y la Alta Gerencia asegurarse de que este se implemente y opere de manera adecuada.

Párrafo II. Las entidades deberán asegurarse de que cada línea de defensa cuente con los aspectos siguientes:

a) Recursos adecuados en términos de presupuesto, herramientas y personal;

b) Funciones y responsabilidades claramente definidas y documentadas;

c) Capacitación continua y adecuada del personal;

d) Sólida cultura de gestión de riesgos en toda la organización; y,

e) Comunicación efectiva entre las líneas de defensa para reforzar el marco de gestión de riesgo operacional.

Artículo 14. Roles y Responsabilidades en la Gestión del Riesgo. Las entidades deberán establecer, documentar y comunicar de manera formal, clara y efectiva, los roles y responsabilidades de su personal respecto de la gestión del riesgo operacional a los fines de

garantizar que estos comprendan sus competencias, así como su autoridad para actuar frente a dicho riesgo.

Artículo 15. Capacitación en Riesgo Operacional. La Alta Gerencia deberá procurar un nivel adecuado de capacitación en riesgo operacional y formación ética en todos los niveles de la organización, debiendo reflejar el rol y las responsabilidades de las personas a quienes estén destinadas.

Párrafo. Se deberá proveer capacitación técnica en gestión del riesgo operacional a los responsables de procesos y gestores de riesgo operacional designados, así como al personal de la unidad especializada de riesgo operacional y la unidad de auditoría interna.

Artículo 16. Enfoque de Resiliencia Operativa. Las estructuras de gobierno de las entidades deberán establecer, supervisar e implementar un enfoque eficaz de resiliencia operativa, con capacidad de proveer y mantener operaciones críticas durante disrupciones, que les permita responder y adaptarse, así como recuperarse y aprender de los eventos adversos para minimizar su impacto en la entrega de operaciones críticas.

TÍTULO III
GOBERNANZA DEL RIESGO OPERACIONAL

CAPÍTULO I
ESTRUCTURA EN LA GESTIÓN DEL RIESGO OPERACIONAL

Artículo 17. Organización. La estructura de la gestión del riesgo operacional deberá estar acorde con la naturaleza, tamaño, complejidad, perfil de riesgo e importancia sistémica de la entidad. Dicha estructura estará conformada por el Comité de Gestión Integral de Riesgos, la Unidad de Gestión Integral de Riesgo y las unidades especializadas. La Unidad de Gestión Integral de Riesgos podrá delegar en las unidades especializadas las distintas funciones relativas al manejo de sus riesgos operacionales, a los riesgos tecnológicos, de seguridad de la información y legales.

Párrafo. Las entidades deberán revisar la estructura, al menos anualmente, para verificar su idoneidad e independencia con respecto a las demás líneas de defensa (primera y tercera línea), a medida que cambien las estrategias y/o estructura de la entidad.

Artículo 18. Comité de Gestión Integral de Riesgos. El Comité de Gestión Integral de Riesgos deberá vigilar que las operaciones relativas a riesgo operacional se ajusten a los objetivos, políticas, estrategias, procedimientos y a los niveles de capacidad, tolerancia y apetito al riesgo aprobados. Dicho Comité reportará al Consejo.

Artículo 19. Comité de Riesgo Operacional. Dependiendo del tamaño y complejidad de la entidad y en función de los criterios de proporcionalidad aplicables, la Superintendencia de Bancos o el Banco Central le requerirán a las entidades disponer de un Comité interno de la Alta Gerencia para la gestión del riesgo operacional. En ausencia de un requerimiento expreso, las

entidades deberán incorporar la gestión del riesgo operacional como parte de las funciones del Comité de Gestión Integral de Riesgos.

Párrafo. Este Comité deberá contar con miembros de la Alta Gerencia de diversos perfiles y experiencias, debiendo abarcar áreas o actividades financieras, asuntos legales, tecnológicos, de seguridad de la información, regulatorios y de gestión de riesgos.

Artículo 20. Unidad Especializada de Riesgo Operacional. Esta responderá funcional y administrativamente a la Unidad de Gestión Integral de Riesgos, que a su vez responderá funcionalmente al Comité de Gestión Integral de Riesgos. No debe tener responsabilidad de una unidad de negocio, ni actividad que asuma riesgo para la entidad.

Artículo 21. Gestión del Riesgo Operacional para Entidades de un Grupo Financiero. Las entidades que dependan de un mismo controlador o conformen un Grupo Financiero podrán contar con una unidad de riesgo que incluya el riesgo operacional a nivel individual y global. Estas entidades deberán adoptar políticas y procedimientos internos, que consideren el riesgo a nivel individual, así como el riesgo operacional transferido de las demás entidades coligadas o vinculadas por administración.

Artículo 22. Gestión del Riesgo Operacional para Entidades que sean Sucursales o Subsidiarias de Bancos Extranjeros. En las sucursales o subsidiarias de entidades extranjeras, la función de gestión de riesgo operacional puede ser realizada por el área encargada de la gestión de riesgos de la casa matriz o unidad regional que tenga un mandato para el grupo financiero completo o para la región a la que pertenece la entidad de intermediación financiera que opera en el país. La función de riesgos de las sucursales o subsidiarias tendrá la responsabilidad de procurar la gestión del riesgo conforme al marco normativo local vigente.

Párrafo. La documentación soporte de la evaluación realizada sobre la gestión de riesgos deberá estar disponible a requerimiento de la Superintendencia de Bancos.

CAPÍTULO II
RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO OPERACIONAL

Artículo 23. Responsabilidad del Consejo. En adición a las responsabilidades definidas en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos, el Consejo tendrá, sin que estas sean limitativas, las funciones siguientes:

a) Aprobar y revisar periódicamente las estrategias, políticas, procesos, apetito de riesgo, así como la eficacia de los controles relacionados, que permitan una adecuada gestión del riesgo operacional al que está expuesta la entidad, y velar por su cumplimiento, vigilando que la Alta Gerencia implemente las medidas necesarias para monitorear y controlar estos riesgos;

b) Velar por que la entidad tenga procesos adecuados para comprender la naturaleza y el alcance del riesgo operacional inherentes de las estrategias, actividades actuales y planificadas por ésta;

c) Asegurar que los procesos de gestión del riesgo operacional estén completamente integrados en el marco general de la entidad;

…/

d) Definir una visión clara sobre los principios del marco de gestión del riesgo operacional y garantizar que las políticas correspondientes, desarrolladas por la Alta Gerencia, estén alineadas con estos principios;

e) Aprobar el sistema de incentivos para la sensibilización del riesgo operacional;

f) Asignar los recursos necesarios para la adecuada gestión del riesgo operacional, como lo son la infraestructura, metodología y personal;

g) Obtener un aseguramiento razonable de que los principales riesgos operacionales identificados se encuentran dentro de los límites de capacidad, tolerancia y apetito al riesgo establecidos;

h) Supervisar regularmente el diseño y la efectividad del marco de gestión del riesgo operacional de la entidad, asegurándose de que se haya identificado y se esté gestionando el riesgo operacional derivado de los cambios del mercado y otros factores externos, así como aquellos asociados a nuevos productos, actividades, procesos o sistemas, cambios en los perfiles y prioridades de riesgo;

i) Velar por que el marco de gestión del riesgo operacional de la entidad esté sujeto a una revisión independiente efectiva por una tercera línea de defensa;

j) Supervisar que la entidad se mantenga actualizada con las mejores prácticas de gestión del riesgo operacional;

k) Establecer líneas claras de responsabilidad de gestión y de implementación para un entorno de control sólido; y,

l) Asegurar que la entidad cuente con canales de reporte claros y estructurados para ser informados en relación con el riesgo operacional.

Artículo 24. Responsabilidad del Comité de Gestión Integral de Riesgos. Las principales responsabilidades de este Comité serán aquellas establecidas en el Reglamento sobre Gobierno Corporativo y en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos, sin que estas sean limitativas.

Artículo 25. Responsabilidad del Comité de Riesgo Operacional. Las responsabilidades de este Comité serán las delegadas por el Comité de Gestión Integral de Riesgos, incluyendo acciones de monitoreo, seguimiento y toma de decisiones para la gestión del riesgo operacional. En adición, este Comité tendrá las responsabilidades siguientes:

a) Revisar la estrategia para la gestión del riesgo operacional;

b) Monitorear y evaluar los resultados de la gestión del riesgo operacional; y

c) Revisar los planes de tratamiento propuestos por la unidad especializada de riesgo operacional, de acuerdo con el nivel de prioridad determinado.

Párrafo. Las decisiones acordadas en el Comité de Riesgo Operacional deberán ser conocidas y ponderadas por el Comité de Gestión Integral de Riesgos.

Artículo 26. Responsabilidad de la Alta Gerencia en la Gestión del Riesgo Operacional. La Alta Gerencia, a través del modelo de gestión de las 3 líneas de defensa, deberá definir una estructura de gobierno clara, efectiva y sólida, con responsabilidades bien determinadas, transparentes y consistentes, la cual deberá contar con la aprobación del Consejo. En adición a las responsabilidades definidas en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos, la Alta Gerencia tendrá, sin que las mismas sean limitativas, las funciones siguientes:

a) Implementar y mantener, de forma consistente en toda la organización, políticas, procesos y sistemas para administrar el riesgo operacional en todos los productos, actividades, procesos y sistemas de la entidad, de acuerdo con la declaración de tolerancia y apetito de riesgo;

b) Establecer y mantener mecanismos sólidos de revisión y procesos efectivos de resolución de problemas, mediante sistemas que permitan informar, rastrear y, cuando sea necesario, escalar problemas para garantizar su resolución;

c) Establecer las relaciones de autoridad, responsabilidad y presentación de informes de rendición de cuentas, solicitando los recursos necesarios para gestionar el riesgo operacional de acuerdo con el apetito, tolerancia y capacidad de riesgo;

d) Verificar que la gestión del riesgo operacional cuente con un proceso adecuado para la supervisión de los riesgos de las actividades de las unidades de negocio;

e) Respaldar que las actividades de la entidad sean realizadas por el personal con la experiencia y las capacidades técnicas necesarias, y que cuente con el acceso a los recursos requeridos para desempeñar sus funciones de forma adecuada;

f) Coordinar que el personal responsable de supervisar y hacer cumplir las políticas de riesgo de la entidad, cuente con autoridad e independencia de las unidades que supervisan; y,

g) Proporcionar al Consejo los reportes oportunos sobre la resiliencia operativa de las unidades de negocio de la entidad, particularmente cuando se presenten deficiencias importantes que pudieran afectar la entrega de operaciones críticas.

Artículo 27. Responsabilidad de la Unidad de Gestión Integral de Riesgos. Las responsabilidades y funciones de la Unidad de Gestión Integral de Riesgos serán aquellas definidas en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos.

Artículo 28. Responsabilidad de la Unidad Especializada de Riesgo Operacional. El personal asignado a la unidad especializada para la gestión de riesgo operacional será responsable de proporcionar una evaluación efectiva, objetiva, oportuna e independiente

…/

respecto a la calidad y la suficiencia de las actividades de gestión de riesgo operacional por parte de las unidades de negocio, la cual deberá ser aplicada a través de las diversas herramientas de gestión, así como estar debidamente documentada. También tendrá la responsabilidad de vigilar que las unidades de negocio estén ejecutando correctamente las estrategias, políticas, procesos y procedimientos de gestión de dichos riesgos, así como proporcionar recomendaciones sobre medidas correctivas. En adición a las responsabilidades definidas en el Reglamento sobre Lineamientos para la Gestión Integral de Riesgos, la unidad especializada de riesgo operacional tendrá, sin que las mismas sean limitativas, las funciones siguientes:

a) Proponer políticas para la gestión del riesgo operacional y la actualización de los manuales para la gestión de dicho riesgo;

b) Desarrollar e implementar el uso de herramientas apropiadas de gestión de riesgo operacional, incluyendo la base de datos de eventos, las matrices de riesgos, entre otros;

c) Desarrollar y mantener políticas, estándares y directrices de gestión y medición de riesgo operacional;

d) Elaborar y mantener actualizado el reporte del perfil de riesgo operacional;

e) Identificar, diseñar y brindar la capacitación y concientización requerida sobre el riesgo operacional;

f) Verificar que existen procesos y procedimientos para proporcionar una supervisión adecuada de las prácticas de gestión de riesgo operacional;

g) Verificar que los procesos de medición del riesgo operacional se integran adecuadamente en la gestión integral del riesgo;

h) Apoyar en la evaluación del riesgo operacional de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o tecnológico;

i) Desarrollar una visión independiente de las unidades de negocio respecto a los riesgos operacionales materiales identificados, el diseño y eficiencia de sus controles y la tolerancia al riesgo;

j) Consolidar y desarrollar los reportes e informes sobre la gestión del riesgo operacional;

k) Mantener una comunicación efectiva con el personal responsable de gestionar el riesgo de crédito, de mercado y otros riesgos, así como con aquéllos que en la entidad son responsables de la adquisición de servicios externos;

l) Promover una adecuada cultura de gestión del riesgo operacional en toda la entidad;

m) Verificar dentro de la entidad la escalada oportuna y precisa de los problemas materiales;

n) Reportar periódicamente y cuando la situación lo amerite a la unidad de gestión integral de riesgos sobre la exposición al riesgo operacional, los cambios sustanciales de tal exposición, el cumplimiento de los niveles de apetito, tolerancia y capacidad; y las actividades relevantes para su mitigación y adecuada administración;

o) Proponer las medidas correctivas cuando se detecten deficiencias en la gestión del riesgo operacional, debiendo mantener registros sobre el nivel de cumplimiento y las medidas adoptadas; y,

p) Utilizar herramientas de análisis de eventos de riesgo operacional ya materializados, para identificar factores y tendencias que permitan mejorar la prevención.

Párrafo. Los responsables de la gestión del riesgo operacional deben contar con las capacidades y habilidades necesarias para desempeñar sus funciones de manera efectiva.

Artículo 29. Responsabilidad de las Unidades de Negocio. Las entidades deberán incluir dentro de las funciones y responsabilidades que corresponden a la primera línea de defensa, las siguientes:

a) Identificar, analizar y valorar los riesgos operacionales inherentes a sus respectivas unidades de negocio, mediante el uso de herramientas de gestión de riesgos;

b) Definir, junto con la unidad especializada de riesgo operacional, los indicadores de riesgo operacional para el monitoreo de los riesgos aplicables a sus procesos y reportar a dicha unidad la información de estos indicadores de manera oportuna;

c) Participar en la definición y establecimiento de controles apropiados para mitigar los riesgos operacionales inherentes, así como evaluar el diseño y su efectividad;

d) Escalar las necesidades de recursos, herramientas y capacitación que tengan las unidades de negocio para garantizar la identificación y evaluación de riesgos operacionales;

e) Monitorear y reportar a la unidad especializada de riesgo operacional, los perfiles de riesgo operacional de sus unidades de negocio y asegurar su adhesión al apetito de riesgo y la declaración de tolerancia y capacidad de riesgo establecidos;

f) Informar riesgos operacionales residuales no mitigados por los controles, incluyendo las deficiencias de control, deficiencias de procesos y el incumplimiento de las tolerancias de riesgos operacionales;

g) Promover una adecuada cultura de gestión del riesgo operacional, apegándose siempre al marco de gestión y a las políticas establecidas; y,

h) Escalar de manera precisa y oportuna los eventos de riesgo operacional identificados en su unidad de negocio.

…/

Artículo 30. Responsabilidad de la Unidad de Auditoría Interna. La unidad de auditoría interna deberá verificar la correcta implementación del marco de gestión de riesgo operacional, así como su efectividad y el cumplimiento de las políticas y procedimientos aprobados por el Consejo para su ejecución. Esta unidad tendrá, sin que las mismas sean limitativas, las funciones siguientes:

a) Revisar el diseño y la implementación de los sistemas de gestión de riesgos operacionales y los procesos de gobernanza asociados a la primera y segunda línea de defensa, incluida la independencia de esta última;

b) Revisar los procesos de validación para garantizar que sean independientes y se implementen de manera coherente con las políticas establecidas por la entidad;

c) Revisar que los sistemas de cuantificación utilizados por la entidad sean lo suficientemente sólidos como para brindar seguridad de la integridad de los insumos, supuestos, procesos y metodologías, así como dar lugar a evaluaciones del riesgo operacional que reflejen de manera creíble el perfil de riesgo operativo;

d) Revisar que la gerencia de las unidades de negocio responda de manera oportuna, precisa y adecuada a los problemas planteados, e informe periódicamente al Consejo o sus comités relevantes, sobre asuntos pendientes y cerrados;

e) Opinar sobre la adecuación general del marco de gestión y los procesos de gobierno asociados en toda la entidad; debiendo verificar el cumplimiento de las políticas y procedimientos aprobados por el Consejo, así como también evaluar si el marco cumple con las necesidades y expectativas de la entidad (tales como el respeto del apetito, la tolerancia y la capacidad de riesgo, y el ajuste del marco a las circunstancias operativas cambiantes) y con la normativa vigente, acuerdos contractuales, normas internas y conducta ética;

f) Verificar el diseño y efectividad operativa de los controles para determinar su capacidad para mitigar los riesgos; y,

g) Comunicar a la Unidad Especializada de Riesgo Operacional los resultados de las evaluaciones de controles, observaciones y hallazgos relacionados con la gestión del riesgo operacional, incluyendo las incidencias, los eventos y la identificación de nuevos riesgos.

TÍTULO IV
DEL AMBIENTE DE GESTIÓN DEL RIESGO OPERACIONAL

CAPÍTULO I
IDENTIFICACIÓN Y EVALUACIÓN DEL RIESGO

Artículo 31. Identificación y Evaluación del Riesgo. Las entidades deberán garantizar la identificación y evaluación integral de los riesgos de todos los productos, actividades, procesos y sistemas, asegurándose de que estos sean de fácil comprensión e incorporando los resultados

…/

de la evaluación del riesgo en el proceso general de desarrollo de la estrategia del negocio de la entidad.

Artículo 32. Herramientas de Gestión del Riesgo Operacional. Las entidades deberán diseñar y monitorear indicadores de riesgo operacional que estén relacionados con los riesgos relevantes identificados para las iniciativas estratégicas o clave, mediante la matriz de riesgos y la base de datos de eventos de riesgos materializados. Asimismo, deberán contar con herramientas eficientes para la correcta identificación y evaluación del riesgo operacional, entre estas se incluyen las siguientes:

a) Mapeo de procesos;

b) Base de datos de registro de eventos de riesgo operacional;

c) Taxonomía o clasificación de tipos de riesgo operacional;

d) Inventario de controles;

e) Evaluaciones de riesgos y controles;

f) Matriz de riesgos operacionales;

g) Mapa de calor de riesgos;

h) Indicadores de riesgos;

i) Análisis de escenarios de posibles fuentes de riesgos, como parte de los insumos para las pruebas de estrés; y,

j) Análisis comparativo de resultados de distintas herramientas.

Párrafo I. Como resultado del mapeo de procesos, la definición de la taxonomía de riesgos, el inventario de controles y las evaluaciones de estos, se deberá elaborar una matriz dinámica donde se registren, de manera detallada, todos los riesgos operacionales de los procesos, incluyendo los riesgos de procesos de tercerización de servicios, que permita visualizar los resultados de la identificación, medición, evaluación y mitigación de estos.

Párrafo II. Los resultados de esta matriz permitirán verificar la evolución del perfil de riesgo de un período a otro a través del mapa de calor de estos, con la finalidad de que la entidad pueda monitorear su perfil de riesgo, priorizar los riesgos identificados, así como desarrollar planes de acción sobre el tratamiento de los riesgos con niveles de exposición fuera del apetito definido por la entidad.

Artículo 33. Reporte de Matriz de Riesgos. Las entidades deberán remitir a la Superintendencia de Bancos y al Banco Central las situaciones de riesgo que puedan afectar a las personas o el negocio de la entidad a través de la matriz de riesgos, cumpliendo con la

periodicidad y plazos establecidos en el Manual de Requerimientos de Información de la Administración Monetaria y Financiera.

Artículo 34. Idoneidad de las Herramientas de Evaluación. Las entidades deberán garantizar que los resultados de las herramientas de evaluación del riesgo operacional estén basados en datos verificados y validados, que consideren los mecanismos internos de medición de desempeño y se sujeten a los planes de acción monitoreados por la Unidad Especializada de Riesgo Operacional, cuando sea necesario.

Artículo 35. Marco de Gestión del Cambio. Las entidades deberán contar con políticas y procedimientos para la evaluación y aprobación de nuevos productos, servicios, actividades, procesos, canales y sistemas, así como para la identificación, administración, revisión, aprobación y monitoreo del cambio. La Alta Gerencia deberá garantizar que el proceso de gestión de cambios de la entidad cuente con los recursos adecuados entre las líneas de defensa, para lo cual deberá evaluar la evolución de los riesgos asociados desde el inicio hasta la finalización de los cambios y monitorear la implementación de estos con controles de supervisión específicos. Asimismo, se deberán establecer, de acuerdo con el modelo de las 3 líneas de defensa, las funciones siguientes:

a) La primera línea de defensa debe realizar evaluaciones del riesgo operacional y control de nuevos productos, servicios, actividades, procesos, canales y sistemas, o cambios en el ambiente operativo o tecnológico, desde las fases de toma de decisiones y planificación, hasta la implementación y revisión posterior; y,

b) La segunda línea de defensa debe revisar los riesgos identificados y los controles definidos por la primera línea, así como las evaluaciones de estos, monitoreando que su implementación sea apropiada y cubra todas las fases de este proceso. Adicionalmente, podrá recomendar ajustes a dicha evaluación y deberá presentar al Comité de Gestión Integral de Riesgos los resultados.

Artículo 36. Registro de Productos y Servicios. Las entidades deberán mantener un registro central de sus productos y servicios, incluidos los subcontratados, con la finalidad de facilitar el seguimiento de los cambios.

CAPÍTULO II
MONITOREO E INFORMES

Artículo 37. Sistema de Información. Las entidades deberán disponer de mecanismos adecuados y eficaces para vigilar, recopilar y analizar datos sobre el riesgo operacional. Dichos mecanismos deberán contar con un esquema organizado de información que contenga, al menos, lo siguiente:

a) Informe de riesgo operacional, en el cual se detalle el nivel de riesgo al que se enfrenta la entidad, así como la revisión de los resultados de los planes de acción, las estrategias establecidas y el monitoreo de los indicadores de riesgo;

b) Informe detallado de los eventos de riesgo operacional que hayan afectado a la entidad;

…/

c) Matriz de los riesgos identificados, que permita evaluar el nivel de exposición, así como establecer las medidas para mitigar el impacto que estos puedan causar en caso de materializarse;

d) Informe de evaluación de riesgos ante nuevas iniciativas (productos, procesos, infraestructura, servicios, canales, sistemas, entre otras); y,

e) Informe de evaluación de la función de auditoría interna sobre el diseño y efectividad del marco y proceso de gestión del riesgo operacional en la entidad.

Párrafo. Los informes deben ser dirigidos a las áreas correspondientes de la entidad, de manera que puedan ser analizados con una perspectiva de mejora continua del desempeño en la gestión del riesgo operacional y establecer o modificar políticas, procesos y procedimientos.

Artículo 38. Calidad de los Informes. Las entidades deberán asegurarse de que sus informes sean completos, precisos, consistentes y procesables en todas las unidades de negocio y productos; y que estén acordes con su perfil, apetito, tolerancia y capacidad de riesgo operacional.

Artículo 39. Presentación Interna de Informes. Los informes deben ser presentados de manera oportuna a la Alta Gerencia y al Consejo, debiendo ser elaborados en condiciones de mercado normales y estresados, e incluyendo los resultados de las actividades de monitoreo en los informes regulares, las evaluaciones de la gestión del marco realizadas por las áreas de auditoría interna, externa y/o gestión de riesgos, así como los generados por o para las autoridades de supervisión, cuando corresponda. Asimismo, la frecuencia de estos deberá reflejar los riesgos involucrados, el ritmo y la naturaleza de los cambios en el entorno operativo.
Párrafo. La primera línea de defensa debe informar a la segunda línea sobre los riesgos operacionales identificados durante el desarrollo de sus funciones, así como los eventos de riesgo operacional, las deficiencias de control y del proceso y el incumplimiento de las tolerancias de riesgo operacional de acuerdo con el nivel de prioridad determinado.

Artículo 40. Revisión de los Procesos de Captura de Datos. Los procesos de captura de datos para la realización de los informes de riesgos deberán analizarse periódicamente por parte de la unidad especializada de riesgo operacional, con el objetivo de mejorar el rendimiento de la gestión de riesgos, así como avanzar en las políticas, procedimientos y prácticas de gestión de riesgos.

CAPÍTULO III
CONTROL DEL RIESGO

Artículo 41. Sistemas de Control Interno. Las entidades deberán contar con sistemas de control interno adecuados que utilicen políticas, procesos, procedimientos y niveles de control formalmente establecidos, revisados, monitoreados y probados periódicamente para asegurar su efectividad, así como con estrategias apropiadas de tratamiento de riesgos. Estos controles deben formar parte integral de las actividades regulares de la entidad, de manera que permitan detectar,

prevenir o generar respuestas oportunas ante los eventos de riesgo operacional y las fallas o insuficiencias que los originan, o sean complementados por transferencia del riesgo a un tercero.

Artículo 42. Procesos y Procedimientos de Control. Los procesos y procedimientos de control deben incluir un sistema para garantizar el cumplimiento de las políticas, regulaciones y leyes, debiendo considerarse para la evaluación de su cumplimiento, la inclusión, de manera enunciativa más no limitativa, de los elementos siguientes:

a) Revisiones del progreso hacia los objetivos establecidos;

b) Verificación del cumplimiento de los controles de gestión;

c) Revisión del tratamiento y resolución de instancias de incumplimiento;

d) Evaluación de las aprobaciones y autorizaciones requeridas para garantizar la rendición de cuentas a un nivel adecuado de gestión; y,

e) Informes de seguimiento de excepciones aprobadas a umbrales o límites, anulaciones de gestión y otras desviaciones de políticas, regulaciones y leyes.

Artículo 43. Controles Internos Efectivos. Las entidades deberán mantener una estrategia adecuada de segregación de tareas, controles duales, así como medidas para la identificación, reducción, monitoreo y revisión independiente de las áreas donde puedan surgir conflictos de interés. Los controles mínimos que se deberán considerar, de manera enunciativa más no limitativa, son los siguientes:

a) Establecer autoridades y/o procesos de aprobación claros;

b) Monitoreo constante de la adherencia a los umbrales o límites de riesgo asignados;

c) Nivel adecuado de personal y capacitación para mantener la experiencia técnica;

d) Verificación y conciliación periódica de transacciones y cuentas; y,

e) Política de vacaciones, contemplando la delegación de funciones sobre personal calificado.

Artículo 44. Transferencia del Riesgo. Una vez que las entidades determinen la necesidad de complementar los controles de la transferencia del riesgo a través de seguros o servicios tercerizados, el Consejo deberá evaluar la exposición máxima a pérdidas que la entidad está dispuesta y tiene la capacidad financiera para asumir, y realizar de manera periódica la verificación de los mitigantes implementados para los riesgos transferidos, considerando los requisitos reglamentarios.

CAPÍTULO IV
GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

Artículo 45. Plan de Continuidad de Negocio. Las entidades deberán implementar planes de continuidad de negocio intensivos y de calidad, considerando sus correspondientes medidas de contingencia, a fin de garantizar su capacidad para operar sin interrupciones y con pérdidas mínimas ante incidentes disruptivos.

Párrafo. Para garantizar la continuidad de las operaciones tecnológicas ante incidentes de seguridad de la información, en adición se deberán considerar los aspectos especificados en el Reglamento de Seguridad Cibernética y de la Información.

Artículo 46. Preparación del Plan de Continuidad de Negocio. Las entidades deberán preparar un plan de continuidad de negocio considerando la evaluación de escenarios de posibles interrupciones, el análisis de impacto ante incidentes disruptivos, así como procedimientos de recuperación. Asimismo, se deberán considerar, como mínimo, los aspectos siguientes:

a) Identificación y clasificación de las operaciones críticas y las dependencias internas o externas clave, cubriendo todas las unidades de negocio, así como los proveedores críticos y los principales terceros;

b) Cada escenario debe estar sujeto a una evaluación de impacto cuantitativa y cualitativa, considerando sus consecuencias financieras, operativas, legales y de reputación; y,

c) Cada escenario de interrupción debe estar sujeto a umbrales o límites para la activación de un procedimiento de continuidad, el cual deberá considerar aspectos de reanudación, establecimiento de tiempo máximo tolerable de inactividad, objetivos de tiempo de recuperación, objetivos de punto de recuperación, estrategias de recuperación y programas de prueba, así como pautas de comunicación para informar a la gerencia, empleados, autoridades reguladoras y supervisoras, clientes, proveedores y, cuando corresponda, autoridades civiles.

Artículo 47. Medidas de Contingencia. Las entidades deberán gestionar las contingencias para prevenir la interrupción de sus operaciones y tener formalmente implementadas las estrategias para el oportuno restablecimiento de estas ante la ocurrencia de eventos que afecten los procesos de negocio o de apoyo considerados críticos, para minimizar su impacto sobre el negocio de la entidad.

Artículo 48. Políticas de Gestión de Continuidad. Una política efectiva de gestión de continuidad debe considerar los aspectos siguientes:

a) Aprobación y revisión periódica por parte del Consejo;

b) Participación de la Alta Gerencia y los líderes de las unidades de negocio en su implementación;

c) Compromiso de la primera y segunda línea de defensa con su diseño; y

…/

d) Revisión periódica por la tercera línea de defensa.

Artículo 49. Revisión de Políticas de Continuidad. Las entidades deberán revisar periódicamente sus políticas de continuidad para garantizar que permanezcan consistentes con las operaciones, riesgos y amenazas actuales, debiendo probarse frecuentemente los procedimientos para asegurar el cumplimiento de los objetivos y los plazos de recuperación y reanudación. Asimismo, se deberán personalizar los programas de capacitación y sensibilización, en función de los roles para que el personal pueda ejecutar con eficacia el plan de continuidad.

Párrafo. Las entidades deberán realizar y evaluar las pruebas de continuidad de negocio con sus proveedores de servicios clave, debiendo informar de los resultados de estas al Consejo y a la Alta Gerencia y manteniendo registros del detalle y los resultados de estas pruebas.

Artículo 50. Delimitación de Funciones para la Gestión de Interrupciones. Los planes de continuidad de negocio deben contener las funciones y responsabilidades para la gestión de interrupciones y proporcionar una guía clara con respecto a la sucesión de autoridad, en caso de una interrupción que afecte al personal clave. Además, deben establecer claramente el procedimiento interno que se deberá implementar durante y después de la ocurrencia del incidente, así como definir los detonantes para activar el plan de continuidad de negocio.

CAPÍTULO V
GESTIÓN DE SERVICIOS TERCERIZADOS

Artículo 51. Gestión de la Tercerización. Las entidades deberán establecer políticas y procesos adecuados para evaluar, gestionar y vigilar las actividades tercerizadas en cumplimiento con el Instructivo sobre Tercerización o Subcontratación de Servicios (outsourcing) vigente.

Párrafo I. Las entidades deberán documentar y gestionar, de manera eficaz, un inventario de los servicios y procesos tercerizados, incluyendo información suficiente para identificar su proveedor, lo tercerizado y su relación con otros servicios, productos, canales, procesos o sistemas.

Párrafo II. Los contratos o acuerdos de prestación de servicios deberán delimitar claramente las responsabilidades entre la empresa subcontratada y la entidad.

Párrafo III. Las entidades desarrollarán e implementarán mecanismos efectivos para la administración continua y adecuada de todos los riesgos inherentes a la cadena de suministro de la tercerización de la actividad o proceso.

Artículo 52. Auditoría y Contingencia de la Tercerización. Las entidades que contraten proveedores de servicios deberán incluir cláusulas contractuales que indiquen que el proveedor le garantizará a la entidad las pistas de auditoría necesarias, de forma que existan pruebas para cualquier acción legal, las cuales deben estar disponibles por el tiempo que exija la normativa vigente. Además, deben requerir informes de terceros independientes de, por lo menos, los componentes que permiten la entrega de lo contratado por la entidad, incluyendo resultados de las pruebas de efectividad, de los controles relacionados, políticas de contingencias y plan de

…/

continuidad de negocio, que certifiquen un ambiente adecuado de los controles en organizaciones de servicio.

Artículo 53. Acuerdos Intragrupo. Las entidades deberán realizar una evaluación de riesgos y debida diligencia antes de celebrar acuerdos de servicios con entidades o empresas que pertenezcan al mismo grupo financiero al que pertenece la entidad, considerando con anticipación si estos cuentan con un adecuado nivel de resiliencia operativa para salvaguardar las operaciones críticas de la entidad tanto en condiciones normales, como en caso de interrupción. Estos acuerdos deben ser evaluados para determinar si clasifican como tercerización de actividad, función o servicios de acuerdo con los criterios definidos en el Instructivo sobre Tercerización o Subcontratación de Servicios (outsourcing).

Artículo 54. Resiliencia Operativa en Interrupción o Fallas por parte de un Tercero. Las entidades deberán desarrollar estrategias adecuadas para mantener su resiliencia operativa en caso de falla o interrupción por parte de un tercero, que pueda afectar las operaciones críticas, evaluando alternativas viables que puedan facilitar su sustitución.

CAPÍTULO VI
EVENTOS DE RIESGO OPERACIONAL

Artículo 55. Gestión de los Eventos de Riesgo Operacional. Las entidades deberán contar con procedimientos y procesos adecuados y debidamente documentados para identificar, recopilar y tratar correctamente los datos internos sobre eventos de riesgo operacional. Dichos procesos deberán estar sujetos a validación, así como a revisiones independientes periódicas de las unidades de auditoría interna o externa.

Párrafo. Como parte de la gestión de eventos de riesgo operacional, la entidad deberá realizar evaluaciones retrospectivas sobre los riesgos relacionados, con la finalidad de verificar que hayan sido registrados en la matriz de riesgo operacional. En adición, se deberá verificar la coherencia de la evaluación de los riesgos al considerar la probabilidad e impacto de su materialización, así como para valorar el análisis costo-beneficio, en caso de que aplique, de ejecutar los planes de acción para su tratamiento.

Artículo 56. Documentación de los Eventos de Riesgo Operacional. Las entidades deberán mantener informaciones suficientes, actualizadas y disponibles sobre los eventos de riesgo operacional materializados, así como las pérdidas económicas o no económicas incurridas como consecuencia de estos. Asimismo, deberán diseñar las políticas, procedimientos de captura y entrenamiento del personal que interviene en el proceso de gestión de los eventos de riesgo operacional originados en toda la entidad.

Artículo 57. Contabilización de las Pérdidas. Para el registro de los eventos de riesgo operacional, las entidades deberán contabilizar tanto las pérdidas brutas como la recuperación de estas.

Artículo 58. Estimación de las pérdidas no económicas. Considerando que las pérdidas no económicas no son pasibles de contabilización, las entidades deberán estimar el efecto negativo

…/

generado como consecuencia del evento, como son la pérdida de clientes, la pérdida de eficiencia, entre otros, siempre que dichos efectos puedan ser razonablemente estimados, para fines de monitoreo, mitigación y control.

Artículo 59. Revisión Independiente de la Integridad de los Datos. Las entidades deberán contar con procesos para revisar de forma independiente la integridad y precisión de los datos sobre pérdidas.

Artículo 60. Base de Datos de Eventos. Las entidades deberán tener una base de datos con las informaciones relevantes de los eventos de riesgo operacional, con pérdidas económicas y no económicas, incluyendo los datos suficientes para su identificación, clasificación, seguimiento y análisis. Esta base de datos deberá clasificar los eventos por tipo, de acuerdo con la taxonomía especificada en el Manual de Requerimientos de Información de la Administración Monetaria y Financiera.

Párrafo. Con el objeto de elaborar indicadores y evaluar riesgos, la entidad deberá mantener de forma separada los registros de los eventos con pérdidas no materializadas. Estos registros incluirán, entre otros, aquellos eventos cuyo impacto fue mitigado por controles internos de la entidad.

Artículo 61. Reporte de Eventos de Riesgo Operacional. Las entidades deberán remitir a la Superintendencia de Bancos los eventos de riesgo operacional que impacten a la entidad con pérdidas económicas o no económicas y cumplan con los criterios para ser reportados de forma individual o agrupada, cumpliendo con la periodicidad y plazos establecidos en el Manual de Requerimientos de Información de la Administración Monetaria y Financiera.

CAPÍTULO VII
DIVULGACIÓN DE INFORMACIÓN

Artículo 62. Política de Divulgación. Las entidades deberán tener una política de divulgación formal que esté sujeta a una revisión periódica e independiente, así como la aprobación del Consejo, previa revisión de la Alta Gerencia. La política deberá abordar el enfoque adoptado por la entidad para determinar las informaciones relativas al riesgo operacional que divulgará y los controles internos requeridos para dicho proceso de divulgación. Asimismo, deberán implementar un proceso para evaluar la idoneidad de sus divulgaciones, así como de la referida política.

Párrafo. Las entidades deberán divulgar su marco de gestión que permita a las partes interesadas conocer cómo identifica, evalúa, monitorea y controla o mitiga, en forma eficiente, sus riesgos operacionales.

TÍTULO V
FACTORES DE RIESGO OPERACIONAL

CAPÍTULO I
GENERALIDADES

Artículo 63. Factores de Riesgo Operacional. Los factores a los que se ven expuestas las entidades son: procesos internos, personas, eventos externos y tecnología de información. Para un efectivo control de dichos factores, es determinante que las entidades cuenten con una definición apropiada de cada uno de estos.

Artículo 64. Clasificación de los Eventos de Riesgo Operacional. Las entidades deberán identificar por unidad de negocio, producto o proceso, los eventos de riesgo operacional, agrupados por tipo de fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos, tales como los siguientes:

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) Incidencias en el negocio y fallos en los sistemas; y,

g) Fallas en la ejecución, entrega o gestión de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Artículo 65. Identificación de los Eventos de Riesgo Operacional. Una vez identificados los posibles eventos de riesgo operacional, las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la entidad, la Alta Gerencia podrá decidir si el riesgo se debe asumir, evitar, mitigar o transferir, reduciendo sus consecuencias y efectos, en base al apetito y tolerancia al riesgo definidos por el Consejo. La identificación de los eventos de riesgo operacional permitirá al Consejo contar con una visión clara de la importancia relativa de los diferentes tipos de exposiciones al riesgo operacional y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones a ser ejecutadas por la Alta Gerencia, como son, entre otras, las siguientes:

a) Revisar estrategias y políticas;

b) Actualizar o modificar procesos y procedimientos establecidos;

c) Establecer o modificar límites de riesgo;

…/

d) Constituir, incrementar o modificar controles;

e) Implantar medidas de contingencias y planes de continuidad de negocio;

f) Revisar términos de pólizas de seguro contratadas; y,

g) Contratar servicios provistos por terceros u otros, según corresponda.

CAPÍTULO II
PROCESOS INTERNOS

Artículo 66. Gestión de Riesgos de Procesos Internos. La gestión de los riesgos asociados a los procesos internos que se implemente en las entidades deberá definirse de conformidad con la estrategia y las políticas adoptadas, de manera que permita minimizar la posibilidad de pérdidas económicas y no económicas relacionadas con el diseño inapropiado de los procesos críticos; o a políticas y procedimientos inadecuados o inexistentes. Esta gestión deberá considerar los riesgos asociados a las fallas en los modelos utilizados, el incumplimiento normativo, contractual o extracontractual, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable y de negocio, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados, entre otros.

Artículo 67. Políticas y Procedimientos de Procesos. Las entidades deberán contar con políticas y procedimientos escritos relativos al diseño, control, actualización, evaluación y seguimiento de los procesos. Dichas políticas y procedimientos se referirán, por lo menos, a los aspectos siguientes:

a) Diseño de los procesos, los cuales deben ser adaptables;

b) Descripción en secuencia lógica y ordenada de las actividades, tareas y controles;

c) Identificación de las personas responsables de ejecutar los procesos para su correcto funcionamiento, a través de establecer medidas y fijar objetivos, garantizando que las metas globales del proceso se cumplan; definir los límites y alcance; mantener contacto con los clientes internos y externos del proceso para asegurar que se satisfagan y conozcan sus expectativas, entre otros;

d) Difusión y comunicación de los procesos; y,

e) Actualización continua producto de la evaluación e identificación de oportunidades de mejora de los procesos.

Artículo 68. Segregación de Funciones. Las entidades deberán tener una adecuada separación de funciones que eviten incompatibilidades, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona o estructura, podría eventualmente permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operacional.

…/

Artículo 69. Inventarios de Procesos. Las entidades deberán mantener inventarios actualizados de los procesos en funcionamiento, los cuales contarán como mínimo con la información siguiente: tipo y nombre del proceso, descripción general, responsable, productos y servicios que genera el proceso, proveedores y clientes internos y externos, fecha de aprobación, fecha de actualización; además, deberá indicar si se trata de un proceso crítico.

CAPÍTULO III
DEL CAPITAL HUMANO

Artículo 70. Gestión de Riesgos de Capital Humano. Las entidades deberán definir formalmente procesos, políticas y procedimientos que aseguren una adecuada planificación y administración del capital humano. Estas deberán considerar los procesos de incorporación, permanencia y desvinculación del personal al servicio de la entidad, así como la devolución de recursos asignados. Además, las normas internas deberán identificar apropiadamente las fallas o insuficiencias asociadas al personal, incluyendo los conflictos de intereses derivados de sus funciones, de tal modo que se minimice la posibilidad de pérdidas económicas y no económicas originadas por una inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información, lavado de activos y similares.

Artículo 71. Adecuadas Competencias para el Desempeño de Funciones. Las entidades deberán evaluar su organización, con el objeto de determinar si se han definido las necesidades de recursos humanos con las competencias idóneas para el desempeño de cada puesto, considerando la experiencia profesional, formación académica, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia de la entidad.

Artículo 72. Actualización de Información de Recursos Humanos. Las entidades mantendrán información actualizada de los recursos humanos, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse a lo siguiente:

a) Personal existente en la entidad;

b) Formación académica y experiencia;

c) Forma y fechas de selección, reclutamiento y contratación;

d) Información histórica sobre los eventos de capacitación en los que han participado;

e) Cargos que han desempeñado en la entidad;

f) Resultados de evaluaciones realizadas;

g) Fechas y causas de separación del personal que se ha desvinculado; y,

h) Otras informaciones que se consideren pertinentes.

…/

CAPÍTULO IV
EVENTOS EXTERNOS

Artículo 73. Gestión de Eventos Externos. La gestión del riesgo operacional también debe considerar la posibilidad de pérdidas ocasionadas por la ocurrencia de eventos ajenos al control de la entidad, que pudiesen alterar el desarrollo de sus operaciones y tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, emergencias sanitarias, atentados y otros actos delictivos, así como las fallas en servicios provistos por terceros.

CAPÍTULO V
TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN (TSI)

SECCIÓN I
MARCO DE GESTIÓN DE RIESGOS DE LA TSI

Artículo 74. Gestión de Riesgos Tecnológicos. Las entidades deberán implementar una gestión de riesgo tecnológico que procure un adecuado desempeño de sus procesos de negocio, administrativos, de control y de cumplimiento, dentro de los umbrales de su apetito, tolerancia y capacidad de riesgo. La gestión del riesgo tecnológico debe estar alineada con el marco de gestión del riesgo operacional y las disposiciones de gestión de riesgo establecidas en el Reglamento de Seguridad Cibernética y de la Información.

Párrafo I. Es responsabilidad del Consejo aprobar las metodologías de gestión de riesgo tecnológico que adopte la entidad y revisar periódicamente la efectividad de estas. La Alta Gerencia debe evaluar de forma rutinaria el diseño y la efectividad operativa de la gestión de riesgo tecnológico, validando, además, que se enmarca en el apetito de riesgo y la declaración de tolerancia de la entidad, así como de la normativa aplicable. Esto con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información.

Párrafo II. Cada entidad deberá coordinar con la unidad especializada de riesgos tecnológicos o en su defecto, de riesgo operacional, todos los aspectos relativos a definir, socializar, implementar y gestionar criterios para la identificación, estimación y evaluación de los riesgos tecnológicos. Esto incluye la consideración de las amenazas, vulnerabilidades, probabilidad e impacto. Esta coordinación deberá contar con la participación de los responsables de las áreas de tecnología y el oficial de seguridad cibernética y de la información.

Párrafo III. Los roles y responsabilidades relacionadas con la gestión de las tecnologías, así como de la gestión de la seguridad cibernética y de la información, deberán estar formalmente definidos y oportunamente comunicados a las partes interesadas. En adición, se mantendrán actualizados de acuerdo con el contexto de los procesos de la entidad.

Párrafo IV. La unidad especializada de riesgos tecnológicos o en su defecto de riesgo operacional, perteneciente a la segunda línea de defensa, deberá contar con las competencias y experiencias en la materia, a fin de monitorear continuamente los factores de riesgo tecnológico

…/

y comunicar oportuna y formalmente a la Alta Gerencia los resultados, así como ejecutar el adecuado seguimiento a los planes de acción.

Párrafo V. La unidad de auditoría interna deberá tener personal especializado con las competencias y experiencias para evaluar periódicamente, y basado en riesgo, el contexto de control en las áreas de tecnología, así como de seguridad cibernética y de la información.

Artículo 75. Controles de la Seguridad de la Información. Las entidades mantendrán actualizados y bajo evaluación periódica, controles técnicos, administrativos y físicos necesarios para mitigar los riesgos sobre los objetivos de la seguridad de la información en cualquiera de sus formatos y estados, de acuerdo con el programa de seguridad cibernética y de la información establecido en el Reglamento de Seguridad Cibernética y de la Información y su instructivo de aplicación.

Párrafo I. Para garantizar la disponibilidad de las informaciones y servicios tecnológicos utilizados por los procesos de apoyo considerados críticos, los misionales o de negocio y de las configuraciones de equipos y versiones de sistemas, cada entidad deberá tener implementados procedimientos de respaldos y retención, así como un plan para la recuperación de la funcionalidad de los procesos impactados por situaciones que afecten los componentes tecnológicos y/o la información del negocio y sus correspondientes contingencias.

Párrafo II. Cada entidad deberá implementar controles de seguridad física y protección ambiental para mitigar riesgos a la integridad de las informaciones y de los componentes tecnológicos. Esto incluye, sin limitarse, los servidores y las áreas que los albergan, equipos de telecomunicaciones, centrales telefónicas y otros componentes importantes para la ejecución de esos procesos. Lo anterior, considerando las políticas de contingencia de la entidad y como parte de su plan de continuidad de negocio.

Párrafo III. Las entidades deberán mantener controles y mecanismos de seguridad en sus sistemas de información y comunicación, para proteger la información de Identificación Personal (Personally Identifiable Information PII, por sus siglas en inglés) de sus colaboradores, clientes, usuarios y relacionados.

Párrafo IV. La gestión de la seguridad de la información, incluyendo los aspectos de ciberseguridad, deben estar asignada a personal con la adecuada experiencia y preparación. Este personal deberá tener la suficiente independencia jerárquica y funcional para realizar objetivamente las labores relacionadas a su cargo y en beneficio de la entidad.

Artículo 76. Gestión de Incidencias de la Tecnología y Seguridad de la Información. Las entidades mantendrán actualizados y bajo evaluación periódica, controles técnicos, administrativos y físicos necesarios para identificar, analizar, prevenir y mitigar los riesgos de las incidencias sobre los componentes tecnológicos y las informaciones del negocio.

Párrafo I. Las incidencias relacionadas con eventos de seguridad cibernética y de la información serán categorizadas y los componentes tecnológicos monitoreados para detectar, analizar y comunicar las que representen riesgo para la entidad. Estos incidentes deberán ser

gestionados de acuerdo con lo establecido en el Reglamento de Seguridad Cibernética y de la Información.

Párrafo II. Las entidades mantendrán planes de respuesta a incidentes de seguridad cibernética y de la información, incluyendo acciones de prevención, detección, notificación, aislamiento, remediación, restauración, recuperación, análisis y seguimiento.

Párrafo III. Las entidades mantendrán facilidades para la existencia de una base de información para el aprendizaje, a partir de las situaciones relacionadas a las incidencias.

Artículo 77. Rendición de Cuentas. Las entidades mantendrán registros o pistas de auditoría de las actividades realizadas en sus sistemas de información, bases de datos y componentes de seguridad de la información que, con datos suficientes, evidencien el intento o ejecución exitosa de una acción considerada como importante sobre las informaciones y servicios tecnológicos que utiliza la entidad. Dichos registros deberán estar disponibles para fines de auditoría y rendición de cuentas ante las instancias internas que determine la Alta Gerencia.

Párrafo. Entre las acciones consideradas como importantes sobre las informaciones, deberán incluirse, sin limitarse, aquellas que pueden modificar, eliminar o evitar su interpretación o uso, ya sea de manera autorizada o no.

SECCIÓN II
GOBERNANZA DE TECNOLOGÍA DE LA INFORMACIÓN (TI)

Artículo 78. Comité de Tecnología de la Información. La Alta Gerencia se asistirá de un comité de tecnología de la información para gestionar todo lo referente a las estrategias, inversión y cumplimiento y marco de gobernanza de TI adoptado por la entidad, sin que sea limitativo.

Artículo 79. Marco de Gobernanza de Tecnología de la Información. Las entidades deberán adoptar, previa aprobación del Consejo, un marco de gobernanza de TI, el cual proporcione a la Alta Gerencia un conjunto estructurado de principios, políticas y procesos, procurando la gestión de los riesgos tecnológicos, la optimización de recursos, la conformidad con regulaciones y estándares en la materia, así como mejorar la toma de decisiones y la entrega de valor a través del uso de las tecnologías.

Artículo 80. Gestión de Inversión en Tecnología y Seguridad de la Información. La aprobación de inversiones y proyectos relacionados a las tecnologías incluirá los correspondientes análisis de riesgo, los objetivos de control que pretenden mantener o implementar y, si aplica, su relación con la estrategia del negocio que apoyan.

TÍTULO VI
GESTIÓN DEL RIESGO LEGAL

Artículo 81. Políticas y Procedimientos para la Gestión del Riesgo Legal. La entidad deberá establecer políticas y procedimientos para la identificación, análisis, evaluación y mitigación de

situaciones que generen riesgos legales, considerando, sin que sea limitativo, los aspectos contractuales y regulatorios. En adición, estas políticas y procedimientos deberán considerar que, en forma previa y posterior a la celebración de actos jurídicos, se asegure la validez y ejecutoriedad de los acuerdos, debiendo vigilar en todo momento que sean observadas las formalidades de fondo y forma establecidas por las disposiciones de derecho común para su perfeccionamiento, en el entendido de que, ante la ocurrencia potencial de eventos de incumplimiento, la ejecución sea efectiva, sin costos importantes ni contratiempos.

Artículo 82. Provisión por Riesgo Legal. La entidad deberá estimar el monto potencial de pérdida esperada por litigios en procedimientos administrativos y procesos judiciales y arbitrales, y provisionar aquellos que se proyecten con resultado desfavorable. Estas provisiones deben ser actualizadas acorde con la evolución del litigio.

Artículo 83. Base de Datos de la Gestión de Riesgo Legal. La entidad deberá mantener una base de datos histórica sobre los procedimientos administrativos y procesos judiciales y arbitrales a los cuales se ha expuesto, sean estos originados por eventos de riesgo operacional o no, identificando sus causas, costos directos e indirectos, fechas de referencia, estatus y resultado, así como de las denuncias y demandas promovidas por la entidad, y las recibidas en contra de esta.

Párrafo. La unidad responsable de la función legal de la entidad deberá presentar al Comité de Gestión Integral de Riesgos, por lo menos trimestralmente, el estado de las acciones legales y administrativas en curso, así como un resumen de los resultados de los casos concluidos luego de la última presentación.

Artículo 84. Registro de las Contrataciones. Las entidades deberán llevar un registro de todas las contrataciones clasificadas por la materialidad, excluyendo las operaciones con clientes, que permita consultar y monitorear las obligaciones contraídas, por fechas de vencimiento o renovación, entre otros aspectos, facilitando el cumplimiento de los contratos. Este registro deberá estar a la disposición de la Superintendencia de Bancos a requerimiento.

TÍTULO VII
GESTIÓN DEL RIESGO OPERACIONAL DE LOS INTERMEDIARIOS CAMBIARIOS

Artículo 85. Política y Marco de Gestión. Los agentes de cambio y los agentes de remesas y cambio implementarán un marco de gestión del riesgo operacional, considerando su naturaleza, volumen y cantidad de operaciones, complejidad y su interconexión con otras entidades. A estos fines, en los instructivos de aplicación del presente Reglamento se establecerán las directrices para su gestión.

Artículo 86. Tecnología y Seguridad de la Información. Los intermediarios cambiarios deberán considerar la gestión del riesgo tecnológico y de seguridad de la información en su marco de gestión del riesgo operacional, tomando en cuenta el principio de proporcionalidad, y de conformidad con lo dispuesto en el Reglamento Cambiario en lo que respecta a las operaciones que estos realizan.

Párrafo. Respecto de su integración y operación a través del Sistema de Pagos de la República Dominicana (SIPARD) y de la Plataforma Cambiaria del Banco Central, los intermediarios cambiarios deberán cumplir los requisitos técnicos y de control que se establezcan mediante instructivos, realizar pruebas de integración y continuidad, y notificar de inmediato al Banco Central y a la Superintendencia de Bancos los incidentes que afecten la disponibilidad, integridad o confidencialidad de la información.

Artículo 87. Remisión de Información. Los intermediarios cambiarios deberán notificar de inmediato al Banco Central y a la Superintendencia de Bancos los incidentes operacionales graves, en los términos y umbrales que se definan mediante instructivo.

Artículo 88. Requerimiento de capital por riesgo operacional de los intermediarios cambiarios. Se establecerán requerimientos de capital por riesgo operacional para los intermediarios cambiarios, con el propósito de cubrir pérdidas inesperadas derivadas de este riesgo.

Párrafo. La metodología, parámetros y umbrales serán definidos mediante instructivos del Banco Central y la Superintendencia de Bancos, observando la proporcionalidad según la naturaleza, volumen y cantidad de operaciones, el grado de interconexión con entidades de intermediación financiera y las contrapartes con las cuales operan.

TÍTULO VIII
SUPERVISIÓN DEL RIESGO OPERACIONAL

Artículo 89. Supervisión de la Gestión del Riesgo Operacional. El ciclo de supervisión de las entidades que realiza la Superintendencia de Bancos, deberá incluir una revisión de la gestión del riesgo operacional de acuerdo con la metodología de evaluación establecida por dicha Superintendencia. Esta revisión podrá ser realizada con mayor o menor frecuencia dependiendo del resultado de la evaluación.

Párrafo I. Cuando las entidades formen parte de un grupo financiero, los supervisores deberán verificar que estas se aseguren de que existan procesos para gestionar el riesgo operacional de forma integrada en todo el grupo.

Párrafo II. La entidad que subcontrate una parte o la totalidad de su procesamiento de datos y otros servicios deberá incluir en los contratos que suscriba, una cláusula que permita a la Superintendencia de Bancos la revisión de los procesos tercerizados en el proveedor del servicio.

Párrafo III. La Superintendencia de Bancos podrá objetar la tercerización de procesos cuando la entidad no cumpla con la normativa vigente establecida por la Administración Monetaria y Financiera.

TÍTULO IX
SOLICITUD DE AUTORIZACIÓN, NO OBJECIÓN Y NOTIFICACIÓN

Artículo 90. Solicitud de Autorización, No Objeción y Notificación. Las entidades deberán solicitar la autorización, no objeción o notificación, según los requerimientos establecidos en el Manual de Solicitudes de Autorización, No Objeción y Notificaciones de las Entidades Supervisadas por la Superintendencia de Bancos y observando los lineamientos dispuestos en los instructivos de aplicación de este Reglamento.

TÍTULO X
REQUERIMIENTOS DE INFORMACIÓN

Artículo 91. Presentación de Informes y Reportes. Las entidades deberán presentar a la Superintendencia de Bancos y al Banco Central, a través del Portal de la Administración Monetaria y Financiera o de otras plataformas y medios comunicados por dichas Instituciones, los reportes e informes requeridos en el Manual de Requerimientos de Información de la Administración Monetaria y Financiera, con la periodicidad y en los plazos establecidos en dicho Manual.

Artículo 92. Solicitud de Información Adicional. La Superintendencia de Bancos y el Banco Central podrán requerir a las entidades cualquiera otra información que considere necesaria para una adecuada supervisión del riesgo operacional, en el ámbito de sus funciones.

Artículo 93. Disposición de Documentación. La entidad deberá tener a disposición de la Superintendencia de Bancos todos los documentos necesarios para la evaluación del riesgo operacional, así como la información de auditoría o revisiones realizadas por la casa matriz, cuando aplique.

Artículo 94. Notificación de Eventos Materiales de Riesgo Operacional. Las entidades deberán informar por escrito a la Superintendencia de Bancos todos los eventos que afecten o pongan en riesgo la continuidad de negocio, los recursos de la entidad o de los ahorrantes, la calidad de los servicios o la imagen de la entidad, conforme al plazo establecido en el Manual de Solicitudes de Autorización, No Objeción y Notificaciones de la Superintendencia de Bancos.

Párrafo. Las entidades deberán mantener informada a la Superintendencia de Bancos y al Banco Central sobre la situación en desarrollo y de las medidas o acciones de detección, respuesta y recuperación del incidente.

TÍTULO XI
DEL REQUERIMIENTO DE CAPITAL POR RIESGO OPERACIONAL

Artículo 95. Del Requerimiento de Capital. Se requerirán exigencias adicionales de patrimonio técnico en función de los riesgos operacionales asumidos por la entidad. La metodología para determinar el requerimiento de capital por riesgo operacional deberá

…/

considerar la naturaleza particular de este tipo de riesgo y los estándares internacionales generalmente aceptados en esta materia. La Superintendencia de Bancos y el Banco Central desarrollarán el instructivo de aplicación correspondiente.

Párrafo I. El requerimiento de capital por riesgo operacional se incorporará como un sumando adicional en el denominador del coeficiente de solvencia definido en el literal e) del artículo 46 de la Ley Monetaria y Financiera.

Párrafo II. Las entidades deberán remitir a la Superintendencia de Bancos y al Banco Central los resultados de la medición del riesgo operacional al que están expuestas, conforme a la metodología establecida, así como la documentación que sustente dichos resultados.

TÍTULO XII
DE LA SUPERVISIÓN Y LAS SANCIONES

Artículo 96. Grado de Supervisión. La gestión del riesgo operacional será considerada por la Superintendencia de Bancos en la determinación de la calificación de riesgo compuesto y del grado de supervisión que podrá requerir de la entidad, de conformidad con lo establecido en el Marco de Supervisión Basada en Riesgos.

Artículo 97. Sanciones. Las entidades que infrinjan las disposiciones contenidas en este Reglamento en cualquiera de sus aspectos serán pasibles de la aplicación de las sanciones establecidas en la Ley Monetaria y Financiera y el Reglamento de Sanciones vigente.

TÍTULO XIII
DISPOSICIONES TRANSITORIAS Y DEROGATORIAS

Artículo 98. Requerimiento de capital. Los requerimientos de capital por riesgo operacional establecidos en este Reglamento entrarán en vigencia a partir del 1º de abril del 2027.

Artículo 99. Plazo de adecuación. Las entidades de intermediación financiera y los intermediarios cambiarios deberán ajustarse a las disposiciones relativas al requerimiento de capital establecidas en este Reglamento, dentro del plazo comprendido entre la fecha de publicación del instructivo de aplicación correspondiente y el 31 de diciembre del 2026.

Artículo 100. Instructivo de aplicación. La Superintendencia de Bancos dispondrá de un plazo de hasta 180 días, contado a partir de la publicación de este Reglamento, para elaborar el instructivo de aplicación correspondiente, en coordinación con el Banco Central.

Artículo 101. Derogaciones. A partir de la entrada en vigencia de este Reglamento, queda derogado el Reglamento sobre el Riesgo Operacional, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 2 de abril del 2009 y sus modificaciones, así como todas las disposiciones que le sean contrarias'.

2. Esta Resolución deberá ser publicada en uno o más diarios de circulación nacional, en virtud de las disposiciones contenidas en el literal h) del artículo 4 de la Ley núm.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002 y sus modificaciones."

Publicado en fecha 21 de abril del 2026.

-FIN-

…/