-DESIGNACIÓN-
RESOLUCIÓN JM 240905-03

-FECHA-
2024/09/05

-TÍTULO-
TERCERA RESOLUCIÓN DE FECHA 5 DE SEPTIEMBRE DEL 2024 QUE AUTORIZA LA PUBLICACIÓN PARA FINES DE CONSULTA PÚBLICA DE LOS SECTORES INTERESADOS, DE LA PROPUESTA DE MODIFICACIÓN AL REGLAMENTO SOBRE RIESGO OPERACIONAL

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

-DESCRIPTORES-
AUTORIZACIÓN PUBLICACIÓN; CONSULTA PÚBLICA; PROPUESTA DE MODIFICACIÓN INTEGRAL; REGLAMENTO SOBRE RIESGO OPERACIONAL; PLAZO DE 30 DÍAS; 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 **Tercera Resolución** en fecha **5 de septiembre del 2024**, cuyo texto se transcribe a continuación:

"VISTA la comunicación núm.7032 de fecha 18 de junio del 2024, dirigida al Gobernador del Banco Central y Presidente de la Junta Monetaria por el Gerente de dicha Institución, mediante la cual remite la propuesta de modificación integral al Reglamento sobre Riesgo Operacional, aprobado mediante la Quinta Resolución adoptada por la Junta Monetaria en fecha 2 de abril del 2009 y sus modificaciones; y, solicitud de autorización de su publicación para fines de consulta pública;

VISTA la comunicación núm.0795 de fecha 21 de diciembre del 2022, dirigida al Gobernador del Banco Central y Presidente de la Junta Monetaria por el Superintendente de Bancos, mediante la cual remite la propuesta de modificación integral al Reglamento sobre Riesgo Operacional antes mencionado;

VISTA la propuesta de modificación integral del Reglamento sobre Riesgo Operacional, aprobado mediante la Quinta Resolución adoptada por la Junta Monetaria en fecha 2 de abril del 2009 y sus modificaciones;

VISTA la Matriz comparativa de las modificaciones propuestas al Reglamento sobre Riesgo Operacional, por parte del Banco Central y la Superintendencia de Bancos;

…/

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

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 Instructivo sobre Tercerización o Subcontratación de Servicios (*Outsourcing*), aprobado por la Superintendencia de Bancos mediante Circular SB:núm.01/12 de fecha 28 de diciembre del 2012;

VISTA la Circular SB: Núm.011/10, dictada por la Superintendencia de Bancos en de fecha 9 de agosto del 2010;

VISTA la Circular SB: Núm.011/12, adoptada por la Superintendencia de Bancos en fecha 28 de diciembre del 2012;

VISTO el Manual de Requerimiento de Información de la Administración Monetaria y Financiera, aprobado por la Superintendencia de Banco mediante Circular SB: núm.011/12 de fecha 28 de diciembre del 2012 y sus modificaciones;

VISTOS los demás documentos que integran este expediente;

…/

CONSIDERANDO que el literal c) del artículo 9 de la mencionada Ley Monetaria y Financiera, establece que corresponde a la Junta Monetaria dictar los Reglamentos Monetarios y Financieros;

CONSIDERANDO que el literal f) del artículo 46 de la referida Ley Monetaria y Financiera, dispone que reglamentariamente se podrán determinar exigencias adicionales de patrimonio técnico en función de riesgos cambiarios, riesgo de tipo de interés, riesgos de liquidez, riesgos de plazo, riesgos de concentración de pasivos, riegos de colateral, riesgos operacionales, riegos legales y cualquier riesgo que en el futuro puedan agregarse;

CONSIDERANDO que asimismo, el artículo 55 de la referida Ley Monetaria y Financiera, dispone que se establezca reglamentariamente, que las entidades de intermediación financiera deben contar con adecuados sistemas de control de riesgos, mecanismos independientes de control interno y, establecimiento claro y escrito de sus políticas administrativas. Adicionalmente, el literal b) de dicho artículo dispone que las entidades de intermediación financiera, deben contar con procesos integrales que incluyan la administración de los diversos riesgos a que puedan quedar expuestos, así como con los sistemas de información adecuados y con los comités necesarios para la gestión de dichos riesgos;

CONSIDERANDO que la presente propuesta de modificación integral del Reglamento sobre Riesgo Operacional, ha sido consensuada entre los equipos técnicos del Banco Central y de la Superintendencia de Bancos, a los fines de ser sometida al conocimiento y decisión de la Junta Monetaria y obtener la autorización correspondiente para su publicación en consulta pública, al amparo de lo dispuesto en el literal g) del artículo 4 de la mencionada Ley Monetaria y Financiera;

CONSIDERANDO que el Reglamento sobre Riesgo Operacional, tiene por objeto establecer los criterios y lineamientos generales que deberán aplicar las entidades de intermediación financiera, para realizar una adecuada administración del riesgo operacional, con base en lo dispuesto en el literal f) del artículo 46 y, los literales a) y b) del artículo 55 de la Ley Monetaria y Financiera;

CONSIDERANDO que mediante la citada Circular SB: Núm. 011/10, la Superintendencia de Bancos aprobó el Instructivo para la Aplicación del Reglamento sobre Riesgo Operacional, que establece los procedimientos y requisitos mínimos que las entidades de intermediación financiera deben cumplir respecto a políticas, procedimientos y criterios para la identificación de actividades, eventos de pérdidas y la determinación de los ingresos y gastos asociados a cada línea de negocio dentro de la planificación estratégica de las mismas;

…/

CONSIDERANDO que asimismo, la Superintendencia de Bancos emitió la Circular SB: Núm.011/12 de fecha 28 de diciembre del 2012, que aprobó y puso en vigencia el Instructivo sobre Tercerización o Subcontratación de Servicios, para establecer los lineamientos y un marco de referencia que permita a las entidades de intermediación financiera tercerizar sus actividades, manteniendo los debidos controles para una gestión adecuada de los riesgos operacionales en su relación con los proveedores de servicios;

CONSIDERANDO que posteriormente, en el año 2017, el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés), publicó el Marco Regulador Internacional para Bancos, el cual incluye los requerimientos de Basilea III mínimos aplicables a bancos con actividad internacional, actualizando la metodología para el requerimiento de capital por riesgo operacional, adoptando un modelo estándar más sensible a los riesgos que las metodologías anteriores;

CONSIDERANDO que en ese orden, en marzo del año 2021, el Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas en inglés), actualizó los 'Principios para la Gestión adecuada del Riesgo Operacional', inicialmente emitidos en 2003 y revisados en 2014. Las revisiones destacan la necesidad de establecer una cultura robusta de gestión del riesgo operacional y de adaptar el marco de gestión de riesgos de las entidades a sus operaciones diarias. Además, refuerzan las responsabilidades de gobernanza y recomiendan la implementación de estructuras de gobierno claras y definidas;

CONSIDERANDO que los citados principios actualizados, abordan la adopción de mecanismos que aseguran procesos eficientes de gestión del cambio, la elaboración de planes de gestión de riesgos sólidos para la tecnología y seguridad de la información, y estrategias de continuidad del negocio para garantizar la operatividad ante eventos adversos. Asimismo, las recomendaciones incluyen el fortalecimiento de los procesos de monitoreo, la mejora de los controles internos y la implementación de mecanismos efectivos para el reporte y divulgación de información relacionada con la gestión del riesgo operacional;

CONSIDERANDO que en el contexto descrito precedentemente y la necesidad de alinearse con las buenas prácticas del Comité de Basilea, en fecha 21 de diciembre del 2022, mediante la citada comunicación núm.0795, la Superintendencia de Bancos remitió la propuesta de modificación integral del Reglamento sobre Riesgo Operacional, la cual se elaboró en colaboración técnica con el Centro Regional de Asistencia Técnica de Centroamérica Panamá y República Dominicana (CAPTAC-DR), destacando el esfuerzo conjunto para mejorar los estándares de gestión de riesgos;

…/

CONSIDERANDO que la presente propuesta de modificación integral al Reglamento sobre Riesgo Operacional, tiene su justificación en la crisis financiera internacional del año 2008, la cual expuso de manifiesto claramente dos limitaciones críticas en el marco de riesgo operacional de los bancos. Por una parte, los requerimientos de capital para cubrir el riesgo operacional se mostraron insuficientes para absorber las pérdidas significativas; y, de otra parte, los sistemas y controles existentes no permitieron un uso efectivo de modelos internos para estimar adecuadamente los requerimientos de capital necesarios. Ante estos retos, la modificación propuesta propende a la convergencia de la regulación de la República Dominicana con las mejores prácticas internacionales en regulación bancaria de Basilea III, tanto en la gestión como en la supervisión prudencial. Este avance no solo se espera que eleve la confianza y la percepción sobre el mercado financiero local, sino que también podría posicionar mejor al país para atraer condiciones de financiamiento más favorables de inversores extranjeros y entidades multilaterales;

CONSIDERANDO que las propuestas de modificaciones están diseñadas para integrarse con el Marco de Supervisión Basado en Riesgo de la Superintendencia de Bancos. Esto incluye un enfoque reforzado en herramientas de gestión y supervisión robustas, atendiendo integralmente a todos los aspectos vinculados al riesgo operacional, incluyendo los tecnológicos, de seguridad de la información y riesgos sistémicos;

CONSIDERANDO que en otro orden, de acuerdo con el Reporte del año 2022 de la Asociación de Supervisores Bancarios de las Américas (ASBA), sobre la implementación de los estándares de Basilea en Latinoamérica y el Caribe, varios países de la región han adoptado el método estándar de Basilea III para el requerimiento de capital por riesgo operacional, incluyendo Argentina, Chile, Colombia, México, Panamá y Uruguay. En Argentina, el Banco Central ha incorporado el referido método como base para el cálculo del capital requerido por riesgo operacional, especificado en detalle en los documentos regulatorios pertinentes;

CONSIDERANDO que en el caso de Colombia, el requerimiento de patrimonio adecuado por riesgo operacional ha sido regulado mediante legislación nacional y detallado posteriormente por la Superintendencia Financiera para establecer las reglas relativas a la aplicación de este método. México y Chile también han integrado el método estándar en sus regulaciones bancarias, buscando mejorar los requerimientos de capital por riesgo operacional;

CONSIDERANDO que asimismo, la gestión de riesgos de tecnología y ciberseguridad también ha tenido un enfoque significativo en la región. Las normativas en El Salvador y Colombia han establecido directrices claras para la gestión de estos riesgos, incluyendo el desarrollo de planes de continuidad operativa para mitigar potenciales fallas

…/

tecnológicas y de seguridad. Costa Rica ha seguido un enfoque similar, incorporando estos aspectos en su marco regulador para fortalecer la resiliencia del sector financiero;

CONSIDERANDO que además se ha hecho un énfasis en fortalecer las fuentes de información para una mejor estimación de las exposiciones, construcción de indicadores eficientes de monitoreo y una apropiada toma de decisiones para la gestión del riesgo operacional. Colombia, con la implementación del Sistema Informático de Administración de Riesgo Operacional (SARO), ha ido un paso adelante en este sentido, mientras que en Costa Rica se ha establecido la necesidad de una base de datos para incidentes y eventos de pérdidas potenciales, con el fin de mejorar la evaluación de riesgos;

CONSIDERANDO que en ese mismo orden, en Chile la normativa ha incluido además el fortalecimiento de los procesos de tercerización y la aplicación rigurosa del marco de gestión del riesgo operacional en líneas de defensa, resaltando la importancia de las matrices de riesgo como herramientas para una evaluación detallada y efectiva del riesgo operacional;

CONSIDERANDO que en respuesta a estos desarrollos regionales, la Superintendencia de Bancos de la República Dominicana, solicitó la asistencia técnica del Centro Regional de Asistencia Técnica de Centroamérica, Panamá y República Dominicana (CAPTAC-DR), para alinear la normativa nacional con los estándares internacionales de Basilea III. Los resultados de esta colaboración están orientados hacia un marco de riesgo operacional más robusto, el requerimiento de capital por método estándar, la implementación de estándares de gobernanza reforzados y mejoras en la gestión del riesgo tecnológico y de seguridad de la información;

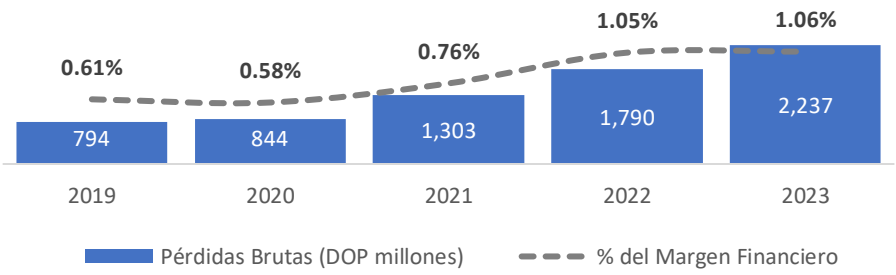
CONSIDERANDO que en tal sentido, de acuerdo con la versión más reciente del 'Informe Anual de Riesgo Operacional al 31 de diciembre del 2023', actualizado en abril del 2024 y publicado por la Superintendencia de Bancos, se han identificado estadísticas sobre los eventos de riesgo operacional en el sector financiero. Entre 2019 y 2023, las entidades de intermediación financiera reportaron un promedio anual de 19,000 eventos de riesgo operacional. A finales del 2023, se registró un incremento significativo, alcanzando un total de 34,100 eventos, lo cual duplicó la cifra del año anterior, con un 88.1% de estos, correspondientes a pérdidas por fraude externo;

CONSIDERANDO que el citado informe señala que, al cierre del 2023, los bancos múltiples reportaron más del 87% del total de eventos; mientras que las asociaciones de ahorros y préstamos contribuyeron con aproximadamente un 13%; presentaron una menor cantidad de eventos, aproximadamente el 0.40%, los bancos de ahorro y crédito, las corporaciones de crédito y las entidades públicas de intermediación financiera. Las

…/

pérdidas brutas durante el año alcanzaron los RD$2,237 millones, lo que equivale a un 1.06% del margen financiero bruto del sistema, manteniendo una proporción similar al 1.05% observado en el 2022, conforme se muestra en el cuadro siguiente:

Pérdidas Brutas por Riesgo Operacional/Margen Financiero Bruto



*Datos obtenidos del 'Informe Anual de Riesgo Operacional al 31 de diciembre del 2023, publicado por la Superintendencia de Bancos, actualizado en abril del 2024.

CONSIDERANDO que el análisis sectorial revela una tendencia ascendente en el porcentaje de pérdidas brutas respecto al margen financiero bruto en la mayoría de las entidades de intermediación financiera, con un incremento notable desde el 2021. Este patrón sugiere un aumento en la frecuencia de los eventos de riesgo operacional o una disminución en la eficacia con que las entidades gestionan estos, según se indica a continuación:

Pérdidas Brutas / Margen Financiero Bruto

Tipo de Entidad	2019	2020	2021	2022	2023
Asociaciones de Ahorros y Préstamos	0.61%	0.56%	0.53%	0.78%	1.08%
Bancos de Ahorro y Crédito	0.08%	0.14%	0.21%	0.24%	0.23%
Bancos Múltiples	0.64%	0.60%	0.81%	1.13%	1.07%
Corporaciones de Crédito	0.40%	0.44%	0.58%	0.34%	0.32%
Sistema Financiero	0.61%	0.58%	0.76%	1.05%	1.06%

* Datos obtenidos del 'Informe Anual de Riesgo Operacional al 31 de diciembre de 2023', publicado por la Superintendencia de Bancos, actualizado en abril del 2024.

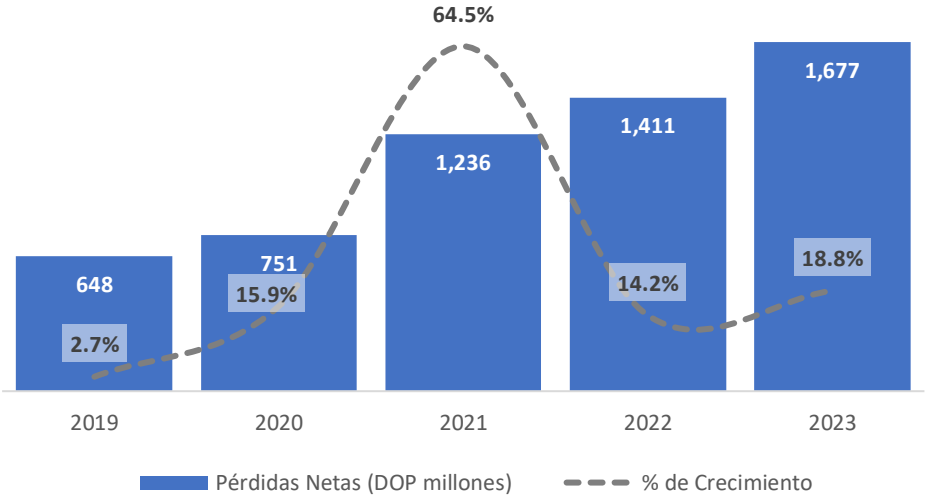
CONSIDERANDO que adicionalmente, el citado informe, indica un aumento en las recuperaciones al final del año 2023, que representaron el 25.1% de la pérdida bruta registrada. Un aumento sustancial se observó en las pérdidas atribuidas a fraudes en

canales de internet y banca electrónica, que promediaron el 38% del total de las pérdidas por canales de distribución;

CONSIDERANDO que según indica el referido informe el fraude externo fue el tipo de evento con mayor impacto en las pérdidas netas durante el período analizado, constituyendo más del 67% del total. Al finalizar el 2023, las pérdidas netas por esta categoría alcanzaron RD$1,121 millones, un incremento del 49% respecto al año anterior, principalmente por transferencias de fondos fraudulentas y robo de información de tarjetas;

CONSIDERANDO que además el mencionado informe se refiere al crecimiento continuo de dichas pérdidas netas, promediando un aumento anual del 16.5%, culminando en RD$1,677 millones en diciembre del 2023. Este aumento representó el 1.74% de las utilidades antes de impuestos del sistema financiero ese año, con un crecimiento nominal del 18.8% y un crecimiento real del 15.2% comparado con el año anterior, según se muestra a continuación:

Histórico de Variación Interanual de Pérdidas Netas



* Datos obtenidos del "Informe Anual de Riesgo Operacional al 31 de diciembre de 2023", publicado por la Superintendencia de Bancos, actualizado en abril de 2024.

CONSIDERANDO que los hallazgos antes mencionados subrayan la necesidad de revisar y fortalecer la normativa vigente sobre la gestión del riesgo operacional. La significativa alza en los eventos, particularmente en pérdidas por fraude externo y el incremento en las pérdidas económicas, justifican una actualización exhaustiva del reglamento, por lo cual esta propuesta de modificación integral al Reglamento sobre

…/

Riesgo Operacional, no solo busca cerrar brechas que han permitido tales vulnerabilidades, sino también mejorar los mecanismos de supervisión y control, además de establecer requisitos más estrictos para la gestión de la tecnología y la seguridad de la información. El objetivo, en sentido general, es alinear más estrechamente las prácticas del sector financiero dominicano con los estándares internacionales de Basilea III, mejorando así la estabilidad y la confianza en el sistema financiero nacional;

CONSIDERANDO en cuanto al análisis de la adecuación patrimonial por riesgo operacional, de conformidad con la evaluación de impacto realizada por el Departamento de Regulación y Estabilidad Financiera del Banco Central, respecto al índice de solvencia frente al requerimiento de capital por riesgo operacional en la banca múltiple, se ha determinado que la implementación del método estándar de Basilea III, es técnicamente factible. La metodología estándar establece los requisitos de capital en función de dos componentes fundamentales: i) los ingresos de la entidad; y, ii) las pérdidas históricas ocasionadas por fallas operacionales, ya sea en procesos, personal, sistemas internos, tecnología o eventos externos. Para determinar el impacto de estas variables en el índice de solvencia, se emplearon datos analíticos suministrados por la Superintendencia de Bancos, cumpliendo con los criterios estipulados por la metodología de Basilea III, para asegurar una evaluación precisa y conforme a las normativas internacionales;

CONSIDERANDO que la evaluación se centró en calcular un índice de solvencia ajustado a los nuevos requerimientos de capital por riesgo operacional, con el objetivo de comprobar la suficiencia y cumplimiento patrimonial. Este cálculo incluyó los activos ponderados por riesgo crediticio y de mercado del subsector de los bancos múltiples, añadiendo el capital estimado necesario para cubrir el riesgo operacional según la metodología empleada;

CONSIDERANDO que los hallazgos de la evaluación, indicaron que la integración del capital destinado a gestionar el riesgo operacional, no resultaría en un incumplimiento del índice de solvencia del 10%, establecido por las Normas Prudenciales de Adecuación Patrimonial aplicables a las entidades de intermediación financiera. Este resultado subraya la factibilidad de aplicar la metodología estándar sin afectar la estabilidad financiera del subsector o, en otros términos, que el sistema financiero ya dispone de los excedentes patrimoniales para absorber los requerimientos de capital por riesgo operacional;

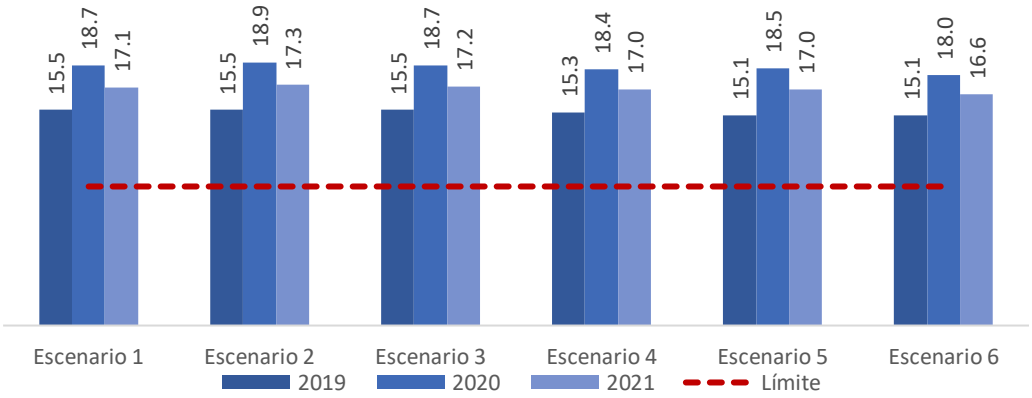
CONSIDERANDO que de igual manera, la Superintendencia de Bancos llevó a cabo ejercicios similares, concluyendo que la carga de capital adicional por riesgo operacional para las entidades de intermediación financiera, resulta mínima en comparación con la

…/

requerida actualmente por los riesgos de crédito y de mercado, evidenciando que la adopción de esta metodología no implica aportes significativos de capital adicional para cumplir con los mínimos regulatorios;

CONSIDERANDO que además se realizaron estimaciones de los requerimientos de capital por riesgo operacional, tomando en cuenta 6 escenarios diferentes, todos bajo el marco de Basilea III, demostrando los resultados que todas las entidades mantuvieron un nivel de solvencia por encima del mínimo requerido del 10% en todos los escenarios analizados, conforme a la norma de adecuación patrimonial, según se muestra en el gráfico siguiente:

Resultados escenarios del Índice de Solvencia con el Requerimiento de Capital por Riesgo Operacional (en porcentaje)



* Datos obtenidos del Informe Anual de la Superintendencia de Bancos sobre Requerimiento de Capital por Riesgo Operacional (ORC, por sus siglas en inglés) con metodología de Basilea III, mayo 2022.

CONSIDERANDO que adicionalmente, se realizó un análisis utilizando datos muestrales de 784 entidades bancarias a nivel mundial al cierre del 2023, en las cuales se verifica que la mediana del riesgo operacional, como proporción de los activos ponderados en base a riesgo, es de 7.8%. Reduciendo esta muestra para entidades bancarias, en Argentina, Brasil, Colombia y México, la citada proporción se ubica en 7.6%, es decir, para entidades bancarias con requerimientos de capital por riesgo operacional implementados en sus jurisdicciones, dicho riesgo absorbe menos del 10% de sus activos ponderados en base a riesgo;

CONSIDERANDO que extrapolando para el caso dominicano, es decir, aumentando los activos y contingentes ponderados por riesgo en 7.7%, se obtendría una reducción en el índice de solvencia del sistema financiero de 16.12% a 16.00% a diciembre del 2023,

…/

evidenciando que implementar esta norma a partir de su impacto en entidades bancarias globales y de la región, no conllevaría el levantamiento de nuevo capital para el sistema financiero nacional, con el fin de mantener el cumplimiento de los requerimientos de capital regulatorio;

CONSIDERANDO que en conclusión, la implementación del método estándar de Basilea III para el cálculo del requerimiento de capital por riesgo operacional, ha demostrado ser viable para la República Dominicana. La rigurosidad del análisis realizado, asegura que las entidades de intermediación financiera pueden adoptar esta metodología sin comprometer su solvencia ni la estabilidad del sistema financiero. Los resultados reafirman la capacidad de las entidades para manejar eficazmente el riesgo operacional bajo los nuevos estándares, permitiendo así una alineación más estrecha con las prácticas bancarias internacionales y fortaleciendo la confianza en el sector financiero nacional;

CONSIDERANDO que es preciso señalar que la presente propuesta de modificación integral del Reglamento sobre Riesgo Operacional, especifica los bloques estructurales del modelo general del método estándar conforme Basilea III, para exigir el cálculo del requerimiento de capital por riesgo operacional. Los detalles y requisitos de la metodología serán establecidos en el instructivo de aplicación de dicho Reglamento, para facilitar una adecuación más dinámica propia de la naturaleza del riesgo operacional;

CONSIDERANDO que en otro orden, la presente propuesta de modificación integral del Reglamento sobre Riesgo Operacional, contempla un conjunto de modificaciones, entre las cuales se encuentran, como las más relevantes, las siguientes:

a) Sobre el alcance, se mejoran las políticas y procedimientos existentes, enfocándose especialmente en la actualización de la metodología para el cálculo del requerimiento de capital por riesgo operacional y la optimización del plan de continuidad de negocios, asegurando que estos componentes cumplan con las últimas normativas y mejores prácticas internacionales;

b) Sobre las definiciones, para mejorar la comprensión y aplicación del Reglamento, se incorporan nuevos términos, tales como Apetito del Riesgo, Capacidad del Riesgo, Confidencialidad, Continuidad de Negocio, Cultura de Riesgo Operacional y Disponibilidad, entre otros;

c) Se incorporan disposiciones para que las entidades desarrollen y mantengan un marco de gestión de riesgo operacional alineado a su apetito y tolerancia al riesgo;

…/

d) Con relación a la cultura de gestión de riesgos, se requiere que el Consejo de Administración establezca y fomente una sólida cultura de gestión de riesgo operacional, la cual deberá ser implementada efectivamente por la Alta Gerencia;

e) Se establece un código de conducta o política de ética que aborda el riesgo asociado a la conducta en todos los niveles de la entidad, estableciendo expectativas claras de integridad y valores éticos;

f) Se establece que el Consejo de Administración deberá aprobar la declaración de apetito y tolerancia al riesgo operacional, definiendo claramente los tipos y niveles de riesgo que la entidad esté dispuesta a asumir. Paralelamente, la Alta Gerencia será responsable de determinar y gestionar la capacidad de riesgo operacional especificado;

g) Se dispone que las entidades establezcan políticas de compensación alineadas con su apetito y tolerancia al riesgo y equilibrar adecuadamente el riesgo con la recompensa;

h) Se establece un modelo de 3 líneas de defensa, que las entidades deberán implementar para la gestión del riesgo operacional, adaptándolo a su naturaleza, tamaño, complejidad y perfil de riesgo. Además, se define claramente la estructura y las funciones específicas de cada una de dichas líneas de defensa;

i) Se dispone que las entidades deben establecer expectativas claras para asegurar que su personal comprenda sus roles y responsabilidades en la gestión de riesgos. Igualmente, deberán garantizar que se proporcione un nivel adecuado de capacitación en riesgo operacional a todos los niveles de la organización;

j) Se establece el uso de la estructura de gobierno existente para implementar un enfoque eficaz de resiliencia operativa, diseñado para permitir una respuesta rápida y adaptación efectiva ante eventos disruptivos;

k) Con respecto a la gobernanza del riesgo operacional, se introducen nuevas disposiciones que diseñan la estructura organizativa para la gestión del riesgo operacional, incluyendo la creación del Comité de Gestión Integral de Riesgos, y unidades especializadas. Asimismo, se establecen las responsabilidades del Consejo de Administración, el Comité de Gestión Integral de Riesgos, el Comité de Riesgo Operacional, la Alta Gerencia y las Unidades Especializadas de Riesgo Operacional, asegurando una gestión cohesiva y eficaz del riesgo en toda la organización;

…/

l) Sobre las unidades de negocio, se clarifican las funciones y responsabilidades de las mismas como la primera línea de defensa en la gestión de riesgo operacional. Esto incluye la responsabilidad directa de identificar, evaluar y gestionar los riesgos dentro de sus operaciones diarias;

m) En cuanto a la responsabilidad de la Unidad de Auditoría Interna, se detallan las funciones de la misma en la implementación y supervisión del marco de gestión de riesgo operacional; incluyendo la evaluación independiente de la eficacia de las políticas y controles de riesgo operacional, así como la recomendación de mejoras continuas;

n) Con respecto a las herramientas de gestión del riesgo operacional, se dispone que las entidades deben implementar herramientas eficientes para la identificación y evaluación del riesgo operacional, tales como, mapeo de procesos, taxonomía de tipos de riesgo operacional, inventario de controles, evaluación de riesgo y controles, matriz de riesgo operacional, mapa de calor e indicadores de riesgos, entre otros;

o) En el marco de gestión del cambio, se incorporan nuevas disposiciones que requieren la implementación de políticas y procedimientos para la evaluación y aprobación de nuevos productos, servicios, actividades, procesos, canales y sistemas. Se incluyen, además, las funciones asociadas a la primera y segunda línea de defensa;

p) Se establece un capítulo que especifica cómo las entidades deben monitorear, recopilar y analizar los datos sobre el riesgo operacional para facilitar la toma de decisiones informadas y oportunas. De igual forma, se disponen criterios claros para la presentación de informes, garantizando consistencia y transparencia en la comunicación de estos riesgos;

q) Se refuerzan las disposiciones sobre el sistema de control interno, que definen los elementos esenciales que deberán considerarse para el cumplimiento de las políticas, así como los controles internos mínimos y efectivos para la adecuada segregación de tareas y responsabilidades esenciales para mitigar riesgos y prevenir conflictos de interés;

r) Se establecen directrices que las entidades de intermediación financiera deben seguir al preparar el plan de continuidad del negocio. Dichas directrices incluyen los aspectos críticos a considerar y las políticas específicas de gestión de continuidad que aseguran la capacidad de la entidad para mantener operaciones críticas ante interrupciones;

…/

s) Se introduce un nuevo capítulo sobre gestión de servicios tercerizados, que establece las políticas y procesos que las entidades deben adoptar para gestionar eficazmente las actividades tercerizadas. Además se requiere que las entidades desarrollen estrategias adecuadas para mantener su resiliencia operativa, en caso de fallas por parte de terceros;

t) Se incluye un capítulo dedicado a los eventos de riesgo operacional, en el cual se especifica que las entidades deben implementar procedimientos y procesos sistemáticos para la identificación precisa y recopilación de datos sobre eventos de riesgo operacional. Asimismo, se establecen disposiciones para la contabilización de pérdidas y la obligación de reportar estos eventos, asegurando transparencia y responsabilidad en el manejo de los riesgos;

u) Se establece la necesidad sobre la divulgación de información, de forma tal, que las entidades desarrollen y mantengan una política formal de divulgación que detalle claramente el enfoque para determinar qué información sobre riesgo operacional se divulgará. Adicionalmente, las entidades deberán implementar un proceso sistemático para evaluar la efectividad de esta política de divulgación, garantizando que cumpla con las expectativas regulatorias y de transparencia;

v) Se incorporan disposiciones, en el marco de gestión de los riesgos tecnológicos, con el objetivo de garantizar que el desempeño de los procesos de negocio de la entidad se mantenga dentro de los límites establecidos por su apetito y tolerancia de riesgo;

w) Se establece un marco de gobernanza de tecnología de la información (TI), que incluye la estructura organizativa, políticas, procedimientos y controles necesarios para gestionar efectivamente la seguridad de la información;

x) Sobre la gestión del riesgo legal, se requiere que las entidades implementen políticas y procedimientos robustos para la identificación, análisis, evaluación y mitigación de situaciones que generen riesgo legal. Además, deben establecer y mantener una base de datos histórica que registre todos los procedimientos administrativos, judiciales y arbitrales a los que la entidad ha estado sujeta;

y) Se amplían las disposiciones relacionadas con las notificaciones y solicitudes de no objeción, especificando claramente que requieren una u otra acción por parte de la Superintendencia de Bancos; y,

z) Se modifica el artículo sobre el requerimiento de capital por riesgo operacional, para especificar que las entidades deben calcular este requerimiento, orientado en su

…/

configuración general, por los bloques estructurales del método estándar establecido en el tercer acuerdo del Comité de Supervisión Bancaria de Basilea, que diseña dicho requerimiento patrimonial, como una métrica definida por distribuciones de probabilidad por cada línea de negocio y valores de exposición estresados por pérdidas históricas.

CONSIDERANDO que las propuestas de modificación citadas precedentemente, están diseñadas para actualizar y fortalecer el marco regulatorio en la gestión del riesgo operacional, alineándolo con las mejores prácticas internacionales. Al introducir cambios estructurales claros y procesos definidos, dichas modificaciones aumentan la coherencia y efectividad del sistema de gestión de los riesgos operacionales en las entidades de intermediación financiera; esto incluye la mejora de las políticas sobre estructura organizativa y responsabilidades, permitiendo una implementación más precisa y efectiva;

CONSIDERANDO que en tal sentido, al reforzar las normativas de gobernanza y establecer requisitos de divulgación más estrictos, esta propuesta de modificación integral al Reglamento sobre Riesgo Operacional, busca garantizar una mayor transparencia y rendición de cuentas dentro del sistema financiero. Estas medidas son esenciales para mantener la confianza del mercado y asegurar que las entidades de intermediación financiera, no solo cumplen con las regulaciones actuales, sino que están preparadas para adaptarse a cambios futuros, fortaleciendo así la resiliencia y sostenibilidad del sistema financiero a largo plazo;

CONSIDERANDO que en atención a todo lo expuesto precedentemente y al análisis exhaustivo, la evaluación y consenso alcanzados por los equipos técnicos del Banco Central y de la Superintendencia de Bancos, donde se han incluido aquellas sugerencias que refuerzan de manera efectiva el proyecto de modificación integral al Reglamento sobre Riesgo Operacional, la Gerencia del Banco Central recomienda a la Junta Monetaria, acoger la presente propuesta, para su puesta en consulta pública a los sectores interesados;

Por tanto, la Junta Monetaria

R E S U E L V E:

1. Autorizar la publicación, para fines de consulta pública de los sectores interesados, de la propuesta de modificación integral del Reglamento sobre Riesgo Operacional, aprobado por la Junta Monetaria mediante su Quinta Resolución de fecha 2 de abril del 2009 y sus modificaciones, en virtud de lo dispuesto en el literal g) del artículo 4

…/

de la Ley núm.183-02 Monetaria y Financiera, de fecha 21 de noviembre del 2002 y sus modificaciones, para que 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, para realizar una adecuada gestión del riesgo operacional, en cumplimiento con las disposiciones contenidas en los artículos 46, literal f) y 55, literales a) y b) de la Ley núm.183-02, Monetaria y Financiera de fecha 21 de noviembre del 2002 y sus modificaciones.

Artículo 2. Alcance. El alcance de este Reglamento comprende las políticas y procedimientos mínimos que deberán implementar las entidades de intermediación financiera para identificar, medir, evaluar, monitorear y controlar el riesgo operacional al que están expuestas, así como las consideraciones de lugar para el desarrollo del plan de continuidad de negocios 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; y,

e) Entidades Públicas de Intermediación Financiera.

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 del 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 del Riesgo:** Es el nivel 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:** Es el 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, a fin de que la misma no sea divulgada, en todo o en parte, a personas físicas o jurídicas, o procesos, a menos que éstos 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 organización para continuar con la entrega de productos y prestación de servicios a niveles predefinidos y aceptables tras una interrupción;

…/

h) **Control:** Cualquier acción, medio o recurso diseñado con la finalidad de disminuir el nivel de uno o varios riesgos a través de la reducción de la probabilidad y/o impacto de estos;

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

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 accesible y utilizable 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 acontecimientos externos que pudieran derivar impactos de pérdidas a las entidades afectadas;

m) **Factores de riesgo:** Se refiere a las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operacional a nivel de la actividad o unidad de negocio;

n) **Gestión del Cambio:** Consiste en un 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;

o) **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;

…/

p) **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;

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

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

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

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

u) **Lucro Cesante:** Es la 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;

v) **Mapa de Calor de Riesgos:** Es una 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;

w) **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;

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

y) **Matriz de Riesgos Operacionales:** Es una 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;

z) **Medidas de Contingencia:** Son aquellas 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;

aa) **Nuevo Producto, Servicio o Canal: Es** 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;

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

cc) **Pérdida Bruta:** Es la pérdida antes de aplicar recuperaciones de cualquier tipo;

dd) **Pérdida Directa:** Es el monto de dinero que se pierde directamente por la ocurrencia del evento de pérdida, sean estas recuperables o no, como es el monto del dinero robado de caja, valor del equipo robado, entre otros. Incluye las provisiones realizadas producto del evento;

ee) **Pérdida Económica:** Es el impacto negativo 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;

ff) **Pérdida Indirecta:** Es el 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;

gg) **Pérdida Neta:** Es la pérdida después de tener en consideración los efectos de las recuperaciones (Pérdida Neta = Pérdida Bruta – Recuperaciones);

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

…/

ii) **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);

jj) **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;

kk) **Pista de auditoría:** Es el 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;

ll) **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;

mm) **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;

nn) **Probabilidad:** Es la 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;

oo) **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;

pp) **Resiliencia Operativa:** Es la 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 su impacto en la entrega de operaciones críticas a través de la interrupción;

…/

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

rr) **Riesgo inherente:** Es el riesgo intrínseco relativo al desempeño de las actividades significativas de la entidad de intermediación financiera 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;

ss) **Riesgo legal:** Es la 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 éstos;

tt) **Riesgo operacional:** Es la 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;

uu) **Riesgo residual:** Es el nivel de riesgo que permanece después de la verificación o estimación de la efectividad de los controles sobre los riesgos inherentes;

vv) **Riesgo tecnológico:** Posibilidad de sufrir un impacto adverso relacionado con la afectación de la confidencialidad, integridad o disponibilidad de la información o de la infraestructura tecnológica;

ww) **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;

…/

xx) **Tercerización de Servicios:** Corresponde a la 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 tenga dependencia del proveedor contratado;

yy) **Tecnología de Información (TI):** Es el 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;

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

aaa) **Unidad de Gestión Integral de Riesgo:** 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;

bbb) **Unidad Especializada de Gestión de Riesgo:** Es la responsable de ejecutar las disposiciones definidas por la unidad de gestión integral de riesgo 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;

ccc) **Unidad de Negocio:** Son las unidades con 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,

ddd) **Vulnerabilidad:** Es una 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. De conformidad con lo dispuesto en el artículo 55 de la Ley Monetaria y Financiera, 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.

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 del riesgo, importancia sistémica y la situación macroeconómica y de los mercados, acorde a su apetito y nivel de tolerancia al riesgo, con el propósito de evaluar la adecuación de su capital y liquidez, en relación con los distintos riesgos que asume.

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

Artículo 7. Alcance del Marco de Gestión. Las entidades deberán asegurar que el marco de gestión del riesgo Operacional defina el alcance de las 3 (tres) 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 liderar el establecimiento de una fuerte cultura de gestión de riesgo operacional, implementada por la Alta Gerencia, así como instaurar una cultura corporativa guiada por una sólida gestión de riesgos, estableciendo estándares e incentivos para un comportamiento profesional y responsable.

Párrafo. La entidad deberá establecer sistemas de sensibilización al riesgo operacional con incentivos monetarios o no monetarios, a través de indicadores medibles sobre la implementación y resultado de la Gestión del Riesgo Operacional.

Artículo 9. Código de Conducta o Política de Ética. El Consejo deberá establecer un código de conducta o una política de ética para abordar el riesgo asociado a la conducta. Este código o política debe aplicarse a todos los niveles de la entidad, tanto a los miembros de dicho Consejo como al personal en general, estableciendo expectativas claras de integridad y valores éticos del más alto nivel, tales como la

…/

prohibición e identificación de posibles conflictos de intereses y del ofrecimiento inapropiado de servicios financieros.

Párrafo. El código de conducta o la política de ética deberán ser aprobados y revisados regularmente por el Consejo y debidamente conocido por los empleados. 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.

Artículo 10. Apetito, Tolerancia y Capacidad al Riesgo. El Consejo deberá aprobar la declaración de apetito y tolerancia para el riesgo operacional que articule la naturaleza, los tipos y niveles de riesgo operacional que la entidad esté dispuesta a asumir, vinculándose a la estrategia a corto y largo plazo de la misma 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 debe definir el marco del apetito por el riesgo alineado a la estrategia de la entidad, incluyendo las políticas, controles y sistemas mediante los cuales se establece, comunica y monitorea el apetito por el riesgo. Este marco 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 del 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 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 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 que estén alineadas con la declaración de apetito y tolerancia al riesgo de la entidad, y equilibrar adecuadamente el riesgo con la recompensa.

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 al 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 (tres) 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 siguientes:

a) **Primera Línea de Defensa:** Esta corresponde a la línea funcional (Unidades de Negocios). Esta línea tiene la propiedad del riesgo, por lo que reconoce y gestiona el riesgo en el que incurre al realizar sus actividades. Esta 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, es responsable de implementar controles apropiados para mitigar el riesgo operacional inherente y evaluar el diseño y efectividad de dichos controles.

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. Dicha función 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, representan 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 revisiones especializadas relacionadas con la Gestión del Riesgo Operacional y evaluaciones objetivas de la medición y/o estimación de riesgos realizadas por las unidades de negocios. En adición, en esta línea se establecen herramientas de informes para proporcionar una seguridad razonable de que estos son adecuadamente completos y bien informados.

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 ni operación de los procesos de gestión de riesgos elaborados por las otras 2 (dos) líneas de defensa. El alcance y la frecuencia de las revisiones, deberán ser suficientes para cubrir todas las actividades de la entidad, así como verificar que el marco de gestión del riesgo operacional se haya implementado según lo previsto y funcione de manera efectiva, así como dar un seguimiento a los informes del ente supervisor.

Párrafo I. Las entidades deben poder demostrar que el enfoque de 3 (tres) líneas de defensa está funcionando satisfactoriamente y explicar cómo el Consejo, la auditoría independiente y la Alta Gerencia se aseguran de que este enfoque 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) Una 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 expectativas y responsabilidades claras para garantizar que su personal comprenda sus roles y responsabilidades para la gestión del riesgo operacional, así como su autoridad para actuar frente al mismo.

…/

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 está destinada.

Párrafo. Se deberá proveer capacitación especializada 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. Mecanismos de Notificación. Las entidades deberán disponer de adecuados mecanismos de notificación de cualquier situación que pudiera afectar el riesgo operacional, para mantener informados al Banco Central y a la Superintendencia de Bancos.

Artículo 17. Enfoque de Resiliencia Operativa. Las entidades deben utilizar su estructura de gobierno existente para establecer, supervisar e implementar un enfoque eficaz de resiliencia operativa, es decir, con capacidad de proveer y mantener operaciones críticas durante disrupciones, que les permita responder y adaptarse, así como recuperarse y aprender de los eventos disruptivos 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 18. Organización. La estructura de la gestión del riesgo operacional deberá estar acorde a 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 legal.

Párrafo. Las entidades deberán revisar dicha 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 19. 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 tolerancia y apetito al riesgo aprobados. Dicho comité reportará al Consejo.

Artículo 20. Comité de Riesgo Operacional. Dependiendo de la naturaleza y tamaño de la entidad, y en función de los criterios de proporcionalidad aplicables, las entidades que califiquen en la categoría más alta, deberán disponer de un Comité interno de la Alta Gerencia para la gestión del riesgo operacional, el cual deberá reportar directamente al Ejecutivo Principal y tendrá la obligación de presentar las iniciativas al comité de gestión integral de riesgos.

Párrafo I. Para las entidades que no estén en la categoría más alta, será de carácter opcional la disposición, mantenimiento e implementación de dicho Comité.

Párrafo II. La Junta Monetaria definirá los criterios de proporcionalidad a ser aplicados para determinar las categorías de cada una de las entidades.

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

Artículo 21. Unidad Especializada de Riesgo Operacional. La posición del responsable de la unidad especializada de riesgo operacional, responderá funcional y administrativamente al responsable de 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 22. Gestión del Riesgo 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; y, deberán adoptar políticas y procedimientos, tanto a nivel individual, como a nivel consolidado de sus filiales.

…/

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 las mismas 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 permita una adecuada gestión del riesgo operacional al que está expuesta la entidad, así como velar por su cumplimiento, vigilando que la Alta Gerencia implemente las medidas necesarias para monitorear y controlar estos riesgos;

b) Velar porque 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) Establecer el sistema de incentivos para la sensibilización del riesgo operacional;

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

g) Obtener 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 externos del mercado y otros factores ambientales, así como aquellos asociados a nuevos productos, actividades, procesos o sistemas, cambios en los perfiles y prioridades de riesgo;

…/

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

j) Supervisar que la entidad se mantenga actualizada con las mejores prácticas de gestión del Riesgo Operacional; y,

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

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

Artículo 25. Responsabilidad del Comité de Riesgo Operacional. Las responsabilidades de este Comité serán las delegadas por el Comité de Gestión Integral de Riesgos, sobre el monitoreo y seguimiento del riesgo operacional, incluyendo aquellas que, por el volumen de las informaciones a revisar, requieran mayor análisis y consenso antes de ser presentadas a dicho Comité. 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.

Párrafo. Las decisiones acordadas en el Comité de Riesgo Operacional, deberán ser conocidas y validadas 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 (tres) líneas de defensa, deberá definir una estructura de gobierno clara, efectiva y sólida, con responsabilidades bien definidas, 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 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 claramente 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 y tolerancia al 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 personal con la experiencia y las capacidades técnicas necesarias, y que cuente con el acceso a los recursos requeridos para realizar sus funciones;

f) Coordinar que el personal responsable de supervisar y hacer cumplir las políticas de riesgos 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 de 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 y asegurar que las unidades

…/

de negocio estén ejecutando correctamente las estrategias, políticas, procesos y procedimientos de gestión de dichos riesgos. 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) Verificar el desarrollo continuo, implementación y el uso de herramientas apropiadas de gestión de riesgo operacional;

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 un punto de vista 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 la escalada oportuna y precisa, dentro de la entidad, de los problemas materiales; y,

n) Reportar 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 y Tolerancia; y, las actividades relevantes para su mitigación y adecuada administración.

Párrafo. Los encargados 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) Identificación, análisis y valoración de 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 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 operativos;

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 metodología, 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 rápida, 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 organización, tales como

…/

el respeto del apetito, la tolerancia y la capacidad al riesgo, el ajuste del marco a las circunstancias operativas cambiantes y con las disposiciones legales y legislativas, 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 a 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 claves, 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 herramientas 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 riesgo operacional;

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, 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 riesgos 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 riesgos, priorizarlos, 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 (tres) líneas de defensa, las funciones siguientes:

a) La primera línea de defensa debe realizar evaluaciones de 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 controles y las evaluaciones de estos realizadas por la primera línea de defensa, monitoreando que su implementación sea apropiada y cubra todas las fases de este proceso. Adicionalmente, deberá de presentar al comité de gestión integral de riesgos, los resultados de la evaluación de riesgo operacional realizada.

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 reportes que contenga, al menos, la información 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) Detalle 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 poder 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 y sistemas); y,

e) 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 constante 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 el perfil, el apetito y la tolerancia al riesgo operacional.

Artículo 39. Presentación Interna de Informes. Los informes se deben presentar 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 la gestión de riesgos, así como los generados por o para las autoridades de supervisión, cuando corresponda. Asimismo, la frecuencia de éstos deberá reflejar los riesgos involucrados, el ritmo y la naturaleza de los cambios en el entorno operativo.

Párrafo. La primera línea de defensa debe garantizar la presentación de informes sobre los riesgos operativos residuales, los eventos de riesgo operacional, las deficiencias de control, las deficiencias del proceso y el incumplimiento de las tolerancias de riesgo operativo.

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 del cumplimiento de dichas políticas, la inclusión 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 mas 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 DEL NEGOCIO

Artículo 45. Plan de Continuidad del Negocio. Las entidades deben implementar planes de continuidad 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 del Negocio. Las entidades deben 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 los aspectos siguientes:

a) Identificación y clasificación de las operaciones críticas y las dependencias internas o externas claves, 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 Contingencias. 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 participar en las pruebas de continuidad del negocio con proveedores de servicios claves, debiendo informar de los resultados de éstas 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 del 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 del 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 conforme a lo establecido en 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 asegurará a la entidad las pistas de auditorías necesarias, de forma que existan pruebas para cualquier acción legal, las cuales deben estar disponibles por el tiempo que exija la Ley. Además, deben requerir informes 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 negocios, 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 éstos 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 de ejecutar los planes de acción para su tratamiento.

Artículo 56. Documentación de los Eventos de Riesgo Operacional. Las entidades deberán mantener informaciones suficientes y actualizadas sobre los eventos de riesgo operacional materializados, así como las pérdidas económicas o no económicas incurridas como consecuencia de estos. Se diseñarán las políticas, procedimientos de captura y entrenamiento al 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.

Párrafo. Considerando que las pérdidas no económicas no son contabilizadas, el monto de pérdida bruta para dichos eventos corresponderá a la estimación de pérdida generada como consecuencia del evento, como son pérdida de clientes, pérdida de eficiencia, entre otros, siempre que este monto pueda ser estimado.

Artículo 58. 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 59. 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 vigente.

Párrafo. La entidad deberá mantener registro de los eventos que no involucren pérdidas económicas o no económicas, es decir, cuando sus impactos sean evitados por controles, o cuando solo involucren lucro cesante. Estos registros deberán ser utilizados como fuente de información para indicadores y evaluaciones de riesgos.

Artículo 60. 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 61. 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 de la entidad para determinar cuáles informaciones de riesgo

…/

operacional develará 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 62. 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 63. 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**:**

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 64. 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 definido 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 del 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 65. 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 al 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, incumplimiento 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 66. 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 procedimiento 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 67. 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 68. Inventarios de Procesos. Las entidades deberán mantener inventarios actualizados de los procesos en funcionamiento, los cuales contarán como mínimo con la información siguiente: tipo de proceso, 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 69. 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. Estos deberán considerar los

…/

procesos de incorporación, permanencia y desvinculación del personal al servicio de la entidad, así como la devolución de recursos asignados. Asimismo, 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 70. 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 institucional.

Artículo 71. 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 72. 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, 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 73. 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 y tolerancia de riesgo. La gestión del riesgo tecnológico debe estar alineada con el marco de gestión del riesgo operacional y las metodologías de gestión de riesgo establecidas de conformidad con 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 las leyes y normativas aplicables. 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 tecnológico 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 a 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 riesgo tecnológico 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 74. 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, esto considerando las políticas de contingencia de la entidad y como parte de su plan de continuidad del 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 (PII, por sus siglas en inglés de *Personally Identifiable Information*) de sus colaboradores, clientes, usuarios y relacionados.

Párrafo IV. La gestión de la seguridad de la información, incluyendo los aspectos de ciberseguridad, deben estar asignadas 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 75. 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 a 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. La entidad mantendrá 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. La entidad mantendrá facilidades para la existencia de una base de información para el aprendizaje, a partir de las situaciones relacionadas a las incidencias.

Artículo 76. 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.

Párrafo I. Entre las acciones consideradas como importantes sobre las informaciones, deberán incluirse, sin limitarse, aquéllas 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 77. 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, sin ser limitativo, las estrategias, inversión y cumplimiento y marco de gobernanza de TI adoptado de la entidad.

Artículo 78. 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 79. Gestión de Inversión en Tecnología y Seguridad de la Información. La aprobación de inversiones y proyectos relacionados a las tecnologías, incluirán 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 80. 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 ser 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 forma y fondo 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 importantes costos ni contratiempos.

Artículo 81. 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 82. 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 Consejo, 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 83. Registro de las Contrataciones. Las entidades deberán llevar un registro de todas las contrataciones clasificadas por la materialidad, 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
SUPERVISIÓN DEL RIESGO OPERACIONAL

Artículo 84. 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 deben asegurarse de que existan procesos para garantizar que el riesgo operacional se gestione de manera adecuada e 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 no cumplan con la normativa vigente establecida por la Administración Monetaria y Financiera.

…/

Artículo 85. Supervisiones Especiales o Temáticas. La Superintendencia de Bancos podrá realizar supervisiones especiales o temáticas, cuando identifique factores comunes de exposición al riesgo operacional o de posibles vulnerabilidades.

TÍTULO VIII
NOTIFICACIÓN Y SOLICITUD DE NO OBJECIÓN PREVIA

Artículo 86. Notificaciones y Solicitud de No Objeción. Las entidades deberán solicitar la no objeción previamente y por escrito a la Superintendencia de Bancos, cuando se presente cualquiera de las situaciones siguientes:

1) Solicitud de No Objeción:

   a) Tercerización de actividad, función o servicios;

   b) Introducción de nuevos productos, servicios o canales;

   c) Sustitución o adquisición de nuevos sistemas informáticos, centros de procesamiento de datos, accesos externos a sistemas; y,

   d) La contratación de servicios de subagente bancario.

2) Notificación, tanto a la Superintendencia de Bancos como al Banco Central de los aspectos siguientes:

   a) Cambios en los recursos humanos de las áreas críticas, tales como gerentes de tecnología, auditoría y seguridad o conversión de sistemas;

   b) Cambios en manuales de políticas y procedimientos; y,

   c) Eventos materiales de riesgo operacional.

TÍTULO XI
REQUERIMIENTOS DE INFORMACIÓN

Artículo 87. 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 (MRI), con la periodicidad y en los plazos establecidos en dicho Manual.

Artículo 88. 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 89. 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, en caso de que ésta no se encuentre en el país.

Artículo 90. Informe de Eventos Materiales de Riesgo Operacional. Las entidades deberán informar por escrito a la Superintendencia de Bancos y al Banco Central, todos los eventos que afecten o pongan en riesgo la continuidad del negocio, los recursos de la entidad o de los ahorrantes, la calidad de los servicios o la imagen de la entidad, en un lapso no mayor a 3 (tres) días calendario desde la fecha del descubrimiento o desde la producción del incidente o evento de riesgo operacional.

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 X
DEL REQUERIMIENTO DE CAPITAL POR RIESGO OPERACIONAL

Artículo 91. 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 XI
DISPOSICIONES FINALES

Artículo 92. 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 93. **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 Núm.183-02 Monetaria y Financiera y el Reglamento de Sanciones vigente.

Artículo 94. 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. Otorgar un plazo de 30 (treinta) días, contado a partir de la fecha de la puesta en consulta de la presente Resolución, a los fines de recabar la opinión de los sectores interesados, sobre la modificación integral del Reglamento sobre Riesgo Operacional, aprobado mediante la Quinta Resolución dictada por la Junta Monetaria en fecha 2 de abril del 2009.

   Párrafo: Las opiniones a que se refiere este Ordinal, podrán ser remitidas por escrito a las Gerencias del Banco Central o de la Superintendencia de Bancos, o por vía electrónica, a través de los correos electrónicos fin.normativa@bancentral.gov.do y regulación@sb.gob.do

3. Esta Resolución deberá ser puesta en consulta, en virtud de las disposiciones del literal g) 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 3 de marzo del 2025.

-FIN-

…/