

REPÚBLICA DE PANAMÁ
SUPERINTENDENCIA DEL MERCADO DE VALORES

Acuerdo No. 1-2026
(De 28 de mayo de 2026)

"Que establece los Lineamientos Generales para la Gestión Integral de Riesgos"

LA JUNTA DIRECTIVA
En uso de sus facultades legales y

CONSIDERANDO

Que la Ley 67 de 1 de septiembre de 2011 reformó el Decreto Ley 1 de 8 de julio de 1999 y creó la Superintendencia del Mercado de Valores (en adelante, "la Superintendencia"), como organismo autónomo del Estado, con personería jurídica, patrimonio propio e independencia administrativa, presupuestaria y financiera.

Que la Junta Directiva, de conformidad con los artículos 5, 6, 10 (numeral 1), 19 y 20 del Texto Único de la Ley del Mercado de Valores (en adelante, el "Texto Único"), actúa como Máximo Órgano de consulta, regulación y fijación de las políticas generales de la Superintendencia y tiene entre sus atribuciones adoptar, reformar y revocar Acuerdos que desarrollen las disposiciones de la Ley del Mercado de Valores.

Que la Superintendencia, en virtud del artículo 3 del Texto Único, tiene como objetivo general la regulación, la supervisión y la fiscalización de las actividades del mercado de valores que se desarrollen en la República de Panamá o desde ella, propiciando la seguridad jurídica de todos los participantes del mercado y garantizando la transparencia, con especial protección de los derechos de los inversionistas.

Que, en ese orden de ideas, el artículo 323 del Texto Único establece que cuando la Superintendencia contemple adoptar un acuerdo, deberá considerar para determinar si la acción es necesaria y apropiada: (a) el interés público, (b) la protección de los inversionistas y (c) si la acción promueve la eficiencia, la competencia del mercado y la formación de capital.

Que el constante desarrollo y la creciente complejidad de los mercados financieros internacionales exigen que los participantes del mercado cuenten con mecanismos de control robustos, dinámicos y eficientes para proteger la integridad del sistema ante la materialización de diversos factores de riesgo.

Que para consolidar la competitividad, estabilidad y madurez de la plaza de valores panameña, resulta imperativo homologar nuestras normativas a los mejores estándares y prácticas internacionales en materia de administración y gestión de riesgos.

Que la adopción de lineamientos generales sobre la Gestión Integral de Riesgos (GIR) proporcionará a los regulados un marco de actuación unificado, permitiéndoles identificar, medir, monitorear, controlar, mitigar y reportar de manera oportuna los riesgos inherentes a sus operaciones.

Que, la implementación de políticas estandarizadas de gestión de riesgos fortalece el gobierno corporativo de las entidades reguladas, promueve una cultura de cumplimiento y mejora la confianza del público inversionista en la solidez del mercado de valores de la República de Panamá.

Que el presente acuerdo ha sido sometido al Procedimiento de Consulta Pública consagrado en el Título XV del Texto Único de la Ley del Mercado de Valores, específicamente en los artículos 323 y ss., cuyo plazo en una primera consulta pública fue del 22 de agosto hasta el 4 de octubre de 2019 y en una segunda consulta pública desde el 29 de mayo hasta el 14 de julio de 2025, según consta en el expediente de acceso público que reposa en la Superintendencia.

Que en virtud de lo anterior, la Junta Directiva de la Superintendencia, en uso de sus facultades legales;

ACUERDA:

ARTÍCULO PRIMERO: Adoptar los Lineamientos Generales para la Gestión Integral de Riesgos, para las entidades con licencia expedida por la Superintendencia, de conformidad con las siguientes disposiciones:

Capítulo I Aspectos Generales

Artículo 1. Ámbito de Aplicación.

Las disposiciones del presente Acuerdo serán aplicables a los siguientes regulados (en adelante “entidad con licencia” o “entidades con licencia”):

1. Administradoras de Inversiones.
2. Administradoras de Inversiones de Fondos de Pensiones y Jubilaciones.
3. Casas de Valores.
4. Organizaciones Autorreguladas.

Las disposiciones del presente Acuerdo se aplicarán de manera adicional y complementaria a lo establecido por los siguientes acuerdos reglamentarios: Acuerdo No. 6-2015 de 19 de agosto de 2015, referido a la prevención de los delitos de blanqueo de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva; Acuerdo No. 5-2018 de 21 de agosto de 2018, sobre Gestión del Riesgo de Tecnología de la Información; Acuerdo No. 6-2018 de 10 de octubre de 2018, que adopta principios de Buen Gobierno Corporativo y cualquier norma regulatoria relacionada con la materia que se vaya adoptando de tiempo en tiempo y cualquier otra que la Superintendencia determine en materia de gestión de riesgos.

Parágrafo. La Superintendencia recomienda como una medida prudencial a las entidades reguladas no incluidas en el ámbito de aplicación del presente Acuerdo, la utilización de los lineamientos contenidos en el presente documento como guía para la gestión adecuada de sus riesgos.

Artículo 2. Objetivos.

Este Acuerdo tiene como objetivo que las entidades con licencia apliquen los lineamientos, criterios y parámetros mínimos para el diseño e implementación de su Gestión Integral de Riesgos, en función del volumen y frecuencia de sus transacciones, el tipo y complejidad de sus operaciones.

La Gestión Integral de Riesgos es una responsabilidad conjunta y fundamental de la Junta Directiva, la Administración y el resto de los colaboradores de la entidad con licencia, que debe estar diseñada para identificar eventos potenciales que puedan afectar a la organización y gestionar de forma efectiva sus riesgos de acuerdo con su Apetito de Riesgo.

La Gestión Integral de Riesgos comprende las políticas, procedimientos y controles establecidos por la entidad con licencia, para identificar, evaluar, monitorear, administrar y mitigar sus riesgos.

Artículo 3. Definiciones.

1. **Apetito de Riesgo:** El Apetito de Riesgo es el nivel y tipo de riesgo, cuantitativo y cualitativo, que una entidad con licencia está dispuesta a asumir consciente y estratégicamente para alcanzar sus objetivos de negocio, dentro de su capacidad de capital, liquidez, solvencia, capacidades operativas y tolerancias regulatorias. Es un marco directivo que establece los límites superiores y la intensidad de exposición que la entidad con licencia acepta bajo condiciones normales y de estrés, considerando su modelo de negocio, su perfil de riesgos, su estrategia, su cultura organizacional y su capacidad para absorber pérdidas inesperadas sin comprometer su viabilidad.
2. **Capacidad de Riesgo:** El nivel máximo de riesgo que puede asumir una entidad con licencia dados sus recursos actuales, sus objetivos y sus obligaciones contractuales, sin incurrir en incumplimientos regulatorios, a fin de lograr sus objetivos y plan de negocio, sin comprometer su solvencia, viabilidad financiera o continuidad operativa.
3. **Calibración:** Es el proceso por el cual se mide el riesgo y se ajustan las premisas que se alineen a la realidad del riesgo identificado que tiene la entidad con licencia.
4. **Gestión Integral de Riesgos:** Es el proceso continuo y proactivo, supervisado por la Junta Directiva y ejecutado por la Administración, por el cual la entidad con licencia identifica, mide, monitorea, controla, mitiga e informa a las distintas áreas dentro de la entidad con licencia, los tipos de riesgo a los que se encuentra expuesta, de acuerdo con el volumen y frecuencia de sus transacciones, tipo y complejidad de sus operaciones. Su objetivo principal es alinear la toma de decisiones con la estrategia de negocio y el perfil de riesgo establecido.
5. **Órgano de Gestión de Riesgos:** Es el área administrativa especializada dentro de una entidad con licencia, encargada de diseñar y ejecutar las políticas y procedimientos para la gestión integral de riesgos. De acuerdo con la estructura definida por cada entidad con licencia, ésta puede ser una gerencia, unidad, persona natural o tercero.

6. **Pruebas de Tensión (stress test):** Las pruebas o ejercicios utilizados para evaluar el impacto de la exposición a un determinado tipo de riesgo ante situaciones o escenarios excepcionales pero posibles.
7. **Pruebas Retrospectivas (back testing):** Son un conjunto de pruebas o ejercicios destinados a evaluar el grado de precisión y la confiabilidad estadística de los resultados obtenidos a partir de un modelo interno de medición de riesgos.
8. **Riesgo Inherente:** Es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que de éste se hagan a su interior. El Riesgo Inherente es propio del trabajo o proceso, que no puede ser eliminado, pero sí mitigado.
9. **Riesgo Residual o Neto:** Nivel de riesgo que permanece después de aplicar todos los controles, mitigaciones y medidas de gestión diseñadas para reducir el Riesgo Inherente. El Riesgo Residual no puede ser eliminado completamente, solo gestionarse dentro de los parámetros de Apetito de Riesgo y Tolerancia al Riesgo definidos por la entidad con licencia.
10. **Tolerancia al Riesgo:** Es el margen aceptable de desviación respecto al Apetito de Riesgo establecido. Concretamente, delimita el rango dentro del cual cada uno de los riesgos puede fluctuar sin que se considere necesario adoptar medidas correctivas. Mientras que el Apetito de Riesgo establece el nivel deseado, la Tolerancia al Riesgo marca los límites operativos superiores e inferiores.

Capítulo II

Gestión Integral de Riesgos

Artículo 4. Cultura de Riesgo.

Las entidades con licencia deberán promover una cultura de riesgo que incluya:

1. Comunicación clara sobre el Apetito de Riesgo, la Capacidad de Riesgo y la Tolerancia al Riesgo.
2. Capacitación continua.
3. Incentivos alineados al riesgo.
4. Responsabilidad individual.

Artículo 5. Modelo de Tres Líneas de Defensa.

Las entidades con licencia deberán estructurar y mantener su sistema de Gestión Integral de Riesgos bajo un modelo de tres líneas de defensa:

1. **Primera línea (Negocio):** Responsable de identificar, gestionar y reportar los riesgos inherentes a sus actividades.
2. **Segunda línea (Riesgos y Cumplimiento):** Responsable de establecer metodologías, monitorear riesgos y asegurar el cumplimiento del Apetito de Riesgo.
3. **Tercera línea (Auditoría Interna):** Responsable de evaluar de forma independiente la eficacia del sistema de gestión de riesgos.

Artículo 6. Marco de la Gestión Integral de Riesgo.

La Gestión Integral de Riesgos deberá implementarse a través de un marco integral y estructurado de gestión de riesgos que incluya, al menos, los siguientes componentes:

1. **Ambiente Interno:** Comprende el entorno de la entidad con licencia que incluye la cultura y valores corporativos, la idoneidad técnica y moral de su personal, la estructura organizacional, y las condiciones para la delegación de facultades y asignación de responsabilidades, entre otros.
2. **Establecimiento de Objetivos:** Proceso por medio del cual se establecen los objetivos corporativos de la entidad con licencia, los cuales deben estar alineados con el Apetito por Riesgo y dentro de su Capacidad de Riesgo.
3. **Identificación de Riesgos:** Procedimientos y metodologías por las cuales se identifican los riesgos internos y externos, y que considera, según sea apropiado, los posibles eventos y escenarios asociados.
4. **Evaluación de Riesgos:** Proceso a través del cual se evalúa la probabilidad de ocurrencia y el impacto de los riesgos de a los que está expuesta una entidad con licencia, mediante técnicas cualitativas o y cuantitativas. Las entidades con licencia deberán garantizar la integridad, calidad y trazabilidad de datos, los controles sobre las fuentes de información y las validaciones periódicas.
5. **Plan de Mitigación de Riesgos:** El Plan de Mitigación de Riesgos deberá establecer las medidas preventivas o de control destinadas a reducir la probabilidad de ocurrencia del riesgo

o disminuir su impacto potencial antes de que el evento se materialice. Las estrategias de tratamiento pueden incluir la transferencia, reducción, aceptación o eliminación del riesgo, en función de su naturaleza, magnitud y del Apetito de Riesgo definido por la entidad con licencia. Cada estrategia debe ser evaluada y aplicada considerando el contexto operativo y los objetivos estratégicos de la entidad con licencia, con el propósito de fortalecer su capacidad de respuesta y asegurar una gestión eficaz del riesgo. El enfoque debe ser proactivo, con el objetivo de fortalecer los controles para evitar o limitar la materialización del riesgo.

6. **Plan de Respuesta a Riesgos:** El Plan de Respuesta a Riesgos debe establecer las acciones que han de ejecutarse cuando un riesgo se materializa o existe una alta probabilidad de que ocurra. Debe incluir los procedimientos de actuación, responsables y tiempos de respuesta. El enfoque es reactivo, orientado a contener el impacto del evento, a recuperar las operaciones y a restablecer la normalidad de la entidad con licencia.
7. **Control de Riesgos:** Es el proceso mediante el cual la entidad con licencia implementa controles y acciones destinadas a prevenir, reducir o mantener dentro de niveles aceptables la exposición a los riesgos identificados. Este proceso incluye la identificación, evaluación y tratamiento de los riesgos, considerando su probabilidad de ocurrencia y su impacto potencial.
8. **Información y Comunicación:** Se refiere a la capacidad de la entidad con licencia para generar, procesar y comunicar información e informes relevantes, confiables y oportunos, que permitan apoyar la toma de decisiones y el adecuado ejercicio de las funciones de supervisión y control. La información debe fluir de manera efectiva a través de los distintos niveles de la organización y hacia las partes interesadas, iniciando con la Administración y la Junta Directiva, asegurando transparencia, claridad y consistencia en la comunicación.
9. **Monitoreo:** Las entidades con licencia deberán evaluar periódicamente la suficiencia de capital en función de su perfil de riesgo, considerando los riesgos financieros y no financieros, los resultados de pruebas de tensión y el riesgo residual. El monitoreo implica la revisión continua de los riesgos y la efectividad de las medidas implementadas. Igualmente, hacer ajustes periódicos para mantener la Gestión Integral de Riesgos alineada con los objetivos de la entidad con licencia y la situación real del mercado.

Artículo 7. Tipos de Riesgos.

Para los efectos del presente Acuerdo, sin perjuicio de cualquier otro riesgo que pueda identificar la entidad con licencia y de lo establecido en otros acuerdos, se establecen las siguientes clasificaciones y tipos de riesgo:

1. RIESGOS FINANCIEROS Y DE VALUACIÓN

- 1.1 **Riesgo de Crédito:** Es la posibilidad de incurrir en pérdidas debido al incumplimiento total o parcial de las obligaciones contractuales por parte de contrapartes, emisores, deudores u otros obligados, así como al deterioro de su capacidad o voluntad de pago, en los términos y plazos acordados.
- 1.2 **Riesgo de Contraparte:** Es la posibilidad de incurrir en pérdidas cuando una contraparte en una operación financiera o contractual no pueda o no esté dispuesta a cumplir sus obligaciones en los términos, montos o plazos establecidos.
- 1.3 **Riesgo de Mercado:** Es la posibilidad de incurrir en pérdidas derivadas de movimientos adversos en los precios o en otras variables de mercado que afectan el valor de los activos, pasivos o instrumentos financieros mantenidos por la entidad con licencia, particularmente aquellos asociados a la cartera de negociación. Este riesgo comprende principalmente:
 - 1.3.1 **Riesgo de Precio:** Es la posibilidad de incurrir en una pérdida debido a variaciones adversas en el precio de mercado de un instrumento financiero o debido a la indeterminación del precio en un momento dado.
 - 1.3.2 **Riesgo de Tasa de Interés:** Es la posibilidad de incurrir en una pérdida debido a variaciones adversas en las tasas de interés, que afecten el valor de los instrumentos financieros o los flujos futuros de efectivo asociados a los mismos.
 - 1.3.3 **Riesgo de Tipo de Cambio:** Es la posibilidad de incurrir en una pérdida debido a variaciones adversas en la tasa de cambio entre distintas monedas.
- 1.4 **Riesgo de Liquidez:** Es la posibilidad de incurrir en pérdidas o enfrentar obstáculos para cumplir oportunamente con las obligaciones financieras debido a la incapacidad de obtener recursos líquidos suficientes o de convertir activos en efectivo en condiciones adecuadas de mercado. Este riesgo comprende:
 - 1.4.1 **Riesgo de Liquidez Financiera (o de Fondeo):** Es la posibilidad de incurrir en pérdidas derivadas de situaciones en las cuales la entidad con licencia no disponga de recursos líquidos suficientes para cumplir oportunamente con sus obligaciones financieras sin incurrir en costos significativos o afectar su situación financiera.

- 1.4.2 Riesgo de Liquidez de Mercado:** Es la posibilidad de incurrir en pérdidas derivadas de situaciones en las cuales un activo financiero no pueda venderse oportunamente o solo pueda venderse con descuentos significativos respecto a su valor razonable, debido a condiciones adversas o a la falta de profundidad del mercado.
- 1.5 Riesgo de Concentración:** Es la posibilidad de incurrir en pérdidas significativas derivadas de exposiciones concentradas en determinados clientes, contrapartes, sectores económicos, instrumentos financieros, mercados o regiones geográficas, que puedan afectar la solvencia o estabilidad financiera de la entidad con licencia.
- 1.6 Riesgo de Valuación:** Es la posibilidad de incurrir en pérdidas debido al uso de metodologías, modelos o supuestos inadecuados para la valoración de activos, pasivos o instrumentos financieros, lo que podría generar estimaciones inconsistentes con su valor económico real o con las condiciones prevalecientes del mercado.
- 1.7 Riesgo País:** Es la posibilidad de incurrir en pérdidas derivadas de condiciones políticas, económicas, legales o sociales adversas en un país determinado que puedan afectar la capacidad de cumplimiento de las obligaciones financieras por parte de los deudores o contrapartes ubicadas en dicha jurisdicción. Este riesgo comprende:
- 1.7.1 Riesgo de Transferencia:** Es la posibilidad de incurrir en pérdidas derivadas de condiciones en que los deudores de un país no puedan cumplir sus obligaciones en moneda extranjera debido a restricciones en la disponibilidad o transferencia de divisas, independientemente de su capacidad financiera individual.
- 1.7.2 Riesgo Político:** Es la posibilidad de incurrir en pérdidas derivadas de cambios o inestabilidad en el entorno político, institucional o regulatorio de un país que puedan afectar negativamente las inversiones o actividades de la entidad con licencia.
- 1.7.3 Riesgo Soberano:** Es la posibilidad de que un gobierno o entidad soberana de un país determinado no pueda o no esté dispuesto a cumplir sus obligaciones financieras.

2. RIESGOS OPERATIVOS, TECNOLÓGICOS Y LEGALES

- 2.1 Riesgo Operacional:** Es la posibilidad de incurrir en pérdidas procedentes de fallas o deficiencias en los procesos internos, en las personas, en los sistemas de información o como consecuencia de eventos externos. Incluye riesgos asociados a tecnología de la información, fraude, errores humanos y fallos en los controles internos.
- 2.2 Riesgo de Tecnología de la Información y Digitales:** Es la posibilidad de incurrir en pérdidas procedente de fallas, interrupciones, vulnerabilidades o uso inadecuado de las infraestructuras tecnológicas, sistemas informáticos, aplicaciones, redes o canales digitales que soportan las operaciones de la entidad con licencia.
- 2.3 Riesgo de Ciberseguridad:** Es la posibilidad de incurrir en pérdidas procedente de accesos no autorizados, ataques cibernéticos, vulneraciones de seguridad o compromisos de la confidencialidad, integridad o disponibilidad de los sistemas de información y datos de la entidad con licencia.
- 2.4 Riesgo de Continuidad del Negocio:** Es la posibilidad de incurrir en pérdidas procedentes de eventos internos o externos que interrumpan o afecten significativamente la continuidad de las operaciones de la entidad con licencia, comprometiendo la prestación de servicios o el cumplimiento de sus obligaciones.
- 2.5 Riesgo de Fraude y Corrupción:** Es la posibilidad de incurrir en pérdidas financieras, materiales o reputacionales procedentes de actos fraudulentos, deshonestos o corruptos cometidos por empleados, directivos, clientes o terceros.
- 2.6 Riesgo Legal:** Es la posibilidad de incurrir en pérdidas procedentes de la aplicación incorrecta o el incumplimiento de disposiciones legales o regulatorias, de litigios o resoluciones judiciales adversas, así como de deficiencias en la formalización o ejecución de contratos y actos jurídicos.
- 2.7 Riesgo Normativo:** Es la posibilidad de incurrir en sanciones legales, regulatorias, pérdidas financieras o daños reputacionales derivados del incumplimiento de las leyes, regulaciones o reglamentos del sector.
- 2.8 Riesgo de Cumplimiento BC/FT/FPADM:** Es la posibilidad de incurrir en sanciones legales, regulatorias, pérdidas financieras o daños reputacionales derivados del incumplimiento de la Ley 23 de 27 de abril de 2015 y sus reglamentaciones, así como de regulaciones sectoriales como el Acuerdo No. 6-2015 de 19 de agosto de 2015 o las que a futuro se establezcan, relativas con la prevención de los delitos de blanqueo de capitales, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva.

3. RIESGOS ESTRATÉGICOS Y DEL ENTORNO

- 3.1 Riesgo Estratégico:** Es la posibilidad de incurrir en pérdidas o de afectar la sostenibilidad del negocio debido a decisiones estratégicas inadecuadas, a la implementación deficiente de dichas decisiones o a la incapacidad de adaptarse oportunamente a cambios en el entorno competitivo, económico o regulatorio.

- 3.2 Riesgo de Reputación:** Es la posibilidad de incurrir en pérdidas económicas o de experimentar un deterioro en la confianza de clientes, inversionistas, autoridades o del público en general, como consecuencia de eventos, decisiones o conductas que afecten negativamente la imagen o credibilidad de la entidad con licencia, incluyendo prácticas inadecuadas de comercialización, conflictos de interés, información engañosa o incompleta y el uso indebido de información privilegiada.
- 3.3 Riesgo de Contagio:** Es la posibilidad de incurrir en pérdidas debido a la materialización de riesgos en entidades relacionadas, empresas del mismo grupo económico o entidades con las que exista una relación financiera o comercial significativa.
- 3.4 Riesgo Ambiental, Social y de Gobernanza (ASG):** Es la posibilidad de que factores ambientales, sociales o de gobernanza corporativa generen impactos negativos en la sostenibilidad, el desempeño financiero, la reputación o el cumplimiento regulatorio de la entidad con licencia.

La identificación, evaluación y gestión de los riesgos definidos en este artículo se realizará bajo un enfoque de materialidad, considerando su relevancia, probabilidad de ocurrencia e impacto potencial sobre la operación y los fondos administrados por la entidad con licencia. En consecuencia, la entidad con licencia determinará la importancia relativa de cada tipo de riesgo identificado en función de su modelo de negocio, la naturaleza de sus actividades y su perfil de riesgo institucional.

Artículo 8. Marco Operativo y Herramientas de Gestión.

Para robustecer la gestión integral de riesgos, las entidades con licencia deberán establecer y mantener políticas, procedimientos y controles operativos efectivos, aplicables a sus actividades diarias, así como a cada uno de los negocios, productos y servicios que desarrollen dentro del marco de las operaciones autorizadas.

Como apoyo a dichas políticas, las entidades con licencia deberán adoptar e implementar metodologías, modelos y herramientas técnicas de medición, monitoreo y control de riesgos, que resulten apropiadas y se mantengan actualizadas conforme a las mejores prácticas de la industria. Estas herramientas podrán incluir, entre otras, matrices de riesgo, análisis de sensibilidad, estructuras de límites y otros mecanismos de medición y seguimiento, que permitan identificar, medir, monitorear y controlar de manera integral todos los riesgos relevantes a los que se encuentra expuesta la entidad con licencia.

Artículo 9. Manual de Gestión Integral de Riesgos.

La entidad con licencia deberá contar con un Manual de Gestión Integral de Riesgos, el cual contendrá, como mínimo, los siguientes elementos:

1. Las políticas y procedimientos de gestión integral de riesgos, alineados con la estrategia de negocio, el tamaño, la naturaleza y la complejidad de las operaciones de la entidad con licencia.
2. Un instrumento o marco metodológico mediante el cual la entidad con licencia identifique, clasifique y agrupe de forma estructurada todos los tipos de riesgos relevantes a los que se encuentra expuesta, el cual deberá ser congruente con su estrategia de negocio, el tamaño, la naturaleza y la complejidad de sus operaciones.
3. La identificación de los riesgos inherentes asociados a cada una de las operaciones desarrolladas por la entidad con licencia, su importancia relativa en relación con los objetivos institucionales, y la protección de los intereses y activos de los clientes, así como los controles y medidas de mitigación correspondientes.
4. La definición de límites internos para los Riesgos Residuales más significativos, considerando la Capacidad de Riesgo de la entidad con licencia y su nivel de Tolerancia al Riesgo.
5. La elaboración de escenarios de riesgo que sean relevantes, incluyendo escenarios adversos o extremos, que puedan afectar las operaciones de la entidad con licencia, así como los correspondientes planes de mitigación o respuesta.
6. La definición de la estructura organizacional de gestión de riesgos, incluyendo la identificación de las áreas, cargos y personas responsables de la implementación de las políticas y procedimientos de gestión integral de riesgos, así como la descripción clara de sus funciones, responsabilidades y líneas de reporte.
7. La descripción de los mecanismos y procedimientos de reporte interno, mediante los cuales se comunique a la Administración, a la Junta Directiva y a otros grupos de interés relevantes, según corresponda, la información relacionada con la identificación, medición, monitoreo y mitigación de los riesgos.

Todo cambio, actualización o modificación del contenido del Manual de Gestión Integral de Riesgos, deberá ser revisado y aprobado por el Comité de Administración de Riesgos y ratificado por la Junta

Directiva, en atención a lo dispuesto en el numeral 3 del artículo 11 y en el numeral 7 del artículo 15 del presente Acuerdo.

El Manual de Gestión Integral de Riesgos deberá ser revisado al menos una vez al año. No obstante, ante cualquier cambio sustancial en el modelo de negocio, en la estructura operativa o en las condiciones de mercado que fundamentaron su diseño, la entidad con licencia procederá con su actualización inmediata, siguiendo el proceso de revisión, aprobación y ratificación antes descrito.

El Manual de Gestión Integral de Riesgos deberá mantenerse en todo momento a disposición de la Superintendencia.

Capítulo III

Estructura requerida y función de la Administración en la Gestión Integral de Riesgos

Artículo 10. Estructura Organizacional y de Soporte.

El soporte operativo y estratégico del proceso de Gestión Integral de Riesgos deberá estar conformado por la Junta Directiva, el Comité de Administración de Riesgos, el Ejecutivo Principal, el Órgano de Gestión de Riesgos, así como por aquellas otras instancias que, dentro de la organización, tengan responsabilidades equivalentes en materia de gestión de riesgos.

La estructura que sirva de soporte al proceso de Gestión Integral de Riesgos deberá incorporar, como mínimo, los siguientes elementos:

1. Una adecuada y claramente definida separación de funciones y responsabilidades entre las áreas de negocio y el Órgano de Gestión de Riesgos al que se refiere el artículo 16 del presente Acuerdo.
2. La certitud del adecuado funcionamiento del Comité de Administración de Riesgos, de conformidad con los parámetros y excepciones establecidos en los artículos 13, 14 y 15 del presente Acuerdo.
3. Mecanismos formales de comunicación y divulgación, que permitan transmitir de manera oportuna y efectiva los alcances y resultados del proceso de gestión de riesgos a las instancias relevantes de la organización.
4. La implementación de programas de capacitación periódica, orientados a asegurar la competencia del personal en materia de gestión de riesgos, los cuales deberán estar alineados con el modelo de negocio y los riesgos identificados por la entidad con licencia. Dichos programas deberán ser impartidos por proveedores que cumplan con los requisitos establecidos en el artículo 16 del presente Acuerdo.

Artículo 11. Responsabilidad de la Junta Directiva en la Gestión Integral de Riesgos.

La Junta Directiva de la entidad con licencia será responsable de asegurar el establecimiento, implementación y cumplimiento de las políticas y procedimientos necesarios para una adecuada gestión de los riesgos a los que se encuentra expuesta la entidad con licencia. De igual forma, deberá definir claramente los roles, responsabilidades y líneas de reporte correspondientes, evitando incompatibilidades o conflictos de interés con otras funciones o comités en los que participen sus miembros.

Para el adecuado cumplimiento de estas responsabilidades, la Junta Directiva deberá conocer, comprender y supervisar los riesgos de la entidad con licencia. A tal efecto, sus miembros deberán recibir capacitación periódica en materia de gestión de riesgos y podrán, cuando sea necesario, recurrir a asesoría especializada.

Entre las responsabilidades de la Junta Directiva en materia de Gestión Integral de Riesgos se incluyen, sin limitar, las siguientes:

1. Establecer y mantener un sistema de Gestión Integral de Riesgos acorde con su estrategia de negocio, el tamaño, la naturaleza y la complejidad de las operaciones de la entidad con licencia, en concordancia con su modelo de negocio y con lo establecido en el presente Acuerdo.
2. Aprobar los recursos necesarios para la adecuada Gestión Integral de Riesgos, incluyendo la estructura organizacional, infraestructura, metodología y personal apropiado.
3. Ratificar el Manual de Gestión Integral de Riesgos y otras políticas relacionadas, una vez hayan sido aprobadas por el Comité de Administración de Riesgos, así como sus respectivas modificaciones o actualizaciones.
4. Designar a los miembros del Comité de Administración de Riesgos o su equivalente.

5. Definir la estructura del Órgano de Gestión de Riesgo de la entidad con licencia, ya sea a través de una gerencia, unidad, persona natural o tercero, conforme a lo establecido en el artículo 16 del presente Acuerdo.
6. Evaluar y aprobar los planes de negocio, considerando los riesgos asociados a los mismos.
7. Establecer un sistema adecuado de delegación de facultades, separación y asignación de funciones, que permita una ejecución efectiva de las responsabilidades en materia de gestión de riesgos, así como un adecuado manejo de posibles conflictos de interés en la entidad con licencia.
8. Definir y aprobar el Apetito de Riesgo y la Capacidad de Riesgo de la entidad con licencia, de conformidad con su estrategia de negocio.
9. Promover una cultura de gestión de riesgos en toda la entidad con licencia, mediante capacitaciones periódicas y una adecuada difusión de las leyes y regulaciones vigentes, así como de las políticas y procedimientos en materia de gestión de riesgos.
10. Velar por el adecuado desempeño de la Gestión Integral de Riesgos, a través de los informes presentados por el Comité de Administración de Riesgos o su equivalente, así como de cualquier otra información que estime necesaria para la toma de decisiones.
11. Aprobar el Informe Anual de Evaluación de la Gestión Integral de Riesgos, que debe detallar la evaluación del sistema de Gestión Integral de Riesgos.
12. Velar por la actualización permanente del sistema de Gestión Integral de Riesgos, en función de los cambios en el entorno, el modelo de negocio y las actividades de la entidad con licencia.
13. Asegurar la capacitación continua, o al menos una vez al año, de sus miembros en materia de riesgos.
14. Asegurar que los nuevos miembros de la Junta Directiva reciban un proceso de inducción formal, que incluya un componente específico sobre la gestión de riesgos de la entidad con licencia.

Artículo 12. Responsabilidad del Ejecutivo Principal en la Gestión Integral de Riesgos de la entidad con licencia.

Además de las obligaciones dispuestas en el artículo 18 del Acuerdo No. 5-2014 de 1 de octubre de 2014 y en el artículo 15 del Acuerdo No. 6-2018 de 10 de octubre de 2018, el Ejecutivo Principal de la entidad con licencia es responsable de implementar, ejecutar y asegurar el cumplimiento de las directrices de la Gestión Integral de Riesgos de acuerdo con las políticas y procedimientos establecidos por la Junta Directiva, velando por su adecuada aplicación en toda la organización.

Capítulo IV

Función de los Órganos operativos en la Gestión Integral de Riesgos

Artículo 13. Comité de Administración de Riesgos.

La Junta Directiva deberá constituir un Comité de Administración de Riesgos, considerando la estrategia de negocio, el tamaño, la naturaleza y la complejidad de las operaciones de la entidad con licencia, con la finalidad de cumplir con las disposiciones del presente Acuerdo.

Cuando, por su naturaleza o tamaño, la entidad con licencia no cuente con la capacidad para constituir dicho Comité, sus funciones deberán ser asumidas por la Junta Directiva. El Ejecutivo Principal deberá notificar esta situación a la Superintendencia, la cual podrá objetarlo en función de la estructura, perfil de riesgos y tamaño de la entidad con licencia.

El Comité de Administración de Riesgos deberá estar integrado por un (1) miembro de la Junta Directiva que no esté involucrado en la gestión administrativa y operativa de la entidad. Adicionalmente, formarán parte del comité, el responsable del Órgano de Gestión de Riesgos, las instancias responsables de las áreas de negocio y cualquier otro ejecutivo que a tal efecto designe la junta directiva.

Los miembros del Comité deberán ser personas de reconocida honorabilidad y contar con formación y experiencia demostrable en materias relacionadas con el sector financiero. En su conjunto, deberán contar con un balance adecuado de habilidades, competencias y conocimientos que les permita analizar los riesgos financieros y no financieros que afectan a la entidad con licencia y a los fondos que administra.

El Comité de Administración de Riesgos deberá reunirse, al menos, cada tres (3) meses para el cumplimiento de sus fines y dejar constancia de todas sus sesiones mediante actas debidamente documentadas, en las cuales se consignen, al menos, los temas tratados, las discusiones sostenidas, los informes revisados, las recomendaciones formuladas y los acuerdos adoptados. Dichas actas podrán ser requeridas por la Superintendencia en cualquier momento.

Artículo 14. Integración de Comités.

La entidad con licencia podrá integrar las funciones del Comité de Administración de Riesgos y del Comité de Ética y Cumplimiento, en función de su tamaño, complejidad y estructura organizativa. En estos casos, deberá asegurarse que las actas identifiquen de manera clara y separada las deliberaciones y decisiones correspondientes a cada función. En estos casos, el Oficial de Cumplimiento solo deberá participar en la gestión pertinente de su responsabilidad en la materia que corresponda al Comité de Ética y Cumplimiento.

El Ejecutivo Principal deberá comunicar la integración de estos Comités a la Superintendencia, la cual podrá objetarla en función de los criterios antes señalados. Lo dispuesto en el presente artículo no será aplicable a las organizaciones autorreguladas, ni a las Administradoras de Inversiones de Fondos de Pensiones y Jubilaciones.

En caso de integración de los comités, la responsabilidad operativa de la Gestión Integral de Riesgos y la del Cumplimiento Normativo (AML/CFT) deberá recaer en personas distintas. El Oficial de Cumplimiento deberá mantener su independencia funcional y limitar su actuación a las materias de su competencia, sin asumir las funciones propias de la gestión de riesgos financieros u operativos de la entidad con licencia.

Artículo 15. Funciones del Comité de Administración de Riesgos.

El Comité de Administración de Riesgos tendrá las siguientes funciones:

1. Aprobar los procedimientos y metodologías para la gestión de los riesgos desarrollados por la Administración y recomendar para ratificación de la Junta Directiva.
2. Dar seguimiento continuo a las exposiciones a los distintos tipos de riesgos descritos en el artículo 7 del presente Acuerdo y comparar dichas exposiciones frente a los límites de Apetito de Riesgo y Capacidad de Riesgo aprobados, dando cuenta de ello a la Junta Directiva.
3. Identificar los riesgos emergentes y recomendar a la Junta Directiva las acciones y estrategias de correspondientes.
4. Evaluar el desempeño del Órgano de Gestión de Riesgos, ya sea una unidad, persona natural o tercero encargado de dicha función.
5. Aprobar los planes sobre políticas de gestión de riesgo, límites de exposición por tipo de riesgo, al igual que las estrategias propuestas por la Administración para la mitigación de los riesgos a los que está expuesta la entidad con licencia.
6. Aprobar los planes de contingencia y continuidad de negocio en marcha desarrollados por la Administración y enviarlos a la Junta Directiva para su ratificación.
7. Aprobar el Manual de Gestión Integral de Riesgos y sus actualizaciones y enviarlo a la Junta Directiva para su ratificación.
8. Revisar el Informe Anual de Evaluación de la Gestión Integral de Riesgos al que se refiere el artículo 21 del presente Acuerdo y emitir las recomendaciones correspondientes.
9. Cumplir otras funciones que le sean asignadas por la Junta Directiva en el ámbito de la Gestión Integral de Riesgos.

Artículo 16. Órgano de Gestión de Riesgos.

Las entidades con licencia deberán organizarse para administrar y gestionar los riesgos a los que se encuentran expuestos, para lo cual deberán contar con al menos un Órgano de Gestión de Riesgos, sea este una gerencia, unidad, persona natural o tercero. Dicho órgano será responsable de diseñar y ejecutar las políticas y procedimientos para la gestión integral de riesgos, de conformidad con lo establecido en el presente Acuerdo y en el Manual de Gestión Integral de Riesgos.

Para el cumplimiento de sus funciones, el Órgano de Gestión de Riesgos deberá ser completamente independiente de las áreas de negocios, operaciones, administrativas y de finanzas, dependiendo organizacionalmente del Comité de Administración de Riesgos. Este órgano no realizará, procesará o aprobará transacciones de negocios, operativas o administrativas, y deberá apoyar y asistir a las demás áreas de la entidad con licencia para la realización de una adecuada gestión de riesgos en sus áreas de responsabilidad. Su función deberá integrar los esfuerzos de la gestión del riesgo para la prevención del delito de blanqueo de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

El responsable del Órgano de Gestión de Riesgo debe poseer la experiencia y conocimientos técnicos que le permitan el adecuado cumplimiento de sus funciones. Para ello, deberá contar con al menos dos o más de los siguientes requisitos:

1. Haber obtenido licencia de Ejecutivo Principal otorgada por la Superintendencia.

2. Haber obtenido al menos una certificación en materia de gestión de riesgos, reconocida internacionalmente (ISO 31000, CFA, FRM, CFI, entre otras afines), distinta a la de Gestión de Riesgos AML.
3. Estudios universitarios en Gestión de Riesgos (Diplomado, Licenciatura, postgrado o maestría en Gestión de Riesgos).
4. Contar con experiencia comprobada, directa o indirecta, en el mercado de valores de al menos tres (3) años.
5. Contar con experiencia comprobada de al menos tres (3) años en gestión de riesgos en el sector financiero.

El ejercicio de funciones en el Órgano de Gestión de Riesgos por parte de las personas naturales con licencia de Ejecutivo Principal, expedida por la Superintendencia, es incompatible para ocupar otras funciones administrativas en la entidad con licencia al tenor de los artículos 5 y 6 del Acuerdo No. 5-2014 de 1 de octubre de 2014.

Artículo 17. Funciones del Órgano de Gestión de Riesgos.

El Órgano de Gestión de Riesgos tendrá las siguientes funciones:

1. Elaborar, implementar y mantener actualizado el Manual de Gestión Integral de Riesgos.
2. Identificar, monitorear, evaluar y controlar integralmente todos los riesgos que son relevantes para la entidad con licencia. Con tal propósito deberá:
 - a. Mantener modelos y sistemas de medición de riesgos concordantes con el volumen y frecuencia de sus transacciones, y con la naturaleza, tamaño y complejidad de sus operaciones, que reflejen con precisión el valor de las posiciones y su sensibilidad a los diversos factores de riesgo.
 - b. Evaluar regularmente dichos modelos y sistemas y plantear ante el Comité de Administración de Riesgos los ajustes requeridos. La periodicidad de estas evaluaciones deberá definirse en los manuales y procedimientos internos de la entidad con licencia.
 - c. Gestionar y requerir que las áreas responsables suministren de forma oportuna la información necesaria que será utilizada en los modelos y sistemas de medición de riesgos.
 - d. Ejecutar un programa periódico de Pruebas Retrospectivas (*back testing*), considerando el volumen y frecuencia de sus transacciones, la naturaleza, tamaño y complejidad de las operaciones de la entidad con licencia, entendido como un ejercicio sistemático de contraste entre las estimaciones de la exposición por tipo de riesgo generadas por los modelos internos y los resultados efectivamente observados para el mismo período de medición, con el fin de evaluar el desempeño del modelo y recomendar las calibraciones necesarias (actualización de parámetros, choques y horizontes temporales), así como los plazos para su implementación.
 - e. Realizar Pruebas de Tensión (*stress test*) sobre las exposiciones relevantes, considerando escenarios adversos y extremos acordes con la estructura del balance y el perfil de riesgo de la entidad con licencia.

La periodicidad inicial de las pruebas a las que se refieren los incisos “d” y “e” será al menos anual.

3. Llevar a cabo estimaciones de la exposición por tipo de riesgo.
4. Presentar al Comité de Administración de Riesgos, para su consideración, las metodologías, modelos, parámetros, herramientas y técnicas para la identificación, medición, análisis y mitigación de los riesgos a los que se encuentra expuesta la entidad con licencia.
5. Verificar la observancia de los límites de exposición globales y específicos, así como los niveles aceptables de Apetito de Riesgo y Tolerancia al Riesgo por tipo de riesgo, desglosados por unidad de negocio o factor de riesgo, causa u origen de éstos, utilizando para tal efecto los modelos, parámetros y escenarios aprobados para la medición y control de riesgo.
6. Proporcionar al Comité de Administración de Riesgos los informes periódicos que incluyan al menos lo siguiente:
 - a. La exposición a los diferentes riesgos que son relevantes para la entidad con licencia, con la periodicidad que se le haya determinado.
 - b. El impacto sobre la suficiencia de capital que conlleva la toma de riesgos por la entidad con licencia, considerando los análisis de sensibilidad bajo diferentes escenarios (*stress testing*), incluyendo eventos extremos.
 - c. Las desviaciones que se presenten con respecto a los límites de exposición y a los niveles de Apetito de Riesgo establecidos.
 - d. Recomendaciones de acciones correctivas que pueden implementarse para subsanar desviaciones identificadas con respecto a los límites de exposición y niveles de Tolerancia al Riesgo autorizados.

- e. Análisis histórico y de tendencias de los riesgos asumidos por la entidad con licencia.
7. Dar seguimiento a los acuerdos del Comité de Administración de Riesgos e informar al mismo sobre los avances.
8. Elaborar y presentar al Comité de Administración de Riesgos o su equivalente los procedimientos y las metodologías para la valoración, medición y control de los riesgos de nuevas operaciones, productos y servicios, así como la identificación de los riesgos implícitos que presentan.
9. Preparar el “Informe Anual de Evaluación Anual de la Gestión Integral de Riesgos” conforme a lo establecido en el artículo 21 del presente Acuerdo.
10. Velar porque la calidad e integridad de la información a ser presentada al Comité de Administración de Riesgos y a la Superintendencia sea óptima y se realice oportunamente, respetando los canales regulares existentes. En este contexto, la entidad con licencia deberá informar a la Superintendencia inmediatamente tenga conocimiento de cualquier circunstancia de riesgo que pueda afectar significativamente su situación patrimonial, su solvencia y/o su liquidez. Para este fin, deberá mantener una debida coordinación con el Oficial de Cumplimiento, salvaguardando cada uno la observancia de sus responsabilidades.
11. Ejercer cualquier otra función que le requiera el Comité de Administración de Riesgos en el ámbito de sus competencias.

Artículo 18. Delegación de las Funciones del Órgano de Gestión de Riesgos a Terceros.

Las entidades con licencia podrán tercerizar las funciones de su Órgano de Gestión de Riesgos considerando el tamaño, la naturaleza, la complejidad de sus operaciones y su estructura organizacional. Para ello, deberán notificar previamente por escrito a la Superintendencia a través de su Ejecutivo Principal, detallando los motivos y el perfil del proveedor (persona natural o jurídica), quien debe cumplir con los requerimientos del artículo 16 de este Acuerdo.

De igual forma, la tercerización estará sujeta a las siguientes disposiciones:

1. Los contratos suscritos con los proveedores de estos servicios deberán incluir cláusulas que garanticen de manera explícita el acceso inmediato, total y sin restricciones tanto a la entidad con licencia como de la Superintendencia a toda la documentación, datos e información relacionada con las funciones tercerizadas. Esta obligación aplica, independientemente del formato, medio o soporte en que se encuentre la información. De igual forma, el contrato debe contener disposiciones sobre la protección de la confidencialidad de la información tanto de la entidad con licencia como la de sus clientes.
2. El tercero deberá participar en las reuniones del Comité de Administración de Riesgo o su equivalente, con derecho a voz. En caso de que dicho comité se encuentre integrado con otros comités, su participación se circunscribirá únicamente a los temas relacionados con las funciones tercerizadas bajo su responsabilidad.
3. El tercero deberá reportar al Comité de Administración de Riesgo o su equivalente y será responsable de ejecutar las funciones delegadas conforme a lo establecido en el presente Acuerdo.

Para preservar la independencia y evitar conflictos de interés, las entidades con licencia no podrán tercerizar dichas funciones en personas naturales o jurídicas que presten servicios de auditoría externa de sus estados financieros.

Las entidades con licencia mantendrán en todo momento la responsabilidad del cumplimiento de las obligaciones establecidas en el presente Acuerdo, aun cuando las funciones hayan sido tercerizadas.

Artículo 19. Grupos Financieros o Económicos.

Aquellas entidades con licencia que pertenezcan a un grupo financiero o grupo económico podrán optar por centralizar a nivel del grupo la ejecución de las funciones operativas previstas en el presente Capítulo; entiéndase, las del Comité de Administración de Riesgos y las del Órgano de Gestión de Riesgos, debiendo cumplir en todo momento con las siguientes condiciones:

1. Asegurar que las funciones y obligaciones del Comité de Administración de Riesgos y del Órgano de Gestión de Riesgos incluyan, como mínimo, las establecidas en el presente Acuerdo, diferenciando claramente los asuntos correspondientes a cada entidad subsidiaria o afiliada. Dichas distinciones deberán quedar debidamente documentadas en las actas de los respectivos comités.
2. Definir expresamente las funciones operativas que serán ejecutadas a nivel del grupo, las cuales deberán contar con la aprobación previa de la Junta Directiva de la entidad con licencia.

3. Asegurar que el soporte que se reciba por parte del grupo no afecte el adecuado funcionamiento del sistema de Gestión Integral de Riesgos que la entidad con licencia debe mantener, conforme a las disposiciones previstas en el presente Acuerdo.
4. La Junta Directiva de la entidad con licencia mantendrá la responsabilidad de las decisiones que se adopten respecto al sistema de Gestión Integral de Riesgos.
5. Cuando las funciones y obligaciones del Órgano de Gestión de Riesgos y/o del Comité de Administración de Riesgos se ejecuten a nivel de grupo, se deberán cumplir integralmente todas las disposiciones establecidas en este Acuerdo para la entidad con licencia.
6. El Comité de Administración de Riesgos a nivel de grupo deberá asegurar la participación de al menos un director que represente a la entidad con licencia.
7. El Órgano de Gestión de Riesgos debe contar con al menos una persona que cumpla con los requisitos establecidos en el artículo 16 del presente Acuerdo.

Las entidades con licencia que opten por este modelo deberán notificar previamente por escrito a la Superintendencia, a través de su Ejecutivo Principal.

Cuando lo estime necesario, la Superintendencia podrá, en función del tamaño, naturaleza, complejidad de las operaciones o perfil de riesgo de la entidad con licencia, requerir que las funciones de gestión de riesgos sean ejecutadas a nivel individual.

Capítulo V

Responsabilidad de la Auditoría Interna en la Gestión Integral de Riesgos

Artículo 20. Función de la Auditoría Interna para la Gestión Integral de Riesgos.

El área de Auditoría Interna deberá evaluar de forma independiente la eficacia del sistema de Gestión Integral de Riesgos, incluyendo el cumplimiento de las políticas, procedimientos y controles establecidos. Dicha evaluación deberá formar parte de las actividades contempladas en el Plan Anual de Auditoría Interna.

El área de Auditoría Interna deberá emitir, al menos, un informe anual dirigido a la Junta Directiva que contenga los resultados de su evaluación, así como las recomendaciones correspondientes para el fortalecimiento del sistema de Gestión Integral de Riesgos. Los informes deberán mantenerse a disposición de la Superintendencia.

La función de Auditoría Interna deberá ser independiente de las áreas operativas, de negocio y de la administración, tanto desde el punto de vista funcional como organizacional. Ante la ausencia de un auditor interno a tiempo completo, se podrá tercerizar sus funciones con un auditor externo independiente. En ningún caso, esta función deberá ser desempeñada por la persona natural o jurídica responsable de la auditoría externa de los estados financieros de la entidad.

Capítulo VI

Sistema de Información

Artículo 21. Informe Anual de Evaluación de la Gestión Integral de Riesgos.

Las entidades con licencia deberán remitir a la Superintendencia, dentro de los seis (6) meses, posteriores al cierre del periodo fiscal, el “Informe Anual de Evaluación de la Gestión Integral de Riesgos”, el cual deberá ser preparado por el Órgano de Gestión de Riesgo, revisado por el Comité de Administración de Riesgo y debidamente aprobado por la Junta Directiva.

Dicho informe deberá contener, como mínimo, lo siguiente:

1. La estructura organizacional y la identificación de las personas responsables de la gestión integral de riesgos de la entidad con licencia.
2. La descripción de las políticas que han sido actualizadas para la Gestión Integral de Riesgos, así como un análisis del grado de cumplimiento de estas.
3. La matriz integral de riesgos detallando los riesgos relevantes a los que está expuesta la entidad con licencia. De igual forma, deberá incluir:
 - a. El análisis de los principales riesgos asumidos durante el período reportado y las medidas adoptadas para su gestión;
 - b. Los principales incidentes y eventos de pérdida registrados con su correspondiente análisis y seguimiento;
 - c. El análisis de los indicadores asociados al Apetito de Riesgo Capacidad de Riesgo;
 - d. La descripción de las metodologías, modelos, sistemas y herramientas utilizadas para la medición y gestión de los riesgos.

4. La descripción de las principales acciones de control y evaluaciones especiales realizadas, con respecto a los distintos riesgos que enfrenta la entidad con licencia, explicando las medidas adoptadas como resultado de las conclusiones de cada informe.
5. La descripción de las diferentes actividades de capacitación realizadas en materia de Gestión Integral de Riesgos.
6. Los proyectos y mejoras en materia de gestión de riesgos previstos para el siguiente ejercicio contable.
7. Las conclusiones generales y recomendaciones sobre la gestión de riesgos de la entidad con licencia.

Artículo 22. Información para la Superintendencia del Mercado de Valores.

La Superintendencia podrá requerir a las entidades con licencia cualquier información adicional que considere necesaria para la adecuada supervisión de la Gestión Integral de Riesgos y de cada uno de los riesgos específicos a los que se encuentre expuesta cada entidad con licencia.

Las entidades con licencia deberán tener en todo momento a disposición de la Superintendencia todos los documentos, registros, archivos en formato físico, digital o cualquier otro medio referido en el presente Acuerdo, así como los informes de control de sus auditorías internas. Lo señalado también abarca los documentos recibidos o generados por el Comité de Administración de Riesgos, o su equivalente, y la identificación del personal responsable de dicha gestión, con el fin de atender oportunamente las consultas o requerimientos del regulador.

Capítulo VII Disposiciones finales

Artículo 23. Adecuación de Códigos de Conducta.

Las entidades con licencia tendrán doce (12) meses, a partir de la promulgación del presente Acuerdo, para adecuar sus Códigos de Conducta en lo que corresponda, en relación con las nuevas disposiciones sobre gestión integral de riesgos incorporadas por el presente Acuerdo.

Artículo 24. Sanciones.

El incumplimiento de lo establecido en el presente Acuerdo se sancionará de conformidad con lo dispuesto en la Ley de Mercado de Valores.

ARTÍCULO SEGUNDO: MODIFICAR el Artículo 2 del Acuerdo No. 5-2018 de 21 de agosto de 2018, que establece los Lineamientos Generales para la Gestión de Riesgo de Tecnología de la Información, el cual quedará así:

Artículo 2. Definiciones

Para los propósitos del presente Acuerdo, los siguientes términos se entenderán de la siguiente manera:

- a) **Contingencia:** Situación potencial derivada de la posible materialización de un evento de riesgo relacionado con los sistemas, infraestructura, servicios o información tecnológica, cuya ocurrencia, aunque incierta, puede afectar la continuidad, disponibilidad, integridad o confidencialidad de las operaciones de la entidad, y que requiere la definición de medidas de respuesta, recuperación y mitigación dentro del marco de la Gestión Integral de Riesgos. La contingencia no elimina el riesgo, pero permite reaccionar de forma rápida y eficazmente para reducir su impacto.
- b) **Gobierno de la Tecnología de la Información:** Conjunto de procesos, responsabilidades, políticas, procedimientos, relaciones y controles que apoyan las metas del negocio, optimizan las inversiones y administran los riesgos y oportunidades asociados a la tecnología de la información, facilitando el logro de los objetivos y planes establecidos por las entidades con Licencia.
- c) **Incidente:** Cualquier evento tecnológico o no, externo o interno, que no forma parte de la operación normal de un servicio y que causa o pueda causar, una interrupción o una reducción de la calidad del mismo.
- d) **Información:** Cualquier forma de registro electrónico, digital, óptico, magnético o en otros medios similares, susceptible de ser reproducida, procesada, distribuida o almacenada e impresa.
- e) **Plan de continuidad de negocios:** Conjunto documentado de políticas, procedimientos, controles y recursos establecidos por la entidad con licencia para asegurar la continuidad, recuperación y oportuna reanudación de sus

funciones, procesos y servicios críticos ante la ocurrencia de interrupciones que puedan afectar sus operaciones normales, con el fin de limitar las pérdidas, proteger los activos e información, preservar la confianza del mercado y garantizar el cumplimiento de sus obligaciones regulatorias y contractuales. Este plan debe definir de manera precisa cómo la entidad va a reaccionar y a operar durante y después de un incidente que afecte sus operaciones.

- f) **Plan de recuperación de desastres:** Es un plan creado por una entidad que contiene instrucciones detalladas acerca de cómo responder a incidentes no planificados como desastres naturales, cortes de electricidad, ataques cibernéticos y cualquier otro evento disruptivo. El plan incluye estrategias o procedimientos para minimizar los efectos de un desastre y permitir que una entidad continúe operando o reanude rápidamente las operaciones importantes. El plan de recuperación de desastres busca restablecer los sistemas y servicios de la tecnología de la información lo antes posible después de un evento crítico, reduciendo al mínimo el impacto en la organización.
- g) **Procedimiento:** Método o sistema estructurado donde es detallada la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.
- h) **Riesgo de tecnología de la información:** Toda posible ocurrencia de daños, interrupción, alteración o fallas derivadas del uso de la Tecnología de la Información que soporta los procesos críticos de la entidad y que conlleve a una pérdida económica, material o de negocio.
- i) **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas, que buscan la confidencialidad, integridad y disponibilidad de la información en sí y de los demás recursos informáticos de la entidad.
- j) **Tecnología de la Información o TI:** Conjunto de instrumentos tecnológicos que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro, acceso y presentación de información.

ARTÍCULO TERCERO: MODIFICAR el Artículo 9 del Acuerdo No. 5-2018 de 21 de agosto de 2018, que establece los Lineamientos Generales para la Gestión de Riesgo de Tecnología de la Información, el cual quedará así:

Artículo 9. Plan de continuidad de negocios y de recuperación de desastres.

Las entidades con licencia deberán contar con un plan de continuidad de negocios para la Tecnología de la Información y de recuperación de desastres debidamente aprobado por el Comité de Administración de Riesgos y ratificado por la Junta Directiva, en razón del tamaño, necesidades y estructura organizativa de la entidad con licencia, que tendrá como objetivo principal brindar respuestas efectivas que garanticen la continuidad en las actividades de servicios y del negocio ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en sus operaciones.

Este plan deberá ser probado al menos una vez al año y deberá contemplar como mínimo lo siguiente:

1. Objetivo del Plan.
2. Procesamiento alternativo, incluyendo el debido respaldo de la información y los sistemas, incluyendo sitio alternativo, de acuerdo al tamaño, actividades autorizadas o naturaleza del negocio.
3. Identificación de los recursos críticos de la Tecnología de la Información.
4. Identificación del impacto por la interrupción de los servicios críticos.
5. Pruebas de resistencia diseñadas para mitigar el impacto de una interrupción mayor de las funciones y de los procesos claves del negocio (tiempos permisibles de interrupción de los servicios).
6. Respuesta a los inversionistas, clientes, usuarios, proveedores y demás grupos de interés.
7. Identificación, descripción de responsabilidades y funciones del personal clave que ejecutará el plan.
8. Capacidad de la recuperación de los servicios críticos de TI.
9. Programación y ejecución anual de pruebas identificadas en el Plan de Contingencia, así como su actualización conforme a los resultados obtenidos en dichas pruebas.

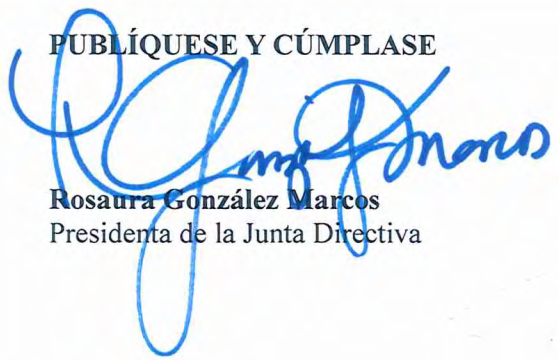
Los resultados obtenidos de las pruebas ejecutadas deberán ser notificados al Ejecutivo Principal y a la Junta Directiva de la entidad.

ARTÍCULO CUARTO (VIGENCIA): Las disposiciones contenidas en el presente Acuerdo entrarán en vigencia a partir de su promulgación en la Gaceta Oficial y las entidades con licencia tendrán doce (12) meses para su implementación.

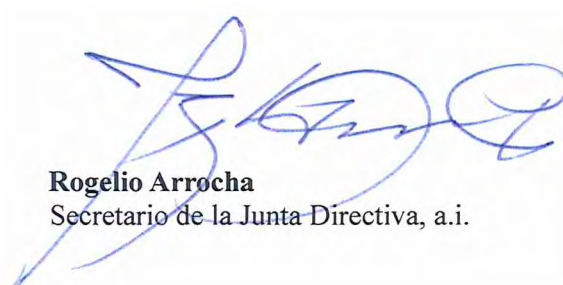
Al finalizar el plazo anterior, deberán haber quedado definidas y efectivamente establecidas las instancias de la Gestión Integral de Riesgos a que se refiere el presente Acuerdo, con su respectiva normativa interna debidamente aprobada.

La Superintendencia podrá solicitar a las entidades con licencia, durante los doce (12) meses indicados, el cronograma de trabajo que evidencie el avance de la implementación del presente Acuerdo.

PUBLÍQUESE Y CÚMPLASE



Rosaura González Marcos
Presidenta de la Junta Directiva



Rogelio Arrocha
Secretario de la Junta Directiva, a.i.

