REPÚBLICA DE PANAMÁ
SUPERINTENDENCIA DEL MERCADO DE VALORES

Acuerdo No. -2025
(De___ de _____de 2025)

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

LA JUNTA DIRECTIVA
En uso de sus facultades legales y

CONSIDERANDO

Que mediante la Ley 67 de 1 de septiembre de 2011, se crea la Superintendencia del Mercado de Valores como organismo autónomo del Estado, con personería jurídica, patrimonio propio e independencia administrativa, presupuestaria y financiera; con competencia privativa para regular y supervisar a los emisores, sociedades de inversión, intermediarios y demás participantes del mercado de valores.

Que la Asamblea Nacional expidió el Texto Único que comprende el Decreto Ley No. 1 de 1999 y el Título II de la Ley 67 de 2011, y sus leyes reformatorias, en adelante (Texto Único).

Que el artículo 3 del Texto Único establece que la Superintendencia tiene como objetivo general la regulación, supervisión y fiscalización de las actividades del mercado de valores que se desarrollen en la República de Panamá

Que el artículo 10 del Texto Único faculta a la Junta Directiva para "adoptar, reformar y revocar acuerdos que desarrollen las disposiciones de la Ley del Mercado de Valores".

Que la Superintendencia del Mercado de Valores desea implementar una política de Supervisión Basada en Riesgos (SBR), a fin de fortalecer su metodología de supervisión, haciéndola más eficiente, buscando mejorar la protección del público inversionista.

Que es necesario establecer los criterios mínimos prudenciales para la identificación y administración de los distintos riesgos que enfrentan las entidades con Licencia expedida por la Superintendencia, a fin de contribuir favorablemente a la estabilidad y eficiencia del Mercado de Valores.

Que este Acuerdo ha seguido el procedimiento de consulta pública contenido en el Título XV del Texto Único, referente al "Procedimiento Administrativo para la Adopción de Acuerdos", según se puede verificar en el expediente de acceso público contenido en los archivos de la Superintendencia.

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

ACUERDA:

ARTÍCULO PRIMERO: Adoptar los Lineamientos Generales para la Gestión Integral de Riesgos (GIR) que deben seguir las Casas de Valores, Administradoras de Inversiones, Administradoras de Inversión de Fondos de Pensiones y Jubilaciones, Administradoras de Inversiones de Fondos de Cesantía y las Organizaciones Autorreguladas, para los efectos de este Acuerdo "entidades con licencia".

Capítulo I
Aspectos Generales

Artículo 1. Ámbito de Aplicación.

Las disposiciones del presente acuerdo serán aplicables a las entidades con licencia, con el objetivo de establecer los criterios mínimos para la evaluación y gestión integral de los distintos riesgos que enfrentan.

La presente norma se ejecuta de manera adicional de lo dispuesto en materia de gestión de riesgos por el 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.

En el caso de bancos oficiales con licencia de casa de valores, las disposiciones del presente Acuerdo les serán aplicables en la medida que no sean contrarias a las disposiciones legales y reglamentarias que rigen dichas instituciones.

Parágrafo. La Superintendencia del Mercado de Valores recomienda como una medida prudencial a las entidades reguladas que se encuentran fuera del ámbito de aplicación del presente Acuerdo, la adopción voluntaria o la utilización como guía de las disposiciones contenidas en el presente documento para la gestión adecuada de sus riesgos.

Artículo 2. Objetivos.

El objetivo de este Acuerdo es que las entidades con licencia apliquen los lineamientos, criterios y parámetros generales mínimos que debe implementar en el diseño y aplicación de su Gestión Integral de Riesgos, el cual debe abarcar la identificación, evaluación, respuesta, control, información y comunicación, así como el monitoreo de los riesgos a los que están expuestas, en función del volumen y frecuencia de sus transacciones, y el tipo, y complejidad de las operaciones que ejecutan.

Artículo 3. Definiciones.

1. Ambiente interno: El entorno 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. Apetito de Riesgo: El nivel y los tipos de riesgos que una entidad con licencia está dispuesta a asumir en relación con los activos propios y de terceros que administra, aprobados por el Órgano de Dirección con antelación y dentro de su Capacidad de Riesgo, para alcanzar sus objetivos estratégicos y plan de negocio.
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.
4. Conflictos de interés: Debe entenderse de conformidad con la definición establecida en el Acuerdo 6-2018 del 10 de octubre de 2018.
5. Control de riesgo: Proceso que busca asegurar que las medidas de respuesta al riesgo y mitigantes se cumplan de acuerdo con lo previsto.
6. Dato Personal: De acuerdo con lo establecido en el numeral 9 del artículo 4 de la Ley 81 de 26 de marzo de 2019, se entenderá como cualquier información concerniente a personas naturales, que las identifica o las hace identificables.
7. Días: Los días calendario, salvo indicación en contrario.
8. Director independiente: Debe entenderse de conformidad con la definición establecida en el Acuerdo No.6-2018 del 10 de octubre de 2018.
9. Establecimiento de objetivos: Proceso por el que se determinan los objetivos que deben encontrarse de acuerdo con el apetito por riesgo y dentro de su capacidad de riesgos.
10. Evaluación de riesgos: Proceso por el que se evalúa la probabilidad de ocurrencia e impacto de los riesgos de una entidad con licencia, operaciones, del portafolio, de los productos o servicios; mediante técnicas cualitativas o cuantitativas o una combinación de ambas.
11. Gestión Integral de Riesgos (GIR): Conjunto de políticas, procedimientos y metodologías, por las cuales la entidad con licencia identifica, mide, monitorea, controla, mitiga e informa a las distintas áreas dentro de la entidad, los tipos de riesgo a los que se encuentra expuesta de acuerdo al volumen y frecuencia de sus transacciones, tipo y complejidad de sus operaciones.
12. 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.

a.e.

13. Información y comunicación: Proceso por el que se informa a la Junta Directiva y a la Administración, así como a los grupos de interés según corresponda.
14. Medidas de mitigación: Conjunto de acciones tomadas por las entidades con licencia para gestionar técnicamente cualquiera de los riesgos que surjan, de forma que se minimicen las potenciales pérdidas derivadas de su materialización.
15. Monitoreo: Proceso de control periódico del adecuado funcionamiento de la gestión integral de riesgos.
16. Plan de continuidad de negocios: Debe entenderse de conformidad con la definición establecida en el Acuerdo 5-2018 de 21 de agosto de 2018.
17. Plan de recuperación de desastres: Debe entenderse de conformidad con la definición establecida en el Acuerdo 5-2018 de 21 de agosto de 2018.
18. 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.
19. Pruebas de Tensión: 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.
20. Pruebas Retrospectivas: Las pruebas o ejercicios utilizados para evaluar el grado de precisión o confiabilidad estadística de los resultados obtenidos de un modelo interno de medición de riesgo.
21. Respuesta al riesgo: Proceso por el que se opta por aceptar el riesgo, disminuir la probabilidad de ocurrencia, mitigar, disminuir el impacto, transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo con el nivel de apetito y límites de riesgo definidos.
22. Riesgo: Es la posibilidad de ocurrencia de eventos que impacten negativamente sobre los objetivos de la entidad con licencia o su situación financiera.
23. Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de la respuesta al riesgo. 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.
24. Riesgo residual o neto: Nivel resultante de riesgo después de aplicar la respuesta o realizar gestiones de mitigación al riesgo sobre el riesgo inherente.
25. 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 con licencia.
26. Tolerancia de Riesgo: La capacidad máxima de riesgo que una entidad con licencia puede asumir en relación con los activos propios y de terceros administrados, considerando su gestión integral de riesgos, medidas de control, limitaciones regulatorias, base de capital u otras variables de acuerdo con sus características.

Capítulo II
Gestión Integral de Riesgos

Artículo 4: Alcance.

La Gestión Integral de Riesgos (GIR) es efectuada por la Junta Directiva, la Administración y el resto de los colaboradores en toda entidad con licencia, diseñada para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos de acuerdo con su apetito por el riesgo y proporcionar una seguridad razonable para el logro de sus objetivos.

La Gestión Integral de Riesgos (GIR) comprende a todas las operaciones, procesos y unidades organizativas de la entidad, que se establecen con el fin de identificar, evaluar, controlar y monitorear sus riesgos. Es responsabilidad de cada entidad contar con políticas, normas y procedimientos, estructuras organizativas, manuales y otros instrumentos que coadyuven a la gestión integral de sus riesgos.

La entidad con licencia debe diseñar y aplicar un sistema de gestión integral de riesgos, según el tamaño y complejidad de sus operaciones, así como al entorno macroeconómico e institucional que afecta a los mercados en los que ésta realiza sus operaciones; para lo cual deberá estructurar un marco de gestión de riesgos que incluya cuando menos lo siguiente:

1. Ambiente interno
2. Establecimiento de objetivos
3. Identificación de riesgos
4. Evaluación de riesgos
5. Plan de mitigación de riesgos
6. Respuesta al riesgo
7. Control
8. Información y comunicación
9. Monitoreo

Artículo 5: Tipo 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 entiende por:

1. Riesgo Ambiental, Social y de Gobernanza: Son aquellos que surgen de factores Ambientales, Sociales y de Gobernanza que una empresa debe enfrentar y gestionar de acuerdo con su modelo de negocio, así como de su entorno (interno y externo).
2. Riesgo de ciberseguridad: son las probabilidades de que una amenaza o un ataque cibernético se materialice y que los sistemas digitales o informáticos de una entidad quede expuesta o sea vulnerada.
3. Riesgo de concentración: Concentración en activos, pasivos u operaciones dentro o fuera de balance, que podría causar pérdidas significativas en la entidad las cuales afectarían la solvencia o capacidad de mantener sus operaciones de manera regular.
4. Riesgo de contagio: Es la posibilidad de pérdida que la misma pueda sufrir directa o indirectamente debido a ocurrencias adversas en empresas o personas con las que se mantiene una vinculación comercial o financiera materialmente relevante para el negocio y actividades de la entidad. Puede referirse a empresas o personas de su propio grupo económico, o de empresas que realicen actividades similares en la plaza de su ubicación o en el sistema financiero de otro país.
5. Riesgo de continuidad del negocio: Es el riesgo relacionado a la posibilidad de que las operaciones de una entidad se vean afectadas por situaciones internas o externas, tales como afectaciones financieras o eventos de fuerza mayor o casos fortuitos.
6. Riesgo de crédito: Situación donde una contraparte no pueda cumplir sus obligaciones financieras en la forma y/o plazos previstos.
7. Riesgo de cumplimiento BC/FT/FPADM: Es la exposición potencial, por fallas en su sistema de prevención o de monitoreo al cumplimiento de Leyes, reglamentos, regulaciones de los organismos de supervisión, políticas y demás procedimientos internos, de una entidad al blanqueo de capitales, financiamiento de terrorismo o financiamiento de la proliferación de armas de destrucción masiva.
8. Riesgo estratégico: Dificultad o incapacidad de la entidad para definir e implementar las políticas o estrategias para la entidad y los fondos que administra, tomar decisiones, asignar recursos o adaptarse a cambios en el entorno.
9. Riesgo de fraude y corrupción: Posible pérdida financiera, material o reputacional que puede derivarse de acciones fraudulentas por parte de actores internos o externos de la empresa.
10. Riesgo legal: Potenciales pérdidas derivadas como consecuencia de demandas o litigios o de la inobservancia o aplicación incorrecta o inoportuna de disposiciones legales o normativas, instrucciones emanadas de los organismos de control o como consecuencia de resoluciones judiciales, extrajudiciales o administrativas adversas, o de la falta de claridad o redacción deficiente en los textos contractuales que pueden afectar la formalización o ejecución de actos, contratos o transacciones.
11. Riesgo de liquidez: Pérdidas potenciales derivadas de situaciones donde la entidad no disponga de recursos líquidos suficientes para cumplir las obligaciones financieras cuándo y cómo se espera. Incluye el riesgo por la venta anticipada o forzosa de activos para hacer frente a las obligaciones, que conllevan descuentos inusuales, o bien, por el hecho de que una posición no pueda ser oportunamente enajenada, adquirida o cubierta mediante el establecimiento de una posición contraria equivalente. También se refiere al riesgo de que un activo financiero tenga que venderse a un precio menor al de mercado o incluso que no se pueda vender debido a la falta de liquidez del mercado.
12. Riesgo de mercado: Posibles pérdidas derivadas de movimientos adversos en los precios de los activos o instrumentos en los mercados financieros donde los mantengan,

con relación a las operaciones de la cartera de negociación. Este riesgo comprende principalmente el riesgo de precio, riesgo de tasa de interés y riesgo de tipo de cambio.

12.1 Riesgo de Precio. Es la posibilidad que ocurra una pérdida económica debido a variaciones adversas en el precio de mercado de un instrumento financiero o debido a la indeterminación del precio en un momento dado.
12.2 Riesgo de tasa de interés. Es la posibilidad de que ocurra una pérdida económica debido a variaciones adversas en las tasas de interés.
12.3 Riesgo de tipo de cambio. Es la posibilidad de que ocurra una pérdida económica debido a variaciones de la tasa de cambio.

13. Riesgo operacional: Pérdidas posibles debido a fallas o deficiencias en los sistemas de información, controles internos, procesos internos, errores humanos, fraudes, fallos de gestión o alteraciones provocadas por acontecimientos externos. Incluye el riesgo de las tecnologías de información.
14. Riesgo país: Riesgo que se genera por factores políticos, económicos, legales o sociales en un país. Es la posibilidad de incurrir en pérdidas ocasionadas por efectos adversos en el entorno económico, social o político. El riesgo país comprende entre otros el riesgo de transferencia, el riesgo político y el riesgo soberano.

14.1 Riesgo de transferencia. Es la incapacidad general de los deudores en un país determinado para cumplir con sus obligaciones financieras, debido a la falta de disponibilidad de la moneda en la cual está denominada la obligación, independientemente de la condición financiera particular del deudor respectivo.
14.2 Riesgo político. Es la posibilidad de que los intereses económicos de una empresa se vean afectados por los cambios o la falta de estabilidad política de un país o región.
14.3 Riesgo soberano. Es la posibilidad que el deudor soberano en un país determinado no pueda o no esté dispuesto a cumplir sus obligaciones financieras.

15. Riesgo de tecnología de la información y digitales: Consiste en riesgo por daños, interrupción, alteración o fallas derivadas en los sistemas físicos e informáticos, aplicaciones de cómputo, redes y cualquier otro canal de distribución necesarios para la ejecución de procesos operativos por parte de las entidades u otros relacionados.
16. Riesgo de reputación: La posibilidad de que, debido a la afectación del prestigio o credibilidad de la entidad, se incurra en pérdidas económicas. El riesgo reputacional es toda acción, evento o situación que podría impactar negativamente en la reputación de una organización.
17. Riesgo de valuación: Riesgo de que los métodos o supuestos usados para estimar el valor de los activos y obligaciones, resulten en valores que difieran de la experiencia o mejor alternativa técnica, dando lugar a incongruencia en las estimaciones u oportunidades artificiales de arbitraje de precios. Este riesgo puede incrementarse por un diseño complejo de los productos y servicios, y los beneficios u obligaciones asociados a éstos.

Artículo 6: Políticas, procedimientos y controles.

Para contribuir a la gestión de riesgos, las entidades con licencia deben establecer y mantener políticas, procedimientos y controles operativos efectivos en relación a su desempeño diario, y respecto a cada uno de sus negocios o actividades permitidas, o también los distintos productos y servicios que proveen. Las mismas deben implementarse en concordancia con las normas de Gobierno Corporativo de la entidad y orientarse a asegurar lo siguiente:

1. Intercambio efectivo de información entre la entidad y sus clientes, que contribuya a una adecuada toma de decisiones y una apropiada información de operaciones ejecutadas.
2. La integridad de las prácticas de la entidad en materia de ejecución de transacciones.
3. La resolución de conflictos de interés que se presenten entre la entidad o sus colaboradores y los clientes.
4. La segregación efectiva entre los activos de sus clientes y sus propios activos.
5. La protección de los activos tanto de sus clientes como de la entidad.

6. El mantenimiento apropiado de los registros contables y otros registros exigidos por la normativa vigente.
7. La independencia del CPA o auditor externo, de los auditores internos y de los consultores que brinden servicios que puedan generar conflicto de interés o riesgo de auto revisión.
8. La separación apropiada de los deberes y funciones claves dentro de la entidad.
9. La continuidad operacional de la entidad.
10. El cumplimiento por parte de la entidad, sus directivos y colaboradores de todos los requisitos legales y normativos aplicables.
11. Contar con mecanismos que permitan oportunamente hacer frente a cambios en el entorno del negocio.
12. Contar con mecanismos que garanticen la calidad de la información y de los datos que son utilizados en la gestión de las entidades o del entorno del negocio.

Artículo 7: Manual de Gestión Integral de Riesgos.

La entidad con licencia debe contar con un Manual de Gestión Integral de Riesgos, que contendrá, como mínimo:

1. Las políticas y procedimientos de gestión integral de riesgos, tanto los que son aplicables al conjunto de riesgos, como aquellos que son de utilidad para cada tipo de riesgo.
2. Mapa de riesgos, que lista y agrupa todos los tipos de riesgos relevantes que enfrenta la entidad, y que resulten congruentes con la estrategia de negocios, el tamaño y complejidad de operaciones y tipo de servicios y productos de la entidad.
3. La identificación de los riesgos inherentes, su importancia relativa en relación con los objetivos de la entidad y la protección de los intereses y activos de los clientes, y los mitigadores asociados, para cada una de las operaciones que desarrolla.
4. Límites internos sobre los riesgos residuales más significativos, teniendo en cuenta la capacidad del riesgo de la entidad.
5. Parámetros para la elaboración de los distintos escenarios, incluyendo el más desfavorable, que pueda enfrentar la entidad en función de los riesgos a los que se encuentran expuestas sus operaciones, y su respectivo plan de contingencia.
6. La identificación de los cargos de las unidades y personas responsables de la aplicación de las políticas y procedimientos de la gestión integral de riesgos, así como la descripción de las funciones que les correspondan.
7. Planes de continuidad de negocio y de recuperación de desastres, así como la designación de las personas responsables de su definición y ejecución.
8. Plan de seguridad de la información y ciberseguridad.
9. Elaboración de los procedimientos internos para comunicar a la Junta Directiva, Gerencia General u otros grupos de interés, según corresponda, sobre aquellos aspectos relevantes vinculados a la implementación y monitoreo de la gestión integral de riesgos.
10. Procedimientos de actualización anual y aprobación de la Junta Directiva o la Administración.

El Manual de Gestión Integral de Riesgos estará a disposición de la Superintendencia y su contenido deberá ser revisado por la Administración de la entidad con licencia al menos cada dos años, y debe ser actualizado en cada oportunidad que exista un cambio en las condiciones que lo fundamentan.

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

Artículo 8: Estructura organizativa y de soporte.

La estructura que sirva de soporte al proceso de gestión integral de riesgos deberá incorporar cuando menos los siguientes elementos:

1. Una clara y adecuada separación de funciones y responsabilidades entre las áreas de negocio y el Órgano de gestión de riesgos al que se refiere el artículo 13.

2. Contar con un Comité de Administración de Riesgo que reporte a la Junta Directiva.
3. Mecanismos de comunicación y divulgación de los alcances y resultados del proceso hacia todas las instancias relevantes, y la organización en general.
4. Contar regularmente con personal con los conocimientos y habilidades necesarios para desempeñar las funciones relacionadas a la gestión de riesgos. La selección de personal y la capacitación para estos fines debe ser parte integral del sistema de gestión de riesgos.

   Las capacitaciones para el desempeño de las funciones deben contemplar como mínimo lo siguiente:

   a. El temario debe estar alineado a los riesgos identificados en el manual de gestión integral de riesgos de la entidad de acuerdo a su modelo de negocios, según su frecuencia y severidad. Debe ser relevante para las funciones diarias del personal de riesgos.
   b. Dicho entrenamiento debe ser diseñado acorde a la experiencia, rol y responsabilidades a quien se brinda.
   c. El entrenamiento debe recibirse anualmente.
   d. El proveedor del entrenamiento deberá cumplir con los requisitos del artículo 13.

Artículo 9: Responsabilidad de la Junta Directiva en la gestión de riesgos.

La Junta Directiva de la entidad con licencia será responsable de establecer el cumplimiento de las políticas y procedimientos para gestionar apropiadamente los riesgos que la entidad afronta y ha identificado, debiendo definir los roles y líneas de reporte que correspondan, evitando incompatibilidades o conflictos de interés con otras funciones o Comités en los cuales formen parte.

Para cumplir apropiadamente esta responsabilidad, la Junta Directiva deberá conocer y entender los riesgos de la entidad; para lo cual serán regularmente capacitados y podrán, de ser necesario, recurrir a asesorías especializadas.

Entre las responsabilidades de las Juntas Directivas, que inciden con la gestión integral de riesgos, se encuentran, sin limitar:

1. Adoptar, establecer e implementar un sistema de gestión integral de riesgos acorde a la naturaleza, tamaño y complejidad de las operaciones de la entidad, 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, a fin de contar con la estructura organizativa, infraestructura, metodología y personal apropiado.
3. Ratificar el Manual de Gestión Integral de Riesgos y otras políticas pertinentes 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. Designar al responsable de las funciones de la gestión de riesgos de la entidad, quien reportará directamente a dicho órgano o al Comité de Administración de Riesgos, según sea su organización, y tendrá canales de comunicación con la Administración y otras áreas, respecto de los aspectos relevantes de la gestión de riesgos para una adecuada toma de decisiones.
6. Evaluar y aprobar sus planes de negocio teniendo en cuenta los riesgos asociados.
7. Establecer un sistema adecuado de delegación de facultades, separación y asignación de funciones, para permitir una ejecución efectiva de las responsabilidades asociadas a la gestión de riesgos; a la par de brindar adecuado tratamiento de posibles conflictos de interés en la entidad.
8. Establecer el apetito y la capacidad de riesgo de la entidad.
9. Velar por la implementación de una adecuada difusión de cultura de gestión integral de riesgos a todos los colaboradores de la entidad, mediante capacitaciones periódicas, dentro de cada ejercicio, sobre la normativa vigente relacionada con la gestión de riesgos; así como respecto a las políticas y procedimientos en materia de gestión de riesgos.

Q.C.

10. Velar por el adecuado desempeño de la Gestión Integral de Riesgos (GIR), mediante los reportes que recibe del Comité de Administración de Riesgos o su equivalente, o los que requiera directamente de forma complementaria.
11. Aprobar el Informe de Evaluación Anual de la Gestión Integral de Riesgos, que contiene la evaluación del sistema de Gestión Integral de Riesgos (GIR), sus desarrollos, avances, mejoras previstas y por realizar, analizando por separado los diferentes tipos de riesgos.
12. Velar porque el sistema de gestión integral de riesgos de la entidad se mantenga actualizado en función de los cambios del entorno, y de los negocios y actividades que desarrolla la entidad.
13. Recibir capacitación anual en temas de riesgo para los miembros de la Junta Directiva.

Los nuevos miembros que sean designados para formar parte de la Junta Directiva de las entidades con licencia recibirán una inducción que debe contener un componente específico relacionado a la gestión de riesgos de la entidad con licencia.

Artículo 10: Responsabilidad del Ejecutivo Principal en la Gestión Integral de Riesgos de la entidad.

El Ejecutivo Principal de la entidad con licencia es el responsable de dar a conocer las directrices de la gestión integral de riesgos de acuerdo con las políticas y procedimientos aprobados por la Junta Directiva, velando por su adecuado seguimiento y cumplimiento al interior de la entidad.

De forma específica, el Ejecutivo Principal es responsable de:

1. Asegurar consistencia entre las operaciones y los niveles de tolerancia de riesgo establecidos.
2. Conocer los niveles y tipos de riesgos de la entidad.
3. Establecer programas de revisión del cumplimiento de los objetivos, procedimientos, controles y límites establecidos por la Junta Directiva para la gestión integral de riesgos.
4. Velar que se cuenten con adecuados sistemas de almacenamiento, procesamiento y manejo de la información requerida para la Gestión Integral de Riesgos (GIR).
5. Velar porque exista un proceso de reclutamiento y selección que permita contratar el personal con las competencias, cualidades morales, la independencia y los conocimientos necesarios para el cumplimiento de sus responsabilidades en el sistema de la Gestión Integral de Riesgos (GIR).
6. Supervisar que se establezcan programas de capacitación y actualización sobre la Gestión Integral de Riesgos (GIR), tanto para los colaboradores responsables de su administración como el personal en general.
7. Definir procedimientos que aseguren el apropiado flujo de la información relevante sobre riesgos entre las unidades de negocio y las unidades responsables de la Gestión Integral de Riesgos (GIR).

Capítulo IV
Función de los Órganos operativos en la Gestión Integral de Riesgos

Artículo 11: Comité de Administración de Riesgos.

La Junta Directiva podrá constituir un Comité de Administración de Riesgos, en razón del tamaño y complejidad de las operaciones de la entidad con licencia con la finalidad de cumplir con las disposiciones del presente acuerdo, y en particular dar soporte para dar cumplimiento a lo establecido en el artículo 9 del presente Acuerdo.

En el caso que la entidad no cuente con un Comité de Administración de Riesgos, las funciones de este deberá ejercerlas la Junta Directiva y el Ejecutivo Principal deberá notificar a la Superintendencia del Mercado de Valores, la cual podrá objetar esto de acuerdo a la estructura, riesgos y /o tamaño de la entidad.

El Comité de Administración de Riesgos estará integrado por al menos dos (2) miembros de la Junta Directiva de la entidad, y será presidido por un director independiente.

Todos los miembros del comité deben ser personas de reconocida honorabilidad. Los miembros del Comité de Administración de Riesgos deben contar con formación y experiencia demostrable en materias relacionadas con el sector financiero, de manera que colectivamente posean un balance de habilidades, competencias y conocimientos para que puedan realizar el análisis de los riesgos financieros y no financieros que afectan a la entidad 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 documentar mediante actas de todas las sesiones que celebren, en las que se consignen las referencias, las discusiones mantenidas, los informes revisados y acuerdos adoptados. Las actas de sesiones podrán ser requeridas por la Superintendencia en cualquier momento.

La entidad con licencia podrá fusionar en un sólo Comité las funciones y responsabilidades del Comité de Ética y Cumplimiento y del Comité de Administración de Riesgos, dependiendo de su **tamaño, necesidades y estructura organizativa**, al igual que adoptar la nomenclatura elegida. El Ejecutivo Principal deberá comunicar la fusión de estos Comités a la Superintendencia, quien podrá objetarla en atención a los parámetros antes establecidos Lo dispuesto en el presente párrafo no es aplicable a las organizaciones autorreguladas, ni a las Entidades Administradoras de Inversión de Fondos de Pensiones y Jubilaciones, ni las Entidades Administradoras de Inversión de Fondos de Cesantía.

Artículo 12: 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.
2. Dar seguimiento continuo a las exposiciones a los distintos tipos de riesgos descritos en el artículo 5 del presente Acuerdo y comparar dichas exposiciones frente a los límites de capacidad de riesgo aprobados, dando cuenta de ello a la Junta Directiva.
3. Identificar los riesgos emergentes y proponer medidas de acción y mitigación a la Junta Directiva.
4. Evaluar el desempeño de la unidad, persona o tercero encargado de la gestión de riesgos (Órgano de la Gestión de Riesgos).
5. Aprobar los planes sobre apetito de riesgo, políticas de gestión de riesgo, límites de exposición por tipo de riesgo, estrategias de mitigación de los riesgos desarrollados por la Administración.
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. Aprobación del Manual de Gestión Integral de Riesgos (GIR) y sus actualizaciones y enviarlo a la Junta Directiva para su ratificación.
8. Otras que le establezca la Junta Directiva.

Artículo 13: Órgano de Gestión de Riesgos.

Las entidades con licencia deberán organizarse para administrar los riesgos a los que se encuentran expuestos; para lo cual deberá contar con al menos un órgano de gestión de riesgos, sea esta una gerencia, unidad, persona o tercero. Dicha gerencia, unidad, persona o tercero, será la encargada de diseñar y ejecutar las políticas y procedimientos para la gestión integral de los riesgos, de conformidad con lo establecido en el presente Acuerdo y en el Manual de Gestión Integral de Riesgos (GIR).

Para el cumplimiento de sus funciones, la gerencia, unidad, persona o tercero, deberán ser completamente independientes de las áreas de negocios, operaciones, administrativas y de finanzas, dependiendo organizacionalmente del Comité de Administración de Riesgos o directamente de la Junta Directiva, según sea el caso. Dicha gerencia, unidad, persona o tercero, no realizará, procesará o aprobará transacciones de negocios, operativas o administrativas y será la encargada de apoyar y asistir a las demás áreas de la entidad para la realización de una adecuada gestión de riesgos en sus áreas de responsabilidad, a excepción de la gestión del riesgo de prevención de blanqueo de capitales, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

Los integrantes de la gerencia, unidad, persona o terceros encargados de la gestión de riesgos deben poseer la experiencia y conocimientos técnicos que le permitan el adecuado cumplimiento de sus funciones. Para ello, el equipo o la persona, deberá contar con al menos dos o más de los siguientes requisitos:

1. Haber obtenido licencia de ejecutivo principal otorgada por la Superintendencia del Mercado de Valores.
2. Haber obtenido alguna certificación en riesgo con reconocimiento internacional (ISO 31000, CFA, FRM, CFI, entre otras.
3. Estudios universitarios en Gestión de Riesgos (Diplomado, Licenciatura, postgrado o maestría en Gestión de Riesgo).
4. Personal con experiencia directa o indirecta en el mercado de valores de tres (3) años.
5. Experiencia comprobada de al menos tres (3) años en gestión de riesgos.

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 del Mercado de Valores, es incompatible para ocupar otras funciones administrativas en la entidad al tenor de los artículos 5 y 6 del Acuerdo No. 5-2014 de 1 de octubre de 2014.

Artículo 14: Funciones del Órgano de Gestión de Riesgos.

El Órgano de Gestión de Riesgos tendrá las siguientes funciones:

1. Identificar, 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 nivel de complejidad y volumen de sus operaciones, que reflejen con precisión el valor de las posiciones y su sensibilidad a los diversos factores de riesgo.
    b. Evaluar regularmente los modelos y sistemas referidos, y plantear ante el Comité de Administración de Riesgos los ajustes requeridos. La periodicidad de estas evaluaciones debe ser determinada 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. Reportar a las áreas responsables pertinentes respecto de cualquier limitación o deficiencia de la información requerida.
    d. Ejecutar un programa periódico de pruebas retrospectivas (*back testing*), en el cual se comparen las estimaciones de la exposición por tipo de riesgo de los modelos internos contra los resultados efectivamente observados para el mismo período de medición, recomendar las calibraciones y el plazo para realizarlas.
    e. Efectuar pruebas de tensión (*stress test*) sobre todas las actividades que generen exposición a riesgos de mercado para aquellos escenarios que se consideren más relevantes dada la estructura de su balance, la escala, y complejidad de sus operaciones.

    La periodicidad inicial de los incisos "d" y "e" será de cada seis (6) meses. La Superintendencia a través circular podrá establecer cambios en la periodicidad establecida.

2. Llevar a cabo estimaciones de la exposición por tipo de riesgo.
3. Presentar al Comité de Administración de Riesgos para su consideración las herramientas y técnicas para identificar y analizar riesgos, y las metodologías, modelos y parámetros para medir y/o mitigar los distintos tipos de riesgos a que se encuentra expuesto la entidad con licencia.
4. Verificar la observancia de los límites globales y específicos, así como los niveles de tolerancia aceptables 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 para la medición y control de riesgo aprobados por el citado comité.
5. Proporcionar al Comité de Administración de Riesgos los informes relativos a:

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 capacidad de riesgo establecidos.
d. Sugerencias respecto a acciones correctivas que pueden implementarse como resultado de una desviación respecto a los límites de exposición y niveles de capacidad de riesgo autorizados.
e. Análisis histórico y de tendencias de los riesgos asumidos por la entidad con licencia.

6. Hacer seguimiento a los acuerdos del Comité, informando al mismo de estos avances.
7. 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.
8. Analizar y evaluar permanentemente los supuestos y parámetros utilizados en los análisis requeridos.
9. Preparar el "Informe de Evaluación Anual de la Gestión Integral de Riesgos" a que se refiere el artículo 21 del presente acuerdo.
10. Velar por que la información prevista a ser presentada al Comité de Administración de Riesgos para ser remitida a la Superintendencia sea atendida oportuna y cabalmente, respetando los canales regulares existentes. En este contexto, la entidad con licencia deberá informar a la Superintendencia apenas se tenga conocimiento de cualquier aspecto materialmente relevante relacionado con la exposición de riesgos, que puedan impactar significativamente la solvencia o liquidez de la entidad. Para este fin mantendrá debida coordinación con el oficial de cumplimiento, salvaguardando cada uno la observancia de sus responsabilidades.
11. Responsable de elaborar y/o ejecutar el Manual de Gestión Integral de Riesgos,
12. Cualquier otra función que le requiera el Comité de Administración de Riesgos.

Artículo 15: Aplicación por terceros de la gestión de riesgos.

La Superintendencia podrá permitir que las entidades con licencia puedan tercerizar para dar cumplimiento a una o más de las obligaciones establecidas en el presente Acuerdo, relacionadas con la gestión de sus riesgos, revisando caso por caso y dependiendo de la estructura organizacional de la entidad con licencia.

Las entidades con licencia no podrán tercerizar a firmas o personas, si estas trabajan en entidades que realizan la auditoría externa de los estados financieros de la entidad, para no generar riesgo de independencia.

La entidad con licencia deberá contratar servicios con proveedores locales. Los contratos con los proveedores del servicio deberán incluir cláusulas que permitan el acceso y revisión a la documentación e información mantenida por cualquier medio o soporte del servicio realizado a la entidad con licencia y a la Superintendencia del Mercado de Valores.

Las entidades con licencia mantienen la responsabilidad del cumplimiento de las obligaciones del presente acuerdo, aunque las mismas hayan sido tercerizadas.

El tercero deberá participar en las reuniones del Comité de Administración de Riesgo con derecho a voz.

El tercero deberá reportar al Comité de Administración de Riesgo y será responsable de las funciones del Órgano de Gestión de Riesgos, sin embargo, no podrán realizar las funciones de aprobación de políticas, límites, reportes y demás facultades exclusivas de la Junta Directiva.

Los terceros deberán cumplir con las obligaciones y prohibiciones establecidas en el artículo 13 del presente acuerdo.

Artículo 16: Grupos financieros o económicos.

Aquellas entidades con licencia que pertenezcan a un grupo financiero o grupo económico podrán plantear que parte de las funciones operativas a que se refiere el presente capítulo sean ejecutadas a nivel del grupo, debiendo cumplir con lo siguiente:

1. Las funciones y obligaciones atribuidas a dichos comités deberán incluir las contenidas en este Acuerdo, distinguiendo entre los temas y asuntos que guarden relación con cada una de las subsidiarias y/o afiliadas de que se trate y de la misma manera se deberá documentar en las actas de los comités.
2. El planteamiento de las labores que serán cubiertas por el grupo debe ser específico, y debe estar debidamente aprobadas por la Junta Directiva.
3. La entidad debe albergar internamente suficiente conocimiento y experiencia para la gestión de riesgos en el sector de valores, por lo que cualquier soporte que venga de parte del grupo, no debe afectar la solvencia del sistema de gestión de riesgos que ésta debe mantener.
4. La Junta Directiva de la entidad mantendrá la responsabilidad de las decisiones que se adopten respecto al sistema de gestión de riesgos.
5. Cuando el Órgano de Gestión de Riesgos y/o el Comité de Administración de Riesgos se lleven en el grupo económico y no en la entidad con licencia, estas se deben asegurar que cumplan con todas las funciones y demás obligaciones establecidas en este Acuerdo.

Las entidades con licencia que vayan a ejecutar parte de las funciones operativas a que se refiere el presente Capítulo a nivel de grupo, deberán notificarlo a través de su ejecutivo principal a la Superintendencia del Mercado de Valores, la cual evaluará cada planteamiento, caso por caso. En caso de requerirse, la Superintendencia del Mercado de Valores podrá solicitar, de acuerdo con la complejidad de la entidad regulada, que las funciones de gestión de riesgo dejen de ser ejecutadas a nivel de grupo.

Capítulo V
Función del Órgano de control en la Gestión Integral de Riesgos

Artículo 17: Función de la auditoría interna para la gestión integral de riesgos

La Auditoría Interna de la entidad con licencia deberá evaluar el cumplimiento de los procedimientos utilizados para la gestión integral de riesgos. Dicha evaluación será parte de las actividades permanentes del Plan Anual de Auditoría Interna de la entidad.

La Auditoría Interna debe emitir, al menos, un informe anual dirigido a la Junta Directiva que contenga las recomendaciones que se deriven de su evaluación. Los informes deberán estar a disposición de la Superintendencia del Mercado de Valores cuando esta así lo requiera.

La entidad con licencia que no cuente con un auditor interno, pero que, de acuerdo con las disposiciones emitidas por la Superintendencia, tenga un colaborador u órgano que ejerza las atribuciones y responsabilidades: i) respecto del control interno de la entidad, o ii) del cumplimiento de sus normas internas de conducta, o iii) de la administración de los patrimonios bajo su gestión, deberá cumplir con las funciones establecidas en el presente artículo, a través de dichos colaboradores u órganos.

La función de auditoría interna deberá ser independiente de la operación, negocios y la administración. Adicionalmente, no debe ser ejecutada por la persona natural o jurídica que realice la auditoría externa de los estados financieros.

Artículo 18. Perfil de la persona responsable de la auditoría interna.

La persona responsable de la auditoría interna de la entidad deberá ser contador público autorizado idóneo y cumplir los requisitos del perfil de auditor interno que dispone la Ley.

Capítulo VI
Gestión por Tipo de Riesgos.

Artículo 19: Obligación de gestionar los riesgos.

La gestión de riesgos se ceñirá a lo establecido en el presente Acuerdo; así como a lo dispuesto en los Acuerdos complementarios específicos emitidos por la Superintendencia respecto de la gestión de algunos de los tipos de riesgos indicados en el artículo 5 del presente Acuerdo.

Las entidades con licencia deberán gestionar cada uno de los riesgos que enfrentan, según quedará consignado en el respectivo mapa de riesgos, de acuerdo a su complejidad, estructura, tamaño, negocio y recursos, así como los riesgos asumidos por los fondos que administren.

Artículo 20: Componentes de la gestión de cada riesgo.

La gestión de cada uno de los riesgos que enfrenta la entidad con licencia deberá atender los aspectos siguientes:

1. Identificar en detalle los factores o variables cuyos movimientos o ejecución de actividades puedan originar un incremento en el riesgo;
2. Definir los indicadores que se utilizarán para hacer seguimiento de cada tipo de riesgo, en concordancia con la normativa aplicable;
3. Establecer los límites o umbrales de los indicadores señalados en el numeral anterior, que permitan establecer la tolerancia al riesgo.
4. Estimar los impactos que generan la ocurrencia de los riesgos;
5. Para evaluar la concentración como fuente de riesgo, se debe considerar a la entidad en conjunto con sus partes relacionadas, según se define este término en las Normas Internacionales de Información Financiera;
6. Disponer de mecanismos para monitorear los factores de riesgo identificados, utilizando para tal efecto modelos, herramientas y límites de riesgo. Asimismo, la entidad debe realizar estimaciones de las tendencias que presentan los factores de riesgo identificados;
7. Establecer medidas para controlar y/o mitigar la exposición a los riesgos.
8. Establecer indicadores o umbrales de alerta temprana que permitan identificar con anticipación las exposiciones al riesgo
9. Analizar y controlar la diversificación de las actividades de la entidad y sus riesgos relacionados a las mismas.

Capítulo VII
Sistema de información

Artículo 21: Informe de Evaluación anual de la Gestión Integral de Riesgos (GIR).

Las entidades con licencia deberán remitir a la Superintendencia, dentro de los ciento veinte (120) días posteriores al cierre del ejercicio contable, el "Informe de Evaluación Anual 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, el mismo que contendrá cuando menos lo siguiente:

1. La estructura organizativa para la gestión integral de riesgos, describiendo las principales responsabilidades de cada colaborador dentro del Órgano de Gestión de Riesgos (gerencia, unidad, persona o tercero);
2. Las políticas actualizadas para la gestión integral de riesgos, así como un análisis del grado de cumplimiento de estas;
3. Detalle del mapa de riesgos que enfrenta la entidad, así como un repaso de los principales riesgos asumidos durante el ejercicio que se reporta y la forma como fueron atendidos. Se deberá proporcionar análisis de los indicadores establecidos para el apetito y capacidad de riesgo, así como los estimados de pérdida potencial esperada bajo los escenarios que se estimen relevantes;
4. Descripción de las metodologías, sistemas y herramientas utilizadas para cada uno de los riesgos;

5. Descripción de las principales acciones de control o evaluaciones especiales realizadas respecto a los distintos riesgos que se enfrentan; explicando las acciones tomadas respecto a las conclusiones de cada informe.
6. Descripción de las diferentes actividades de capacitación realizadas en relación con la gestión integral de riesgos;
7. Proyectos asociados a la gestión de riesgos a desarrollar en el ejercicio contable siguiente al reportado;
8. Cuestionario de autoevaluación completado.
9. Conclusiones generales y recomendaciones sobre la gestión de riesgos de la entidad.

Parágrafo. Cuestionario de autoevaluación

La Superintendencia del Mercado de Valores remitirá a las entidades con licencia para su atención, un cuestionario de autoevaluación, con al menos sesenta (60) días calendario de antelación a la fecha de entrega del Informe de Evaluación Anual de la Gestión Integral de Riesgos que trata el presente artículo.

Artículo 22: Información para la Superintendencia.

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 la entidad de que se trate.

Las entidades con licencia deberán tener en todo momento a disposición de la Superintendencia todos los documentos, registros, archivos, en forma física, electrónica o por cualquier otro medio, a que se refiere el presente Acuerdo, así como los informes resultantes de acciones de control por parte 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 determinación de los nombres de las personas involucradas en la gestión de riesgos de la entidad con licencia, para la atención en caso de consultas que el regulador pueda mantener.

Capítulo VIII
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

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, el cual quedará así:

> **Artículo 2. Definiciones.**
>
> Para los propósitos del presente Acuerdo, los siguientes términos se entenderán de la siguiente manera:
>
> a) **Contingencia:** Es la posibilidad de que algo acontezca, es decir, la posibilidad de que algo ocurra o no. Una contingencia es un evento más o menos esperable de acuerdo con los modelos predictivos en la Gestión Integral de Riesgos (GIR) que trata este Acuerdo, aunque no necesariamente en tiempo, espacio y magnitud.
> 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:** Proceso diseñado para reducir el riesgo de la falta de continuidad de las operaciones, actividades y negocio de la entidad con licencia que surja de una interrupción inesperada de sus funciones u operaciones críticas, independientemente de si éstas son manuales o automatizadas, las cuales son necesarias para la supervivencia y buena gestión de la entidad. 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 para minimizar los efectos de un desastre y permitir que una entidad continúe operando o reanude rápidamente las operaciones importantes. Este plan busca restaurar el nivel de operatividad de la entidad al momento anterior a la crisis.
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, 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 aprobada 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 de continuidad 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 alterno, 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 los doce meses, deberán quedar establecidas las instancias de la Gestión Integral de Riesgos a que se refiere el Acuerdo, con su respectiva normativa interna debidamente aprobada.

La SMV podrá solicitar a las entidades, durante los doce meses indicados, el cronograma de trabajo que evidencie el avance de la implementación del presente Acuerdo.

PUBLÍQUESE Y CÚMPLASE

Adriana Carles
Presidente de la Junta Directiva

Luis E. Vásquez Brown
Secretario de la Junta Directiva