MANUAL CORPORATIVO DEL SISTEMA DE GESTIÓN DEL RIESGO DEL GRUPO EMPRESARIAL COOPERATIVO COOMEVA

COPIA CONTROLADA

COPIA CONTROLADA

COPIA CONTROLADA

INTRODUCCIÓN

La Cooperativa Médica del Valle y de Profesionales de Colombia, COOMEVA, sus fondos mutuales y unidades de negocio y las empresas que conforman el **GRUPO EMPRESARIAL COOPERATIVO COOMEVA**, **(GECC)** desarrollan sus actividades con sujeción a las normas legales y a los más altos principios éticos; por tal motivo, en cumplimiento de lo establecido en las normas emitidas por la Superintendencia de la Economía Solidaria, por la Superintendencia Financiera de Colombia, por la Superintendencia de Sociedades y demás entidades y organismos de vigilancia y control, el Consejo de Administración de COOMEVA aprueba el marco general del **SISTEMA DE GESTIÓN DEL RIESGO (SGR)** para el Grupo, el cual es de obligatorio cumplimiento por parte de los administradores, directivos y en general de todos los colaboradores**.**

1. OBJETIVO

Definir el marco de referencia, instrumentos y metodologías generales para la implementación y funcionamiento del **SISTEMA DE GESTIÓN DEL RIESGO-SGR-** para Coomeva, sus fondos mutuales y unidades de negocio y las empresas que conforman el Grupo Empresarial Cooperativo Coomeva **(GECC)** y el Conglomerado en su conjunto, con el fin de identificar, analizar, monitorear, medir y controlar los riesgos operativos implicados en los procesos.

En lo sucesivo, cuando en este Manual se haga referencia al **GECC** y a las disposiciones, obligaciones y en general a requerimientos que este debe cumplir, se entenderá que estas se refieren a todas y cada una de las entidades, fondos y unidades que lo conforman y cuando se haga referencia al **Nivel Corporativo**, se entenderá que se refiere al conjunto del grupo visto como conglomerado.

2. ALCANCE

El presente Manual tiene carácter vinculante y alcance para todo el **GECC**-, y todas las áreas y procesos que conforman el Grupo, incluyendo los procesos que las empresas y unidades decidan tercerizar.

Este Manual y los demás que lo complementan, definen clara y explícitamente el marco conceptual y de actuación para la aplicación objetiva, sistemática y estandarizada de la Gestión Integral de Riesgos y en tal sentido incluye los lineamientos para la gestión de los siguientes sistemas y subsistemas:

- Subsistema de Gestión de Riesgo Estratégico (Incluye la Gestión de los Riesgos de Gobierno Corporativo)
- Subsistema de Gestión de Riesgo de Conglomerados
- Subsistema de Gestión de Riesgo Operativo (SGRO)
- Subsistema de Gestión de Riesgo de Liquidez (SGRL)
- Subsistema de Gestión de Riesgo de Mercado (SGRM) (Incluye Riesgo de Contraparte)
- Subsistema de Gestión de Riesgo de Crédito (SGRC)
- Subsistema de Gestión del Riesgo del Lavado de Activos y Financiación del Terrorismo (LA/FT)
- Subsistema de Gestión del Riesgo de Fraude y Corrupción
- Subsistema de Gestión de Riesgos en Proyectos
- Subsistema de Gestión de Riesgo Propio del Negocio
- Sistema Especial de Administración de Riesgos de Seguros (SEARS)

- Sistema de Gestión de la Continuidad del Negocio (SGCN)
- Sistema de Gestión de la Seguridad de la Información (SGSI)

Las directrices y lineamientos corporativos plasmados en este documento, complementan la normatividad al interior del GECC, de acuerdo al Sector al cual pertenezcan cada una de las empresas y unidades que lo conforman, así por ejemplo:

- La Cooperativa y sus Fondos Mutuales tendrán como referente normativo para la implantación de su Sistema de Gestión de Riesgo, lo dispuesto por la Superintendencia de Economía Solidaria, los Estatutos, Acuerdos, Resoluciones y reglamentos particulares, así como las demás normas que les apliquen.

- Las empresas del Sector Salud, tendrán como referente normativo para la implantación de su Sistema de Gestión de Riesgo, lo dispuesto por la Superintendencia de Salud de Colombia y demás normas que les apliquen.

- Las empresas del Sector Financiero, tendrán como referente normativo para la implantación de su Sistema de Gestión de Riesgo, lo dispuesto por la Superintendencia Financiera de Colombia y demás normas que les apliquen.

- Las empresas del Sector Recreación, tendrán como referente normativo para la implantación de su Sistema de Gestión de Riesgo, lo dispuesto por la Superintendencia de Sociedades y demás normas que les apliquen.

- Las empresas del Sector Protección, tendrán como referente normativo para la implantación de su Sistema de Gestión de Riesgo, lo dispuesto por la Superintendencia de la Economía Solidaria y la Superintendencia Financiera de Colombia y demás normas que les apliquen.

Todas las empresas del GECC deben incorporar las directrices corporativas y a su vez garantizar el cumplimiento normativo relacionado con la gestión de riesgo propio de su actividad y sector.

3. APROBACIÒN

El presente Manual fue aprobado por el Consejo de Administración, mediante Acuerdo No. ____de ___ de enero de 2015.

COPIA CONTROLADA

4. TÉRMINOS Y DEFINICIONES

4.1 Asociados

Son quienes están vinculados como cooperados a la Cooperativa.

4.2 Apetito de Riesgo

Es una ponderación de alto nivel acerca de cuál es el límite de riesgo (cuánto riesgo), el Consejo de Administración y/o las Juntas Directivas están dispuestos a aceptar para alcanzar el logro de sus metas.

4.3 Causa/Falla/Insuficiencia

Es lo que hace que un evento de riesgo se materialice y se convierta en un evento de pérdida.

4.4 Clientes/usuarios

Toda persona natural o jurídica con la cual EL GECC establece y mantiene una relación contractual o legal para el suministro de cualquier producto o servicio propio de su actividad.

4.5 Conglomerado

En Colombia, son conglomerados quienes se encuentren en las situaciones previstas en los artículos 260 del Código de Comercio (subordinación) y el 28 de la Ley 222 de 1995 (de Grupo Empresarial) y las normas que los modifiquen o adicionen, aquellos respecto de los cuales la Superintendencia competente, en uso de sus atribuciones legales, ordene la consolidación de estados financieros, y los demás que determinen las normas pertinentes. Según lo anterior:

Una sociedad será subordinada o controlada cuando su poder de decisión se encuentre sometido a la voluntad de su matriz o controlante, bien sea directamente, caso en el cual aquélla se denominará filial o con el concurso o por intermedio de las subordinadas de la matriz, en cuyo caso se llamará subsidiaria

Hay grupo empresarial cuando además del vínculo de subordinación, entre las entidades existe unidad de propósito y dirección, o sea cuando la existencia y actividades de todas las entidades persigan la consecución de un objetivo determinado por la matriz o controlante, en virtud de la dirección que ejerce sobre el conjunto, sin perjuicio del desarrollo individual del objeto social o actividad de cada una de ellas.

Una de las principales razones para la conformación de los conglomerados mixtos, es la ventaja de ofrecer una variedad de servicios, el aprovechamiento de las sinergias a través de compartir activos, compartir el nombre o imagen conjunta y activos intangibles, uso de infraestructura, aprovechamiento de sistemas operativos y manejo de información y por supuesto la comercialización conjunta de los servicios, con los consecuentes riesgos que dichas interrelaciones conllevan, los cuales son mayores que los que se presentan en las empresas individuales.

El **GECC** es un grupo empresarial de naturaleza cooperativa, inscrito en la Cámara de Comercio de Cali, conformado por la Cooperativa, quien en su calidad de matriz vela por el mantenimiento de la unidad de propósito, dirección y control, conformado por diecisiete (17) empresas y unidades de negocio, agrupadas en cuatro (4) sectores: Salud, Financiero, Protección y Recreación,, con vínculos de propiedad por tener un mismo beneficiario real controlante,, las cuales interactúan a través de un amplio portafolio de productos y servicios que se destinan al grupo objetivo de asociados a la matriz, Coomeva, así como a terceros y a cubrir por tercerización las necesidades de las mismas empresas del Grupo.

4.6 Consolidación

Proceso a través del cual se agregan de manera coherente y consistente todos los riesgos de la Organización.

4.7 Contraparte

Entidades autorizadas por la Superintendencia Financiera de Colombia como intermediarios del mercado de valores para negociar títulos valores o cualquier otro activo financiero.

4.8 Evaluación

Medición del riesgo frente a su probabilidad de ocurrencia y la severidad de sus consecuencias, de acuerdo con las escalas metodológicamente preestablecidas para cada recurso y que permite definir la prioridad para su gestión.

4.9 Evaluación del control

Revisión sistemática de los procesos para garantizar que los controles siguen siendo eficaces y adecuados. La revisión periódica de la gestión en línea de los controles se denomina" Auto evaluación del control".

4.10 Eventos de Pérdida

Son aquellos incidentes que generan pérdidas cuando se materializa un riesgo.

4.11 Eventos de Riesgo

Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado y que corresponde a la materialización de un riesgo.

4.12 Factores de riesgo

Se entienden por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo. Son factores de riesgo Operativo: El recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Dichos factores se deben clasificar en Factores Internos o en Factores Externos, según se indica a continuación:

4.12.1 Factores Internos

Son factores internos los siguientes:

4.12.1.1 Infraestructura

Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

4.12.1.2 Recurso Humano

Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente. La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.

4.12.1.3 Procesos

Es el conjunto interrelacionado de actividades que se ejecutan para la transformación de elementos de entrada en productos o servicios, con el fin de satisfacer una necesidad.

4.12.1.4 Tecnología

Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluyen: hardware, software, telecomunicaciones y medios de respaldo.

4.12.2 Factores Externos

Son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan al control de la entidad en cuanto a su causa y origen.

4.13 Financiación del Terrorismo (FT)

Es el proceso por medio del cual se obtienen los bienes, recursos o activos de procedencia ilícita o licita para realizar actividades terroristas (Delito descrito en el artículo 345 del Código Penal). Apoyo económico a las personas que fomentan actos terroristas, fondeo o inyección de capital.

4.14 Gerencia de Riesgos Empresariales - ERM (Enterprise Risk Management)

Proceso que implica el ejercicio de análisis sistemático, efectuado por todas las personas de la organización, aplicado desde la definición estratégica hasta las actividades del día a día, para identificar los eventos que podrían afectar la organización, gestionando los riesgos dentro de su apetito, con el fin de crear y preservar valor empresarial, brindando una seguridad razonable respecto del logro de los objetivos del **GECC.**

4.15 Gestión Integral del riesgo

Conjunto de actividades estandarizadas, sistemáticas y coordinadas para dirigir y controlar la organización y sus procesos con respecto al riesgo.

4.16 Gestión de Continuidad de Negocio (GCN)

Proceso holístico y sistemático de la organización por medio del cual se identifican impactos potenciales que pueden amenazar la continuidad del negocio y que provee un marco de referencia para establecer y desarrollar estrategias pro-activas, construir respuestas eficaces y eficientes con la flexibilidad y la capacidad necesarias para aumentar la capacidad de reacción de la organización y brindar respuestas eficaces que permitan salvaguardar los intereses de las diferentes partes interesadas, involucradas y afectadas (Stakeholders), garantizar la gobernabilidad, la reputación, la imagen y las actividades de creación de valor de una organización.

4.17 Gestión de Riesgos en los Proyectos

Se refiere a la posibilidad de pérdidas en que incurren las empresas y unidades de negocio del **GECC** como consecuencia de la incertidumbre de los proyectos relacionadas con el alcance, el cronograma, el presupuesto (costos), la calidad, las adquisiciones, las personas del proyecto, los interesados, las comunicaciones y la credibilidad de los proyectos.

4.18 Identificación

Proceso mediante el cual se determinan los posibles eventos que podrían afectar los recursos o desviar el logro de los objetivos del Grupo Empresarial.

4.19 Incertidumbre

Corresponde a aquella situación sobre la cual no se conoce con seguridad si ocurrirá y, de ocurrir, cómo se comportará en el futuro.

4.20 Lavado de Activos (LA)

Son todas las acciones para dar apariencia de legalidad a recursos de origen ilícito con el fin de introducirlos en la economía a través del sector real o el sector financiero. En la mayoría de los países del mundo ésta conducta es considerada delito y también se conoce como lavado de dinero, blanqueo de capitales, legitimación de capitales, entre otros. Delito que comete toda persona que busca dar apariencia de legalidad a bienes o dinero provenientes de alguna de las actividades descritas en el artículo 323 del Código Penal.

4.21 Liquidez

Cualidad de los activos para ser convertidos en dinero efectivo de forma inmediata sin pérdida significativa de su valor.

4.22 Marco de referencia para la gestión del riesgo

Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo a través de toda la organización.

Las bases incluyen la política, los objetivos, el gobierno y el compromiso para gestionar el riesgo.

Las disposiciones de la organización incluyen planes, relaciones, rendición de cuentas (Accountability), recursos, procesos y actividades.

El marco de referencia para la gestión de riesgo está incluido en las políticas y prácticas estratégicas y operacionales globales de la organización.

4.23 Máximo órgano social.

Según el tipo societario, será la Junta de Socios o la Asamblea General de Accionistas; para el caso de la Cooperativa es la Asamblea General de Delegados y está conformada por todos los asociados delegados de la Cooperativa.

4.24 Monitorear

Verificar, supervisar, observar críticamente o medir y registrar regularmente el progreso de una actividad, una acción y/o un sistema para identificar los cambios en el nivel de desempeño requerido o esperado y retroalimentar las oportunidades de mejora en la Gestión Integral del Riesgo.

4.25 Pérdidas

Cuantificación económica de la ocurrencia de un evento de riesgo, así como de los gastos derivados de su atención.

4.26 Perfil de Riesgo

Resultado consolidado de la medición de los riesgos a los que se ve expuesta la entidad.

4.27 Plan de Continuidad del Negocio

Es el resultado de la aplicación de una metodología interdisciplinaria para la Administración de Continuidad de Negocio, usada para crear y validar planes logísticos para la práctica acerca de cómo una organización debe recuperar y restaurar sus funciones críticas, parcial o totalmente interrumpidas, dentro de un tiempo predeterminado después de una interrupción no deseada o de un desastre. Es el cómo la organización se prepara para futuros incidentes que puedan poner en peligro a ésta y a su misión básica a largo plazo.

4.28 Plan de Contingencia

Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

4.29 Proceso para la gestión del riesgo

Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

4.30 Recursos

Son los talentos y activos fundamentales con que cuenta el **GECC** para cumplir con sus objetivos, los cuales deben ser protegidos mediante la Gestión Integral de Riesgos.

4.31 Riesgo

Es el efecto de la incertidumbre que podría afectar los recursos y la capacidad de la organización para lograr sus objetivos empresariales, ejecutar con éxito sus estrategias de negocio o cumplir con los requisitos normativos y legales.

En particular, el impacto generado por los riesgos en las empresas afecta la reputación, el desempeño operativo o del servicio, el desempeño financiero y el balance social frente a los grupos de interés.

4.32 Riesgo de Conglomerado

Corresponde a la probabilidad de pérdida o insolvencia como consecuencia de las fallas que se derivan de las decisiones, operaciones, y relaciones entre la empresa controlante y sus subordinadas, y/o entre ellas.

La gestión de este riesgo posibilita la medición unificada y más acertada de los riesgos del grupo completo y no de sus partes, evitando el traspaso y la concentración de riesgos desde entidades reguladas hacia aquellas no reguladas y busca garantizar:

- Que existan personas idóneas al frente del control y la administración del Conglomerado.
- Que el Conglomerado cuente con una estructura administrativa consistente con el perfil de riesgo y que ésta sea entendida por la alta dirección.
- Que se definan niveles de riesgo tolerables.
- Que se dirijan bien los riesgos asociados con nuevos negocios.
- Que se realicen pruebas y análisis de escenarios negativos.
- Que se agregue prudencialmente el riesgo.
- Que se realicen los estados financieros de todas las actividades bajo la supervisión del conglomerado.
- Que exista una fuerte administración del capital y de los riesgos de liquidez.

Los tipos de riesgos asociados a un Conglomerado, se pueden tipificar así:

4.32.1.1 Riesgo de contagio:

Se entiende por riesgo de contagio la probabilidad de pérdida que puede sufrir la casa matriz o una o varias de las entidades que hacen parte del conglomerado, por acciones, decisiones, resultados, situaciones o experiencias de una o varias de las entidades que lo conforman, o, por un evento externo o una combinación de ellos.

4.32.1.2 Riesgo de adecuación de capital:

Consiste en la probabilidad de incremento en las necesidades de inversión en la matriz o en las subordinadas, para cumplir con exigencias propias de cada actividad o por decisiones de los entes de control.

4.32.1.3 Riesgo de operaciones entre-vinculadas:

Consiste en la probabilidad de pérdida originada por sanciones y/o multas generadas por operaciones no permitidas, no consensuadas, y/o no controladas entre la matriz y las partes, o entre ellas.

4.32.1.4 Riesgo de subsidios cruzados:

Consiste en la probabilidad de pérdidas por desviación de la tarifa media, o modificación de tarifas, en una o varias de las entidades del conglomerado, con el fin de favorecer los intereses de la casa matriz o de alguna(s) de las otras empresas del grupo, afectando el margen de contribución de las otras.

4.32.1.5 Riesgo de doble apalancamiento:

Consiste en la probabilidad de pérdidas y/o insolvencia, generadas por decisiones de inversión entre las entidades y la casa matriz, sin la debida regulación y sin el debido respaldo.

4.32.1.6 Riesgo de Solvencia

Consiste en la probabilidad de pérdida por deterioro de la estructura financiera del conglomerado o de la de sus empresas, lo cual puede disminuir el valor de la inversión o la capacidad de pago para garantizar sus deudas y compromisos, principalmente de largo plazo (Ligado a Riesgo de Crédito, liquidez y rentabilidad).

La solvencia depende de dos factores: La capacidad de generar y contar con recursos financieros suficientes (base de la solvencia) y la puntualidad en los pagos.

4.32.1.7 Riesgo de Gobierno Corporativo:

Consiste en la pérdida de control, disciplina, transparencia, independencia, responsabilidad, imparcialidad, autonomía, responsabilidad social y liderazgo, con fallas en revelación de estados financieros y rendición de cuentas o cuando se evidencia un desplazamiento del centro de poder de la matriz a las subsidiarias, generando incapacidad para cumplir sus responsabilidades y obligaciones, como resultado de una influencia indebida de los miembros del conglomerado.

4.32.1.8 Riesgo de Concentración

Consiste en una exposición que podría causar pérdidas que pudieran amenazar la solvencia o la capacidad del conglomerado de mantener las operaciones centrales de sus empresas. Las concentraciones de riesgo pueden surgir en los activos, pasivos o ítems fuera de la hoja de balance de un conglomerado, a través de la ejecución o el procesamiento de transacciones (productos o servicios), o a través de una combinación de exposiciones en estas categorías grandes.

El análisis del riesgo de concentración implica examinar:

- Composición y concentración de los Activos
- Composición y concentración de los Pasivos
- Concentración de operaciones
- Volumen de operación (facturación en uno o pocos clientes).
  - Inversiones: Permanentes, de Portafolio, e intragrupo.
  - Servicios: proveedores de servicios core, poder monopólico en la tarifa por la contraparte.
  - Cuentas por cobrar.
  - Cuentas por pagar.

4.32.1.9 Riesgo Sistémico:

Es el "Riesgo de Riesgos", el cual corresponde a la probabilidad de pérdida o insolvencia, que puede sufrir la totalidad o varias de las empresas que conforman el conglomerado, incluyendo a lamatriz, por incumplimiento de las obligaciones, o por una acción, decisión, resultado o experiencia de una o varias de las entidades que lo conforman o, por un evento externo o una combinación de ellos.

4.33 Riesgo de Contraparte

Probabilidad de pérdidas como consecuencia del incumplimiento de las contrapartes con las cuales se realizan negocios de inversión; esto aplica en los procesos de administración de liquidez y estructuración de portafolios de inversión.

4.34 Riesgo de Corrupción

Es la posibilidad de pérdida en que incurren las empresas y unidades de negocio del **GECC** como consecuencia de actuaciones deshonestas que generan desviación fraudulenta o abusiva de potestades de control y decisión en la búsqueda de sobornos, extorsión, pagos inapropiados o beneficios personales directos o indirectos, favoreciendo inequitativamente a terceros y generando conflictos de interés.

4.35 Riesgo de Crédito (RC):

Es la posibilidad de incurrir en pérdidas por el no pago o pago inoportuno de las obligaciones a cargo de: clientes, aseguradores, anticipos otorgados, riesgo de contraparte de las inversiones permanentes y/o cualquiera otra operación que determine una deuda a favor de la entidad.

4.36 Riesgo de lavado de activos y de la financiación del terrorismo (LA/FT):

Es la posibilidad de pérdida que puede sufrir una entidad por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o el financiamiento del terrorismo.

4.37 Riesgo Estratégico

Corresponde a la probabilidad de pérdida como consecuencia de incertidumbres asociadas a la formulación estratégica que pueden volver el modelo de negocio inefectivo u obsoleto, afectando seria y adversamente la capacidad de la entidad para cumplir sus objetivos estratégicos, para crear valor y para mantener la sostenibilidad. Esta incertidumbre es interna y externa.

Este riesgo se relaciona con la imposibilidad de formular e implementar apropiadamente los planes de negocio, las estrategias, las decisiones de mercado, la asignación de recursos y su incapacidad para adaptarse a los cambios en el entorno de los negocios. Así mismo, se debe analizar el riesgo que emerge de la pérdida de participación en el mercado y/o disminuciones en los ingresos que puedan afectar la situación financiera de la entidad.

Por ello, el punto de partida para el análisis de los riesgos estratégicos debe comenzar a partir del proceso de Planeación Estratégica en el **GECC**, y de la identificación de las partes interesadas, sus objetivos, intereses y percepciones, así como de las estrategias, acciones y canales de comunicación con ellas.

4.38 Riesgo Legal

Es la posibilidad de pérdida en que incurre la organización al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas legales, de la inobservancia de disposiciones reglamentarias, de códigos de conducta o normas éticas o regulaciones y obligaciones contractuales.

El riesgo legal surge también como consecuencia de fallas, errores u omisiones en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

El riesgo Regulatorio se refiere a los riesgos derivados de los cambios en las normas que rigen la entidad o la actividad.

4.39 Riesgo de Liquidez (RL)

Posibilidad de que una Empresa no sea capaz de adquirir u obtener fondos necesarios para atender el pago de obligaciones tanto en el corto, mediano o largo plazo**.**

4.40 Riesgo de Mercado (RM)

El riesgo de mercado, también conocido como riesgo sistemático, es la posibilidad de incurrir en pérdidas asociadas al incremento no esperado en el monto de sus obligaciones con acreedores externos, o a la pérdida de valor de activos, o a cambios en el valor de los portafolios, a causa de variaciones en las tasas de interés, tasa de devaluación o cualquier parámetro de referencia que produzca cambios en el precio de los instrumentos financieros en los cuales se mantienen posiciones dentro o fuera del balance. Incluye el Riesgo de Contraparte.

4.41 Riesgo de Seguro

Consiste en la posibilidad de incurrir en pérdidas por riesgos propios de la actividad de aseguramiento y asociados a los eventos cubiertos por los productos de cada línea de negocio, así como a los procesos asociados con la administración del negocio del seguro; en particular por los riesgos de suscripción, de tarifación, de descuento sobre primas, de mortalidad y morbilidad, de concentración, de siniestros, de diseño, de retención, de comportamiento inesperado del asegurado, de diferencias en condiciones y de insuficiencia de primas y de reservas técnicas, entre otros.

4.42 Riesgo Inherente

Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

4.43 Riesgo Operativo (ROP)

Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.

Para identificar y evaluar los riesgos operativos se requiere comprender la organización, sus procesos, sus capacidades, sus metas y objetivos y las estrategias para lograrlos, porque es en éste contexto que se gestionan los riesgos de la operación.

Es necesario que éste análisis garantice el alineamiento de la operación, incluyendo toda la cadena de valor, la red de contratistas y la gestión de sus riesgos con el Sistema de Gestión.

4.43.1 Clasificación de los eventos de riesgo operativo

Para todos los efectos, los riesgos operativos se clasifican de la siguiente manera como Riesgos de:

4.43.1.1 Relaciones Laborales

Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

4.43.1.2 Clientes

Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

4.43.1.3 Daños a activos físicos

Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.

4.43.1.4 Fallas tecnológicas

Pérdidas derivadas de incidentes por fallas tecnológicas.

4.43.1.5 Fraude Externo

Actos realizados por una persona externa a la entidad que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

4.43.1.6 Fraude Interno

Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad.

4.43.1.7 Ejecución y administración de procesos

Pérdidas derivadas de errores en la ejecución y administración de los procesos.

4.44 Riesgo Propio del Negocio

Es la posibilidad de pérdida en que incurre la organización por riesgos propios de la naturaleza de los sectores o los negocios específicos y en desarrollo de su objeto social. Por ejemplo: riesgos del sector salud, del sector financiero, sector recreación y turismo, o protección.

4.45 Riesgo Reputacional

Es la probabilidad de pérdidas en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios; o derivadas de acciones de mercado o sanciones impuestas, por la autoridad; debilidades financieras que minen la confianza de los clientes o acreedores, procesos judiciales, fallas en la prestación del servicio, entre otras, que causen pérdida de asociados/clientes/usuarios, procesos judiciales, disminución de ingresos o aumento de costos.

4.46 Riesgo Residual

Nivel resultante del riesgo después de aplicar los controles (Riesgo que permanece).

4.47 Riesgos Propios

Corresponde a la probabilidad de pérdida como consecuencia de la materialización de riesgos inherentes a los procesos propios de cada actividad y/o sector.

4.48 Riesgos Sociales

Los riesgos relacionados con efectos negativos ocasionados al medio ambiente, a los grupos de interés o a la sociedad, derivados de decisiones, operaciones o actividades del **GECC**.

4.49 Seguridad de la Información

Medidas preventivas y reactivas de las personas, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información,

buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Se entiende como la preservación de las características: confidencialidad, integridad y disponibilidad de la información. Pueden estar involucradas características adicionales: autenticidad, responsabilidad, no repudio y confiabilidad.

4.50 Sistema de Gestión de Riesgos (SGR)

Es el conjunto de políticas, estructuras, objetivos, metodologías, procedimientos y procesos para la administración y el desarrollo sistemático de las tareas de planear, hacer, verificar y ajustar y mejorar las acciones frente al riesgo, el cual debe hacer parte integral de los Sistemas de Gestión del **GECC**.

4.51 Tolerancia de Riesgo

Es la capacidad de aceptar riesgo; es el grado de variación de apetito de riesgo que se considera aceptable y que los inversionistas o la organización pueden o están dispuestos a soportar.

4.52 Tratamiento del Riesgo (Manejo)

Proceso de selección e implementación de medidas con el fin de reducir la probabilidad de ocurrencia o la severidad de las consecuencias del riesgo, modificando el riesgo.

5. MARCO DE REFERENCIA PARA LA GESTIÓN DEL RIESGO

5.1 Definición Del Sistema de Gestión de Riesgo en el GECC

La Gestión del Riesgo es el proceso mediante el cual se contextualizan, identifican, analizan, evalúan, tratan o manejan, monitorean, controlan y comunican los riesgos generados en una actividad, función o proceso, de tal forma que le sea posible a las empresas u organizaciones minimizar las pérdidas y maximizar las oportunidades; consiste en un conjunto de actividades coordinadas para dirigir y controlar una organización con respecto al Riesgo.

La Gestión Integral de Riesgos constituye una práctica inherente a la actividad empresarial y por ello obedece al direccionamiento estratégico del **GECC** para preservar la integridad de los recursos empresariales, incrementar la ventaja competitiva, garantizar la continuidad del negocio y contribuir a la creación de valor frente a los diferentes riesgos a los cuales se ve expuesta la organización.

El GECC sigue una política de Gestión de Riesgo á definida desde el contexto estratégico, alineada con la política corporativa, teniendo en cuenta la naturaleza del negocio y unas metas y objetivos muy claros.

El Sistema Corporativo de Gestión del Riesgo en el **GECC** está compuesto por los siguientes sistemas y subsistemas:

- Subsistema de Gestión de Riesgo Estratégico (Incluye la Gestión de los Riesgos de Gobierno Corporativo)
- Subsistema de Gestión de Riesgo de Conglomerados
- Subsistema de Gestión de Riesgo Operativo (SGRO)
- Subsistema de Gestión de Riesgo de Liquidez (SGRL)
- Subsistema de Gestión de Riesgo de Mercado (SGRM) (Incluye Riesgo de Contraparte)
- Subsistema de Gestión de Riesgo de Crédito (SGRC)
- Subsistema de Gestión del Riesgo del Lavado de Activos y Financiación del Terrorismo (LA/FT)
- Subsistema de Gestión del Riesgo de Fraude y Corrupción
- Subsistema de Gestión de Riesgos en Proyectos
- Subsistema de Gestión de Riesgo Propio del Negocio
- Sistema Especial de Administración de Riesgos de Seguros (SEARS)
- Sistema de Gestión de la Continuidad del Negocio (SGCN)
- Sistema de Gestión de la Seguridad de la Información (SGSI)

5.2 Políticas para la Gestión de Riesgo

5.2.1 Objetivo

Mediante la definición de las Políticas de Gestión del Riesgo, el **GECC** establece sus criterios y define los elementos y el marco general de referencia y actuación para implementar y gestionar integralmente sus riesgos, sin perjuicio de las políticas específicas que se definan para los diferentes negocios y sectores en los cuales participa.

Las Políticas de Gestión del Riesgo establecidas en el presente Manual y en aquellos que lo complementan, son de obligatoria aplicación en EL GECC y en todas las áreas y procesos que conforman el **GECC**, con el fin de propender por el cumplimiento de la misión y objetivos estratégicos de cada una de las empresas y unidades que lo conforman en particular y del Grupo en su conjunto y coadyuvar a garantizar el cumplimiento de sus compromisos con todos los grupos de interés.

5.2.2 Política General

El **GECC** entiende que una organización sostenible es aquella que gestiona sus riesgos y oportunidades, logrando el balance en las dimensiones económica, social y ambiental para el cumplimiento de su estrategia.

Para ello se compromete a revisar periódicamente las estrategias, identificando los riesgos relevantes frente a los objetivos, el gobierno corporativo, la sostenibilidad y la continuidad de operaciones, teniendo en cuenta los grupos de interés y los cambios en el entorno interno y externo: cambios normativos, la política macroeconómica, la recomposición de la competencia y, en general, el comportamiento del mercado, así como el funcionamiento interno de la organización, incluyendo el análisis de la cadena de valor y la dinámica de los negocios.

5.2.3 Aplicación

El marco de referencia establecido para la gestión de riesgo corporativo se debe cumplir efectivamente en todo el GECC y debe ser garantizado y patrocinado por la Alta Gerencia.

5.2.4 Gobierno Corporativo del GECC

Debe proporcionar mecanismos que aseguren la existencia y puesta en práctica de elementos que permitan el balance entre la gestión de cada órgano y el control de dicha gestión mediante sistemas de pesos y contrapesos, con el fin de que las decisiones adoptadas en cada instancia se realicen con un adecuado nivel de comprensión y entendimiento y de acuerdo con el mejor interés de la entidad, sus asociados, sus accionistas, sus inversionistas y acreedores y respetando los derechos de los usuarios, los clientes y de todos los grupos de interés.

5.2.5 Planificación, gestión y toma de decisiones

La gestión del riesgo debe estar incorporada en el proceso de planeación estratégica e integrada a cada función de negocio, dentro del proceso gestión del día a día y de toma de decisiones en todos los niveles de la organización, permitiendo contar con mejor información acerca de posibles efectos, tanto positivos como negativos de las decisiones.

5.2.6 Monitoreo y control de las estrategias

El **GECC** garantiza el monitoreo y control de todas las estrategias implementadas en la organización, siempre teniendo en cuenta el enfoque de riesgo. Los impactos que se generen por desviación en el cumplimiento de metas se informarán al Consejo de Administración o a las Juntas Directivas, directamente, o a través del

cuerpo colegiado que los asesora (Comité de Riesgo), con el correspondiente plan de acción, tendiente a normalizar la situación.

5.2.7 Integración en la cadena de valor

El **SGR** es una herramienta de gestión gerencial de tal manera que el proceso de gestión del riesgo hace parte de los procesos estratégicos de su cadena de valor y fortalece el ambiente de control interno. Para ello se debe desarrollar un lenguaje común con un alto grado de integración, comunicación y coordinación entre las áreas de tecnología de la información, control, auditoría interna, cumplimiento y gestión del riesgo, así como un enfoque colaborativo y de reporte unificado para la gestión de los riesgos a lo largo de toda la cadena de valor en todo el **GECC**.

5.2.8 Integración de los Sistemas de Gestión

Los sistemas que conviven al interior de la entidad, a saber: Sistema de Gestión Integral, Sistema de Garantía de la Calidad, Sistema de Gestión del Riesgo, Sistema de Control Interno, Sistema de Sostenibilidad y Responsabilidad Social, entre otros, operarán de manera integrada y sinérgica, siempre en función del cumplimiento de los Objetivos Misionales de la Organización.

5.2.9 La Estructura del Gobierno de Riesgos en el GECC

Está conformada por el Consejo de Administración de Coomeva, las Juntas Directivas de las empresas, los Comités de Auditoría, los Comités de Riesgo, la Presidencia Ejecutiva del Grupo Coomeva, las Presidencias y Gerencias de las empresas, la Unidad Corporativa de Gestión del Riesgo, las Vicepresidencias y áreas de riesgo de las empresas y unidades de negocio, las Gerencias y Direcciones Corporativas y de las Unidades de Negocio, los Comités específicos por tipo de riesgo, la alta dirección y los responsables de todas las áreas, procesos, proyectos, productos, negocios y todos los colaboradores.

5.2.10 Gobierno de Riesgos

La **Unidad Corporativa de Gestión del Riesgo** como líder del proceso, así como las áreas encargadas de la gestión del riesgo en las empresas y unidades de negocio del **GECC**, reportarán al máximo nivel jerárquico de cada entidad, serán independientes del órgano de control, y de todas las áreas de negocio y de los procesos que soportan la administración y operación de las empresas, los cuales generan y gestionan los riesgos, de tal manera que se garantice total autonomía y transparencia y se eviten los conflictos de interés.

5.2.11 Escalamiento y Delegación de Autoridad

En el GECC, se debe definir el proceso de delegación de autoridad para la aceptación de los niveles de riesgo, el cual debe ser comunicado a toda la organización.

La toma de decisiones frente a posiciones que excedan los límites de apetito de riesgo fijados deberá contar con niveles de aprobación sucesivamente más altos dentro de la organización a medida que se aumenta el margen de tolerancia, llegando hasta el Consejo de Administración, Juntas Directivas o Asambleas Generales, según el caso.

Esta definición debe establecer claramente los límites para cada posición y los niveles de aprobación y escalamiento. Su no cumplimiento configura una falta disciplinaria frente a la cual se establecerá el régimen de sanciones correspondiente, sin perjuicio de las medidas legales que puedan emprenderse por violación a la normatividad interna o externa.

5.2.12 Definición de Roles

Con el fin de implementar el **SGR**, la alta dirección de la Cooperativa, de las empresas y unidades de negocio del **GECC** deben asignar a cada una de las áreas y colaboradores los roles, funciones y responsabilidades que consideren necesarios y pertinentes, de acuerdo con su estructura organizacional, su cadena de valor y su perfil de riesgo y que estén orientadas a facilitar su participación en la definición y gestión de los aspectos que rigen el **SGR** y su monitoreo a través del tiempo.

5.2.13 Responsabilidades de los colaboradores

Todos los colaboradores del **GECC** están en la obligación de cumplir las políticas, procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento de los Sistemas de Gestión de Riesgo, orientando sus acciones a la comunicación y mitigación de los riesgos y particularmente a la recolección y análisis de información.

Los colaboradores son responsables de la correcta aplicación del Sistema de Gestión del Riesgo, mediante la comunicación de los riesgos que podrían afectar la organización y la identificación, evaluación, manejo, monitoreo, comunicación y divulgación de los riesgos asociados con los propios procesos a cargo, implementando los mecanismos de verificación.

Es deber de todos los colaboradores denunciar y alertar sobre hechos que conozcan y que puedan vulnerar la imagen y la reputación de la organización o que puedan derivar en la pérdida de confianza pública hacia la misma.

Cualquier conflicto de intereses que pueda surgir, deberá ser resuelto e informado a las instancias correspondientes por el líder del área de riesgo de cada empresa.

5.2.14 Gestión del Desempeño

Los criterios e indicadores de gestión del riesgo deben formar parte de la definición de metas y logros en el **GECC,** así como de las evaluaciones de desempeño y del plan de incentivos de los gerentes y directivos a nivel nacional, regional y local, por cuanto el logro de los objetivos está ligado a las implicaciones de los riesgos, cuya gestión forma parte de las responsabilidades de trabajo en equipo y de la rutina diaria para todos los colaboradores.

5.2.15 Cultura Organizacional

El **GECC** desarrollará una cultura orientada a anticipar y gestionar los riesgos de la organización, por lo cual, este será un tema prioritario en los procesos de fortalecimiento del talento y la cultura, al cual se destinarán los recursos necesarios para la formación y para la generación de campañas motivacionales y de difusión de políticas, de prácticas, de controles internos y de casos.

5.2.16 Presupuesto

El **GECC** debe asegurar las partidas presupuestales, recursos humanos, tecnológicos y demás que se requieren para la estructuración, implementación y operación del Sistema de Gestión del Riesgo, incluyendo las iniciativas, proyectos y decisiones necesarias para el debido tratamiento y monitoreo de los riesgos.

5.2.17 Racionalidad Económica

EL **GECC** propenderá por la eficiencia y la integralidad en la gestión de riesgos, por lo cual las medidas adoptadas para el tratamiento de riesgos y mejoras del **SGR** deben contar con el sustento necesario y la evaluación de su costo/efectividad.

5.2.18 Disciplina de Análisis de Causa Raíz

El GECC adelantará una gestión proactiva de los riesgos, para lo cual impulsará un enfoque de análisis que permita desarrollar escenarios y realizar un seguimiento de los eventos, rastreando la causa raíz de los problemas, de forma que ligue los eventos con sus procesos fuente para reducir la incertidumbre y guiar la recopilación de información y la medición de la efectividad de los controles.

5.2.19 Apetito de Riesgo

El GECC definirá y contará con límites de riesgo explícitos acerca del grado de exposición que tanto la administración, como el Consejo de Administración y las Juntas Directivas, están dispuestos a aceptar para el logro de los objetivos estratégicos y las metas, entendiendo y aprovechando el balance de riesgo-beneficio-oportunidad dentro de los negocios y las empresas. El apetito de riesgo será periódicamente revisado.

5.2.20 Tolerancia al Riesgo

El GECC establecerá un nivel de tolerancia al riesgo que defina el grado de variación de apetito de riesgo que consideran aceptable y que los asociados, los inversionistas y la organización están dispuestos o en capacidad de soportar o aceptar, de tal forma que no se comprometa la oferta de valor, el cumplimiento de los objetivos institucionales, ni la sostenibilidad del negocio.

5.2.21 Perfil de Riesgo

El **GECC** definirá su perfil de riesgo en congruencia con su direccionamiento estratégico, el cual debe ser avalado por el Consejo de Administración de Coomeva o las Juntas Directivas según el caso.

5.2.22 Perfil de Riesgo en Inversiones

El **GECC** garantizará que sus inversiones empresariales y de portafolio cumplan con los principios de rentabilidad y de no concentración, que inviertan en instrumentos y entidades con baja exposición al riesgo y que éstas en todo caso cumplan con los límites de apetito de riesgo definidos por la Alta Dirección.

5.2.23 Continuidad de Negocio

Los aspectos de resiliencia y sostenibilidad del negocio deben ser considerados a través de cada paso del proceso de gestión del riesgo y deben estar integrados a la planeación operativa, con un alcance más allá de la recuperación de las plataformas tecnológicas, garantizando un enfoque integral que considere todos los aspectos internos de la organización, de las personas, de la tecnología, de los sistemas, de los procesos, de las relaciones y lo externo.

5.2.24 Transparencia, comunicación y cultura de reporte

El **GECC** impulsará la adopción de sistemas de información, de control interno y de una cultura de comunicación y reporte permanente de los riesgos hacia todas las partes interesadas, garantizando la evaluación y la disponibilidad de información suficiente, veraz, de calidad y oportuna según las necesidades y competencias de éstas y para la toma de decisiones informadas, así como el establecimiento de líneas y mecanismos de permanente comunicación y reporte

hacia el Consejo de Administración, Juntas Directivas, Presidencias, Gerencias, Comités de Auditoría y Comités de Riesgo.

5.2.25 Gestión del Riesgo en Iniciativas, Proyectos y Decisiones

El **GECC**, incorporará y aplicará el marco de gestión y la metodología del **SGR** en todos los proyectos, iniciativas, nuevos negocios y en las decisiones que adopten, con criterio de flexibilidad y dinamismo, atendiendo las directrices de perfil o apetito de riesgo definido por el Consejo de Administración o las Juntas Directivas.

5.2.26 Gestión del Riesgo de Seguros

Cuando alguno de los integrantes del GECC esté expuesto al riesgo de seguros en razón de la naturaleza de sus negocios y productos, deben implementar y gestionar el Sistema Especial de Administración de Riesgos de Seguros (**SEARS**), garantizando su total independencia de las áreas y personas que realizan los estudios y análisis de mercado, del negocio, de su marcha, suficiencia y operación, así como de los análisis y recomendaciones para la definición de los nuevos productos y la toma de decisiones de gestión.

5.2.27 Gestión del Riesgo de Nuevos Productos, Servicios y Procesos

En el **GECC**, todo diseño o rediseño de procesos/productos/servicios y la definición y el desarrollo de proyectos, será analizado por la Unidad Corporativa de Gestión del Riesgo y/o las vicepresidencias o áreas de riesgo de las empresas correspondientes, a través de la emisión de un informe que contenga los riesgos y fallas identificadas, factores de riesgo relevantes, concentración de riesgos, fallas y/o controles y las recomendaciones a ser tenidas en cuenta por el líder del proceso/proyecto/área.

5.2.28 Gestión del Riesgo de los Proyectos

Todo proyecto desde su concepción como iniciativa hasta el cierre del mismo, debe asegurar la Gestión del Riesgo, enmarcado dentro del Gobierno Corporativo de Riesgos del **GECC**. En tal sentido, todos los proyectos que se aprueben y ejecuten deben contar con el Plan de Gestión de Riesgos en Proyectos, aplicando la metodología del Project Management Institute – Risk Management Process (PMI-**RMP**) y lo establecido en el presente Manual.

5.2.29 Documentación de Procesos

El GECC garantizará la documentación de la totalidad de sus procesos y su oportuna actualización a través de los mecanismos que la Alta Dirección defina en su Sistema de Gestión de la Calidad, para que sirvan como insumo necesario que permita realizar el ciclo de Gestión de Riesgo.

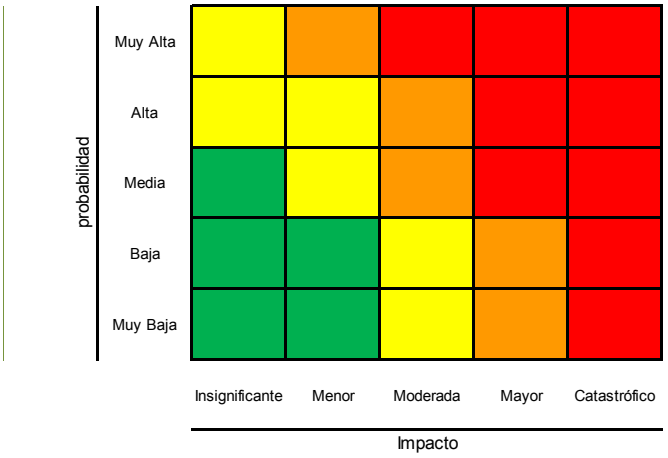
5.2.30 Escalas de Medición del Riesgo

En el **GECC** la medición del riesgo se realiza en escalas de 5 variables, en términos de la probabilidad y el impacto, siendo responsabilidad de cada una de las empresas, determinar las medidas que corresponde a cada variable, que son:

Probabilidad	Impacto
• Muy Alta • Alta • Media • Baja • Muy Baja	• Catastrófico • Mayor • Moderado • Menor • Insignificante

La combinación de probabilidad e impacto define un mapa acogido por el GECC con cuatro zonas de severidad del riesgo:

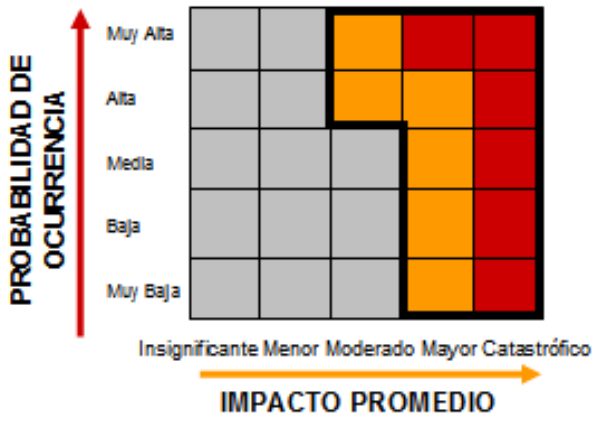
- Crítica (Zona roja)
- Alta (Zona naranja)
- Moderada (Zona Amarilla)
- Baja (Zona Verde)



5.2.31 Riesgo Inaceptable

En el **GECC** se considera inaceptable el Riesgo Residual en las zonas de severidad Crítica (Zona roja del mapa) y Alta (Zona naranja del mapa), y por lo tanto, frente a los riesgos en dichas zonas siempre deben definirse y ejecutarse medidas adicionales para mitigar el riesgo y llevarlo a zonas toleradas, es decir, zonas de severidad Moderada (Zona Amarilla del Mapa) y Baja (Zona verde del mapa), o Zona Gris. Las medidas que se definan deben estar comprendidas en

planes de acción y/o de tratamiento para lograr disminuir el nivel de riesgo, los cuales deben incorporar además las respuestas ante la posible materialización de riesgos.



En todo caso, frente a posiciones que exceden los límites fijados, todos los colaboradores tienen la obligación de acoger y aplicar las definiciones acerca de los niveles de delegación y de escalamiento sucesivo de autoridad establecidos frente a los diferentes límites de riesgo.

5.2.32 Gestión Corporativa del Riesgo desde la Unidad Corporativa de Gestión del Riesgo

Sin perjuicio de las responsabilidades de cada una de las empresas y unidades de negocio del GECC en cuanto a la administración directa de sus propios Sistemas de Gestión del Riesgo y de la autonomía requerida por éstas para su cabal ejercicio, la Unidad Corporativa de Gestión del Riesgo liderará, impulsará, gestionará, monitoreará y evaluará el Sistema Corporativo de Gestión del Riesgo en el GECC.

5.2.33 Gestión del Conocimiento

En el **GECC** propiciará y promoverá el conocimiento sistemático y actualizado de las mejores prácticas en gestión de riesgos y todas las áreas de la organización deben realizar la evaluación de los riesgos, documentando riesgos y oportunidades a partir de la experiencia interna y externa para descubrir dependencias, correlaciones de riesgos y oportunidades, promoviendo siempre la participación de los empleados del front, middle y back.

5.2.34 Aprobación de Cambios

Todo ajuste del Sistema de Gestión de Riesgo requerido por cambios en la normatividad o por disposiciones de carácter interno, será evaluado por el Comité

de Riesgo o quienes hagan sus veces y deberá someterse a aprobación del Consejo de Administración o las Juntas Directivas, según corresponda.

5.3 Gobierno para la Gestión del Riesgo en el GECC

La estructura de Gobierno de la Gestión del Riesgo a nivel Corporativo del **GECC** involucra: al Consejo de Administración, al Comité de Auditoría de **COOMEVA**, al Presidente Ejecutivo del Grupo Coomeva, al Comité Corporativo de Riesgos, a la Unidad Corporativa de Gestión del Riesgo, a la Auditoria Corporativa, a los directivos de las áreas de responsabilidad de dirección, administración, operación y control corporativo y a todos los colaboradores.

La estructura de Gobierno de la Gestión del Riesgo a nivel de las empresas y unidades de negocio del **GECC** involucra: a las Juntas Directivas, a los Comités de Auditoría, a los representantes legales, a los Comités de Riesgos, a las áreas responsables de la Gestión del Riesgo, a la Auditoría Interna, a los directivos de las áreas de responsabilidad de dirección, administración, operación y control, y a todos sus colaboradores.

Las entidades del **GECC** aplicarán el modelo de Gobierno establecido en el presente Manual, sin perjuicio de los ajustes que sean necesarios según las normas empresariales o sectoriales y de organismos de vigilancia y control que le sean aplicables a cada empresa o unidad de negocio y cumplirán como mínimo las siguientes funciones:

5.3.1 Consejo de Administración - Juntas Directivas

En cuanto al riesgo, son funciones del Consejo de Administración de Coomeva y de las Juntas Directivas de las empresas las siguientes:

a) Aprobar el Sistema de Gestión de Riesgos, con base en los estatutos y lineamientos de la organización, según los requisitos expedidos por los entes de control internos y externos, aplicables a cada empresa o sector y exigir y realizar seguimiento a su aplicación y a la alineación con el presente Manual.

b) Adoptar formalmente las políticas, las estrategias y los Manuales generales para la gestión del riesgo en las entidades del **GECC**, expedir las reglamentaciones y fijar las metodologías de medición de riesgo, las responsabilidades y reglas de actuación necesarias para lograr el cabal cumplimiento del **SGR**.

c) Participar de manera efectiva y eficaz en la planeación estratégica, así como en el sistema de control interno y en el proceso de gestión de riesgos y hacer seguimiento y pronunciarse sobre el perfil de riesgo de la entidad.

d) Adoptar formalmente las políticas que definan su posición institucional en materia de exposición al riesgo (límites de apetito de riesgo), reflejando su nivel de tolerancia de una forma coherente con la estructura financiera y operativa y en función de la estrategia corporativa y de los objetivos estratégicos.

e) Establecer los niveles de escalamiento, de decisión y de delegación de autoridad para la definición y aceptación de niveles de exposición y de tolerancia al riesgo a lo largo de la organización.

f) Establecer las medidas relativas al perfil de riesgo, teniendo en cuenta el apetito de riesgo y el nivel de tolerancia al riesgo de la entidad, fijados por la administración, o por el mismo Consejo de Administración o la misma Junta Directiva.

g) Aprobar el diseño y plan de implementación del Sistema de Gestión de Riesgos y sus actualizaciones.

h) Exigir de la administración, reportes periódicos sobre los niveles de exposición a los riesgos, las implicaciones de los mismos y las actividades relevantes para su mitigación y/o adecuada gestión, pronunciándose respecto de los puntos que contengan dichos informes.

i) Conocer toda la información relevante, solicitar aclaraciones, correctivos, hacer seguimientos y presentar informes a las Asambleas Generales de Delegados o de Accionistas según el caso.

j) Aprobar los planes de contingencia y de continuidad del negocio presentados por el Presidente del Conglomerado o Presidente o Gerente General o Director Ejecutivo de las empresas o quien haga sus veces.

k) Aprobar los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el Sistema de Gestión de Riesgos.

l) Aprobar la estructura organizacional que actuará como responsable de la implementación, seguimiento y mantenimiento del Sistema de Gestión de Riesgos.

m) Revisar y aprobar los ajustes requeridos en el **SGR** debido a cambios en la normatividad o por disposiciones de carácter interno

5.3.2 Comité de Auditoría Corporativo de COOMEVA.

El Comité de Auditoría Corporativo de **COOMEVA**, según el Acuerdo No. 443 de septiembre 26 de 2014 del Consejo de Administración de Coomeva, es un órgano asesor del Consejo de Administración, cuyo objetivo principal es supervisar la integridad de los informes financieros y evaluar el sistema de control interno de la Cooperativa, así como su mejoramiento continuo, encaminado a proteger los intereses de los asociados y terceros.

Para el cumplimiento de su objetivo el Comité de Auditoría Corporativo, entre otras, tendrá a cargo las siguientes funciones relacionadas con la Gestión de Riesgos:

a. Evaluar la estructura del Control Interno de la entidad a través de la evaluación que sobre el sistema desarrollan los auditores externos e internos, de forma tal que se pueda establecer si los procedimientos diseñados protegen razonablemente los activos de la entidad, así como los de terceros que administre o custodie y si existen controles para verificar que las transacciones están siendo adecuadamente autorizadas y registradas.

b. Velar porque la preparación, presentación y revelación de la información financiera se ajuste a lo dispuesto en las normas aplicables, verificando que existen los controles necesarios.

c. Examinar el perfil de riesgo de negocio y asegurar que las estrategias de administración de riesgos han sido definidas.

   i. Presentar ante el Consejo de Administración su posición hacia el riesgo y las políticas establecidas para asegurar que la administración opera dentro de estos parámetros.

ii. Entender el marco de la Cooperativa y del Grupo Empresarial Cooperativo para la evaluación de riesgos, la dirección y la asignación de responsabilidades.

iii. Examinar los riesgos a los que el Grupo Empresarial Cooperativo está expuesto y las medidas existentes para su gestión, supervisión y control.

d. Efectuar seguimiento sobre los niveles de exposición de riesgo, sus implicaciones para la entidad y las medidas adoptadas para su control y mitigación, por lo menos cada seis (6) meses o con una frecuencia mayor si así resulta procedente y presentar al Consejo de Administración un informe sobre los aspectos más importantes de la gestión realizada.

e. Proponer al Consejo de Administración, para su aprobación, los programas y controles para prevenir, detectar y responder adecuadamente a los riesgos de fraude y mala conducta entendiendo por fraude un acto intencionado cometido para obtener una ganancia ilícita y por mala conducta, la violación de leyes, reglamentos o políticas internas y evaluar le efectividad de dichos programas y controles.

f. Velar porque existan los controles necesarios para evitar que la entidad sea utilizada como instrumento para la realización de actividades delictivas, en especial para el lavado de activos y la financiación del terrorismo.

g. Revisar las operaciones entre partes relacionadas.

h. Analizar el funcionamiento de los sistemas de información, confiabilidad y su integridad para la toma de decisiones.

i. Revisar los sistemas puestos en práctica por la Administración para monitorear el cumplimiento con las leyes y regulaciones, lo cual implica:

i. Obtener actualizaciones periódicas de la Administración con respecto al cumplimiento de los resultados de las investigaciones adelantadas por la Administración y del seguimiento a circunstancias de incumplimiento.

ii. Examinar los hallazgos de cualquier revisión realizada por las agencias reguladoras.

iii. Evaluar si todos los asuntos legales y de reguladores han sido considerados en la preparación de los estados financieros.

iv. Revisar el programa para monitorear el cumplimiento del Código de Ética y Código de Buen Gobierno Corporativo y periódicamente, obtener una actualización por parte de la Administración relacionada con su cumplimiento.

j. Asegurar que **COOMEVA** cuente con mecanismos apropiados para tratar asuntos financieros, contables e informes que surjan de asociados, empleados, inversionistas y terceros.

k. Solicitar los informes que considere convenientes para el adecuado desarrollo de sus funciones.

l. Elaborar el informe que el Consejo de Administración deberá presentar al máximo órgano social respecto al funcionamiento del Sistema de Control Interno (SCI), el cual deberá incluir entre otros aspectos:

i. Las políticas generales establecidas para la implementación del Sistema de Control Interno (SCI) de la entidad.

ii. El proceso utilizado para la revisión de la efectividad del Sistema de Control Interno (SCI), con mención expresa de los aspectos relacionados con la gestión de riesgos.

5.3.3 Comité Corporativo de Riesgos

El **GECC** contará con un Comité Corporativo de Riesgos dependiente de la Presidencia Ejecutiva de Coomeva, el cual rendirá informes directamente al Consejo de Administracion y al Comité de Auditoría, con la periodicidad que se establezca en los respectivos reglamentos.

El objetivo primordial de este Comité es el de apoyar al Consejo de Administración, al Comité de Auditoría Corporativo, a las Juntas Directivas, a la Presidencia Ejecutiva del **GECC** y a los Presidentes y Gerentes de las empresas y Unidades de Negocio que lo conforman en la definición, seguimiento y control de las políticas y del Sistema Corporativo de Gestión del Riesgo.

Corresponde al Presidente Ejecutivo reglamentar el funcionamiento de este Comité.

5.3.3.1 Conformación del Comité Corporativo de Riesgos

El Comité Corporativo de Riesgos está conformado por los siguientes Miembros:

- Presidente Ejecutivo de Coomeva, quien preside el Comité y actúa como su vocero.
- Responsable de la Unidad Corporativa de Gestión del Riesgo quien presidirá el Comité cuando el Presidente Ejecutivo no pueda estar presente, o cuando este lo delegue para tal fin.
- Gerente Corporativo Financiero
- Gerente Corporativo Administrativo
- Gerente Corporativo Jurídico
- Gerente Corporativo de Estrategia y Mercadeo

A las reuniones del Comité de Riesgos asistirá en calidad de invitado el Auditor Corporativo.

Actuará como secretario el responsable de la Unidad Corporativa de Gestión del Riesgo. El Comité podrá solicitar la participación de cualquiera de los funcionarios del GECC cuando considere necesaria su presencia en calidad de invitados especiales, con la finalidad de presentar y sustentar temas específicos de interés del Comité.

5.3.3.2 Reuniones

El Comité será convocado por el Presidente Ejecutivo y la periodicidad de las reuniones será mensual.

Como mínimo dos (2) veces al año el Comité sesionará de manera ampliada, con participación de todos los Gerentes y Directores Corporativos y los Presidentes, Gerentes y Directores de las empresas y unidades de negocio del **GECC,** para revisar y trabajar sobre los riesgos del conglomerado.

5.3.3.3 Funciones del Comité Corporativo de Riesgos

El Comité Corporativo de Riesgos deberá cumplir cuando menos con las siguientes funciones:

a) Establecer y garantizar el cumplimiento y aplicación del marco de referencia, políticas y metodologías definidos por el Consejo de Administración de Coomeva para la gestión y administración de riesgos en el **GECC**; velando por

la conveniencia, alcance y eficacia de la Gestión de Riesgo y por la segregación de funciones para garantizar la independencia en la ejecución de las actividades de las áreas comerciales, de control y operativas.

b) Presentar a través de su Presidente, directamente al Consejo de Administración de Coomeva, y a las Juntas Directivas de las empresas del **GECC**, cuando ello sea necesario por tratarse de riesgos que proviniendo de las empresas, expongan al conglomerado, los informes de la gestión de los diferentes riesgos, entregados por la Unidad Corporativa de Gestión del Riesgo o los organismos de control interno y pronunciarse sobre los mismos.

c) Proponer al Consejo de Administración de Coomeva los límites de exposición para los distintos riesgos, revisando los resultados, con el fin de incorporar cambios de acuerdo con las condiciones del mercado, del entorno, la situación del **GECC** o nuevas decisiones derivadas de los análisis de riesgo internos o externos.

d) Para gestionar los riesgos a los cuales está expuesto el conglomerado, el Comité definirá la metodología para análisis y toma de decisiones que permitan a las empresas fijar límites individuales de exposición, de forma que se mitiguen los riesgos del conglomerado en su conjunto.

e) Definir para Coomeva, los procedimientos a seguir en caso de sobrepasar o exceder los límites de exposición establecidos, así como los planes de contingencia a adoptar respecto de cada escenario extremo. En el caso de las empresas y unidades de negocio, el Presidente Ejecutivo recomendará dichos procedimientos a través de sus representantes legales, correspondiendo al Comité velar por su adopción.

f) Velar por la capacitación del personal del **GECC** en lo referente a la gestión y administración de los riesgos, para que al interior de la organización exista el conocimiento adecuado de los riesgos asumidos, su cuantificación y todos asuman la responsabilidad de su tratamiento.

g) Realizar seguimiento y control mensual de las negociaciones y operaciones entre compañías vinculadas, sobre sus condiciones, políticas y límites, así como sobre los indicadores de desempeño de la calidad, eficiencia, oportunidad y legalidad de la gestión entre vinculados económicos y de los planes de acción acordados para garantizar y mejorar dicha gestión, recomendando a la Presidencia Ejecutiva de Coomeva la adopción de las medidas necesarias.

h) Propender e impulsar la disponibilidad de los recursos humanos, técnicos y económicos necesarios para desarrollar la adecuada administración del riesgo en el **GECC**.

i) Velar, en relación con los riesgos en general, que se dé cumplimiento a los lineamientos establecidos en los códigos de buen gobierno, en los códigos de ética y demás normas aplicables especialmente en materia de conflictos de interés y uso de información privilegiada.

j) Revisar y conceptuar sobre los ajustes al **SGR** y controlar que la normatividad emitida por los diversos entes de control en materia de Riesgos, sea adoptada al interior del **GECC** según su aplicabilidad e informar al Consejo de Administración de Coomeva y/o a las Juntas Directivas acerca del impacto de las mismas.

k) Hacer seguimiento mínimo una vez al año, o cuando se requiera o lo exijan las normas, a la metodología de cuantificación de riesgos en relación con todos los sistemas y subsistemas que componen el **SGR** en el **GECC** y pronunciarse respecto a las recomendaciones y planes de tratamiento determinados para cada uno de ellos.

l) Hacer las veces de Comité Directivo de Continuidad del Negocio, el cual aprueba políticas, estrategias y acciones para el mantenimiento y mejora continua de todos los elementos del Sistema de Gestión de Continuidad del Negocio. Adicionalmente, debe atender las situaciones clasificadas como críticas para la organización, involucrando a los colaboradores que sean requeridos, dependiendo del evento.

m) Analizar y evaluar la responsabilidad de los colaboradores, asociados, clientes, usuarios y proveedores de la Cooperativa en los hechos relevantes sujetos de revisión sobre incumplimiento a procedimientos que denoten riesgos operativos, hechos dolosos o fraudes, y ordenar a las áreas correspondientes de la cooperativa, que pongan en marcha las acciones/recomendaciones derivadas de las investigaciones, con el fin de asegurar la operación y mitigar los riesgos.

n) En el caso de incumplimiento a procedimientos que denoten riesgos operativos, hechos dolosos o fraudes en las empresas y unidades de negocio, y dependiendo del nivel de exposición del conglomerado, el Presidente Ejecutivo del GECC les recomendará, a través de sus representantes legales,

poner en marcha las acciones/recomendaciones derivadas de las investigaciones, con el fin de asegurar la operación y mitigar los riesgos.

o) Actuar como facilitador e impulsor a nivel gerencial para la implementación, mantenimiento y mejora del **SGR** y de Gestión de Seguridad de la Información en el **GECC**.

p) Realizar revisiones periódicas del estado del **SGR** y del estado de la información de perfil de riesgo y de gestión de eventos y hacer seguimiento semestral a la evolución del riesgo estratégico y de conglomerado.

q) Evaluar en la Cooperativa los eventos de riesgo materializados de **LA/FT** y adoptar o aprobar decisiones al respecto y velar por que las empresas y unidades de negocio hagan lo propio, evitando la exposición del conglomerado.

5.3.4 Presidente Ejecutivo del GECC, Presidentes, Gerentes Generales o quienes hagan sus veces.

En cuanto al **Sistema Corporativo de Gestión del Riesgo-SGR-** son funciones del Presidente Ejecutivo del **GECC** y de los representantes legales de sus empresas y unidades de negocio:

a) Liderar, impulsar y apoyar permanentemente y a través de toda la organización, el diseño, la implementación, el monitoreo, control y ajuste del **SGR** y la aplicación del presente Manual.

b) Diseñar y someter a aprobación del Consejo de Administración de Coomeva o Juntas Directivas, el **SGR** y sus actualizaciones.

c) Velar por el cumplimiento efectivo de las políticas establecidas por el Consejo de Administración de Coomeva o las Juntas Directivas en relación con el **SGR**.

d) Asegurar la implementación y el mantenimiento adecuado de cada una de las etapas y elementos del SGR en concordancia con los objetivos, planes y procedimientos establecidos en los manuales de riesgos, con especial énfasis en aquellas empresas o unidades que por las normas propias de su actividad requieren un mayor rigor y profundidad (financiero, protección y salud).

e) Velar por la correcta implementación de los procedimientos para la adecuada gestión del riesgo a que se vea expuesta la entidad en desarrollo de su actividad

f) Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de riesgos implica para la entidad.

g) Realizar un seguimiento permanente de la aplicación del **SGR**, incluyendo los aspectos de cultura organizacional requeridos para su buen desarrollo y su alineación con el presente Manual.

h) Asignar los roles y responsabilidades a la estructura que actuará como responsable de la implementación, seguimiento y mantenimiento del **SGR**, asegurando la idoneidad técnica del recurso humano asignado.

i) Establecer claramente los responsables de la gestión del riesgo para cada una de las áreas, procesos, proyectos, productos y negocios a lo largo de toda la organización y frente a cada actividad de los Planes de Gestión del Riesgo.

j) Apropiar y garantizar la disponibilidad de los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el Sistema de Gestión de Riesgos.

k) Adoptar las medidas relativas al perfil de riesgo en concordancia con las políticas y lineamientos definidos por el Consejo de Administración de Coomeva o de la respectiva Junta Directiva.

l) Velar por la correcta aplicación de los controles del riesgo identificado y medido.

m) Adoptar los correctivos para los procesos de administración de riesgos que sean de su competencia y proponer los que estime convenientes al Consejo de Administración de Coomeva o a las Juntas Directivas.

n) Realizar seguimiento permanente al nivel de riesgo de la entidad y establecer el mecanismo de reporte y comunicación periódica de la Administración al máximo órgano de dirección (Consejo de Administración y/o Junta Directiva)

o) Presentar un informe periódico, como mínimo de forma trimestral, al Consejo de Administración de Coomeva o a la Junta Directiva respectiva acerca de la evolución y aspectos relevantes del **SGR**, incluyendo, entre otros, el nivel de riesgo de la entidad, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

p) Realizar seguimiento sistemático a las medidas de tratamiento adoptadas para los riesgos, así como las acciones que se deriven para atender los eventos que se materialicen.

q) Establecer el ámbito de interacción, así como, la forma y los mecanismos de comunicación y consulta con la Auditoría Interna, la Revisoría Fiscal y las otras áreas que deben concurrir en el propósito de mejorar la gestión del riesgo.

r) Incluir los criterios e indicadores de resultado de la gestión del riesgo como parte integral de la fijación de metas y logros, así como de las evaluaciones de desempeño y del plan de incentivos y promociones de los gerentes y directivos de cada una de las áreas a nivel nacional, regional y local.

5.3.5 Unidad Corporativa de Gestión del Riesgo.

La **Unidad Corporativa de Gestión del Riesgo,** cumplirá con las responsabilidades establecidas en el Acuerdo **AC-CA-GH-2014.444** del 26 de Septiembre de 2014, aprobado por el Consejo de Administración de COOMEVA, o con las que se establecieren en las normas que lo modifiquen o sustituyan.

Frente a los sectores, empresas y unidades de negocio del GECC, y con el fin de precisar el alcance de las responsabilidades de la Unidad Corporativa de Gestión del Riesgo establecidas en el mencionado acuerdo, la Unidad en términos generales responderá por:

5.3.5.1. Alcance a todo el GECC:

La Unidad Corporativa de Gestión del Riesgo debe:

a) Definir, diseñar, proponer e impulsar la adopción e implementación de un marco de referencia estandarizado que garantice un lenguaje común en cuanto a políticas, estrategias, lineamientos, metodologías, indicadores, metas, procedimientos, instrumentos y reglas de actuación que permitan el desarrollo de sinergias, la coordinación e interacción, la integralidad, la eficiente y efectiva recolección de información, la comparabilidad y la consolidación de datos estructurados para el correcto análisis de la agregación de riesgos y del nivel de exposición a los mismos, con el fin de garantizar la óptima gestión y toma de decisiones frente a los riesgos estratégicos y de conglomerado del GECC.

b) Impulsar y supervisar que en todo el GECC, cada una de las empresas y unidades de negocio cumpla con la adopción y correcta implementación y gestión del marco de referencia, las políticas, estrategias, lineamientos,

metodologías, indicadores, metas, procedimientos, instrumentos y reglas de actuación corporativas establecidas por el Consejo de Administración.

c) Diseñar, planificar, dirigir, implementar, administrar, mantener, coordinar y realizar el monitoreo, supervisión y control de los riesgos de conglomerado y estratégico del GECC (como Grupo).

d) Implementar un sistema de reportes periódicos que le permita conocer, consolidar, analizar e informar acerca del estado de los riesgos estratégicos y de conglomerado del GECC, definiendo la información que periódicamente y con tal fin, deberán obligatoriamente reportarle las entidades que lo conforman.

e) Evaluar el marco de referencia, las políticas, estrategias, lineamientos, metodologías, indicadores, metas, procedimientos, instrumentos, reglas de actuación y normatividad vigente y proponer los ajustes que sean necesarios.

f) Brindar apoyo, asesoría y capacitación al GECC.

En todo caso, Bancoomeva, Coomeva Corredores de Seguros, Coomeva Servicios Administrativos y todas las empresas del Sector Salud son responsables de aprobar, implementar, gestionar, monitorear y evaluar directamente sus propios Sistemas de Gestión del Riesgo, y de desarrollar los esquemas de gestión para los riesgos propios de cada negocio, definiendo autónomamente los respectivos controles y planes de tratamiento.

5.3.5.2. Alcance a Coomeva y sus Fondos Mutuales, al Sector Recreación y a Coomeva Fundación:

Además de las funciones ya establecidas, la Unidad Corporativa de Gestión del Riesgo será responsable de:

a) Dirigir, planificar, implementar gestionar, mantener, coordinar y realizar el monitoreo, supervisión y control directo del Sistema de Gestión del Riesgo y de los Sistemas y Subsistemas que lo conforman, en Coomeva Cooperativa y sus Fondos Mutuales, en las empresas del Sector Recreación y en Coomeva Fundación.

b) Definir con la Alta Dirección de la organización el nivel de tolerancia al riesgo que están dispuestos a asumir.

c) Diseñar, construir, mantener y administrar las bases de datos relacionadas con la medición y evaluación del Sistema de Gestión de Riesgos.

Con el fin de garantizar la sinergia, alineación, integralidad, coordinación y lenguaje común, la Unidad Corporativa de Gestión del Riesgo en el GEC y para sus empresas, fondos mutuales y unidades de negocio, ejercerá funciones de dirección y coordinación técnica en cuanto al Gobierno del Riesgo, los responsables de la gestión del riesgo, la Gestión del conocimiento de los riesgos y la gestión del Sistema Corporativo de Gestión del Riesgos**.**

5.3.6 Comités Técnicos Corporativos de los Subsistemas de Riesgo

Con el fin de fortalecer la alineación, el análisis integral de los riesgos del **GECC**, el desarrollo de un lenguaje común, la sinergia, la gestión del conocimiento, la cultura de gestión de riesgos, la adopción de mejores prácticas, la autoevaluación de la gestión individual y conjunta de los colaboradores responsables de las áreas de gestión del riesgo en el GECC y para que sirva como herramienta de apoyo técnico a la gestión de la Unidad Corporativa de Gestión del Riesgo, ésta propondrá a la Presidencia Ejecutiva la conformación de los Comités Técnicos para los diferentes sistemas y subsistemas de riesgos establecidos en el numeral 2 del presente Manual, los cuales estarán conformados por los colaboradores de las áreas responsables de la gestión del riesgo en el GECC y por los dueños de los riesgos, siendo una responsabilidad inherente al cargo desempeñado por cada colaborador que integre cada uno de los comités, la obligación de asistir, participar y cumplir con las tareas encomendadas.

Los Comités podrán solicitar la participación de cualquiera de los funcionarios de Coomeva o sus empresas, cuanto consideren necesaria su presencia en calidad de invitados especiales, con la finalidad de presentar y sustentar temas específicos de interés del Comité.

Los Comités serán liderados y coordinados por el responsable de la Unidad Corporativa de Gestión del Riesgo o por quien este delegue y estarán conformados por los responsables de la gestión de los riesgos y sus subsistemas en el **GECC**. El alcance de la gestión de estos Comités es técnico y administrativo, no decisorio.
La Unidad Corporativa de Gestión del Riesgo, reglamentará el funcionamiento de dichos Comités.

5.3.7 Auditoría Corporativa

En cumplimiento de sus funciones de evaluar y supervisar el control interno para Coomeva y sus empresas y unidades de negocio y en relación con la gestión de riesgos, corresponde a la auditoría:

a) Proveer asesoría y aseguramiento objetivo sobre la efectividad de las actividades de la Gestión del Riesgo en la organización, monitoreando el proceso y el cumplimiento de políticas y procedimientos, y evaluando las valoraciones del riesgo y los controles por parte de los responsables, para ayudar a asegurar que los riesgos claves del negocio están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente".

b) Contribuir a la mejora de los procesos de gestión del riesgo, de control y de gobierno.

5.3.8 Áreas de responsabilidad de dirección, administración, operación y control, establecidas en la estructura del GECC

Con el fin de brindar seguridad razonable respecto del logro de los objetivos del **GECC**, de sus empresas y unidades de negocio, será una responsabilidad común para todas y cada una de las áreas de dirección, administración, operación y control, establecidas en la estructura del mismo a todo nivel y en todos los ámbitos geográficos:

a) Identificar, evaluar y comunicar los riesgos que podrían afectar la organización.

b) Cumplir las políticas e incorporar la cultura de gestión de riesgos a la planificación, a la toma de decisiones y a la gestión del día a día.

c) Identificar, evaluar y gestionar los riesgos asociados con los propios procesos relacionados con el área a su cargo.

d) Validar y mantener la eficacia de los procesos de control y de los planes de tratamiento establecidos y promover la mejora continua de los mismos.

5.3.9 Todos los colaboradores

Los colaboradores del **GECC** deben:

a) Conocer los riesgos que son inherentes a sus actividades y ser responsables por adelantar una eficiente gestión, control y reporte de los mismos, lo cual debe formar parte de la evaluación de desempeño y de los programas de incentivos de cada colaborador.

b) Participar activamente en las capacitaciones y cursos obligatorios u opcionales que sobre la gestión de riesgos sean puestos a disposición de los colaboradores.

c) Conocer y cumplir las políticas, normas y procedimientos definidos en los manuales de riesgo del **GECC**.

d) Conocer y cumplir con la normatividad y las regulaciones legales vigentes sean aplicables.

e) Conocer y ejecutar los controles definidos en su proceso.

f) Efectuar permanente autocontrol; evaluar y controlar su propio trabajo y en el evento en que se detecten desviaciones o eventos de riesgo, informar a los niveles jerárquicos establecidos según los procedimientos definidos y aplicar los correctivos necesarios

g) Evitar y en todo caso reportar todo conflicto de intereses, propios o de terceros, que puedan presentarse en cuanto a su responsabilidad frente a la gestión de los riesgos.

5.4 Mecanismos de comunicación interna y externa

La Unidad Corporativa de Gestión del Riesgo propondrá a la Presidencia Ejecutiva las políticas, lineamientos, metodologías y directrices generales acerca de los mecanismos y medios de divulgación interna y externa a desarrollar por parte de las empresas y unidades de negocios del **GECC**, a fin de aprovechar sinergias y garantizar un lenguaje común con unidad de criterios para la divulgación de los avances de los diversos subsistemas, teniendo en cuenta, en todo caso, la normatividad aplicable, los desarrollos, las necesidades y posibilidades específicas de cada sector y empresa del **GECC**.

Algunos mecanismos a tener en cuenta son: Publicaciones en intranet, mailings, publicaciones en boletines virtuales, material impreso (Cartillas, agendas, boletines), videos institucionales para colaboradores, publicaciones en la página web, correos electrónicos, videos institucionales en oficinas de atención al público,

espacios en los sobres con correspondencia para asociados, los informes de sostenibilidad, de responsabilidad social empresarial o de balance social, entre otros.

5.5 Mecanismos de capacitación

La capacitación es un factor crítico de éxito en la implementación y mantenimiento de cualquier Sistema de Gestión de Riesgo, por lo cual todas las empresas y unidades de negocio del **GECC** deben contar con un Plan de Capacitación acerca del Sistema Gestión del Riesgo.

Siendo su propósito general facilitar el proceso de implementación y mantenimiento del **SGR** y preparar a los colaboradores para ejecutar eficientemente cada una de sus responsabilidades y roles en relación con el **SGR**, la capacitación se lleva a cabo para contribuir a:

a) Divulgar los objetivos, procesos y demás elementos del **SGR** que provean a los funcionarios del **GECC** de las herramientas necesarias para el ejercicio de sus funciones.

b) Vincular a todos los funcionarios del **GECC** en las distintas etapas de implementación del **SGR.**

c) Dar a conocer a los funcionarios del **GECC** cada una de sus funciones y responsabilidades frente al **SGR.**

d) Fomentar la colaboración y el trabajo en equipo para la gestión del riesgo.

e) Facilitar a los órganos de control la recolección de información durante las etapas de monitoreo y control del **SGR.**

f) Mejorar la interacción entre los colaboradores y, con ello, a elevar el interés por el aseguramiento de las políticas y procesos del **SGR**.

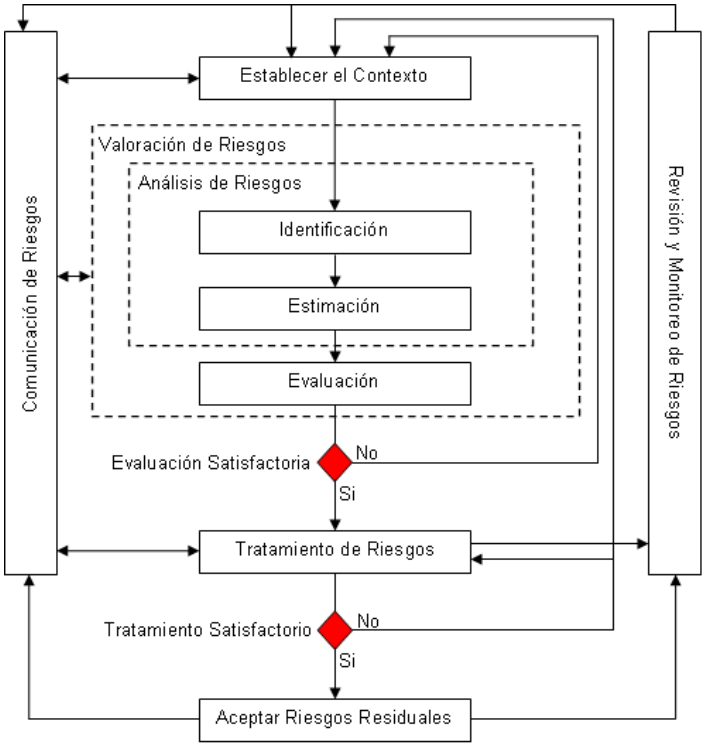
La Unidad Corporativa de Gestión del Riesgo propondrá a la Presidencia Ejecutiva las políticas, lineamientos, metodologías y directrices generales acerca de los mecanismos y medios de capacitación en riesgo a desarrollar en el **GECC**, a fin de aprovechar sinergias y garantizar coherencia y un lenguaje común en la capacitación e información impartida a los diferentes grupos de interés, sin perjuicio de las estrategias particulares que según el perfil y los riesgos propios de cada negocio establezcan las empresas y unidades de negocio del GECC.

La Unidad Corporativa de Gestión del Riesgo, con el apoyo de la Gerencia Corporativa de Gestión Humana deberá definir y realizar seguimiento al Plan de Capacitación Corporativo sobre el **Sistema Corporativo de Gestión del Riesgo,** garantizando como mínimo el cumplimiento de lo dispuesto en los manuales de cada uno de los subsistemas, así como en las disposiciones normativas y requerimientos específicos de los entes de vigilancia y control aplicables a los diferentes sectores y empresas.

6. PROCESO PARA LA GESTIÓN DEL RIESGO

La Gestión del Riesgo se incorpora a los procesos del GECC como herramienta de Gestión Gerencial, propendiendo por la continuidad, la viabilidad y la sostenibilidad del negocio. Es un proceso iterativo e integral que da inicio con el establecimiento del contexto y culmina con la comunicación, divulgación y monitoreo de los riesgos identificados.

Con el fin de implementar adecuadamente el **SISTEMA DE GESTION DE RIESGOS** en el **GECC,** se desarrollará el ciclo de gestión del riesgo que contiene las siguientes actividades:



6.1 Establecer el contexto

Con el fin de establecer el contexto del proceso para la gestión del riesgo, la organización debe articular y analizar sus diferentes objetivos, definir los parámetros (factores) internos y externos que se han de tomar en consideración cuando se procede a gestionar el riesgo y establecer el alcance y los criterios del riesgo para el resto del proceso. Al establecer el contexto es necesario que estos parámetros se consideren en detalle y, en particular, la manera como se relacionan con el alcance del proceso para la gestión del riesgo particular.

6.1.1 Contexto Externo

Ambiente externo en el cual el GECC busca alcanzar sus objetivos: Ambiente Cultural, Social, Político, Legal, Reglamentario, Financiero, Tecnológico, Económico, Natural y Competitivo, bien sea internacional, nacional, regional o local; los impulsores clave y las tendencias que tienen impacto en los objetivos de la organización; y las relaciones con las partes involucradas externas y sus percepciones y valores. Entender el contexto externo es importante con el fin de garantizar que los objetivos y las preocupaciones de las partes involucradas externas se toman en consideración al desarrollar los criterios del riesgo.

6.1.2 Contexto Interno

Ambiente interno en el cual el GECC busca alcanzar sus objetivos: Gobierno, Estructura Organizacional, Políticas, Objetivos, Estrategias implementadas, Sistemas de información, Cultura Organizacional, Normas, Directrices, Modelos adoptados por la organización, forma y extensión de las relaciones contractuales.

El proceso para la gestión del riesgo está alineado con la cultura, los procesos, la estructura y la estrategia de la organización. El contexto interno es todo aquello dentro de la organización que pueda tener influencia en la forma en que la organización gestiona el riesgo.

6.1.3 Contexto del proceso para la Gestión del Riesgo

Este varía de acuerdo con las necesidades del GECC . Implica la definición de los objetivos, las estrategias, el alcance y los parámetros de las actividades de gestión del riesgo, así como la definición de las responsabilidades, de las metodologías, de las formas de evaluación y la definición y justificación de los recursos necesarios, entre otros.

6.1.4 Definir los Criterios del Riesgo

El **GECC** debe definir los criterios que se van a utilizar para la evaluar la importancia del riesgo. Los criterios deben reflejar los valores, objetivos y recursos de la organización. Algunos criterios pueden estar impuestos por requisitos legales y reglamentarios o derivarse de ellos y de otros requisitos a los cuales la organización se suscribe. Los criterios del riesgo deberían ser consistentes con la política para la gestión del riesgo de la organización, estar definidos al comienzo de todo proceso para la gestión del riesgo y ser revisados continuamente.

6.2 Valoración de riesgos

Es el proceso total de identificación, análisis y evaluación del riesgo.

6.2.1 Identificar los Riesgos

Consiste en identificar las fuentes de riesgo, las áreas de impacto, los eventos (cambios en las circunstancias), así como sus causas y consecuencias potenciales. Además se deben determinar y documentar cuáles son las exposiciones al riesgo o vulnerabilidades de las entidad para el negocio en que opera (visión integral de la empresa). Para caracterizar correctamente el riesgo se debe establecer una perspectiva de la entidad en su conjunto y analizar la totalidad de las incertidumbres que la afectan.

6.2.2 Analizar los riesgos

Implica el desarrollo y la comprensión del riesgo. Este análisis brinda una entrada para la evaluación del riesgo y para las decisiones sobre si es necesario o no tratar los riesgos y sobre las estrategias y métodos más adecuados para su tratamiento y también brinda una entrada para la toma de decisiones, en la cual se deben hacer elecciones sobre las opciones que implican diversos tipos y niveles de riesgo.

El análisis del riesgo involucra la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que tales consecuencias puedan ocurrir. Se deberían identificar los factores que afectan a las consecuencias (impacto) y a la probabilidad. El riesgo es analizado determinando las consecuencias y su probabilidad, y otros atributos del riesgo. Un

evento puede tener consecuencias múltiples y puede afectar a objetivos múltiples. También se deben considerar los controles existentes y su eficacia y eficiencia.

6.2.2.1 Establecer los criterios de medición

Dentro del análisis de los riesgos, el primer paso a ejecutar consiste en definir los criterios de evaluación de riesgos, lo cual permite establecer parámetros estándar que soporten la aplicación de la metodología de administración de riesgos para el **GECC**:

- **Probabilidad de ocurrencia:** Es la posibilidad que un riesgo se materialice. Criterio de frecuencia, medida de las veces que puede presentarse un riesgo, expresado como la cantidad de ocurrencias en un tiempo dado. La probabilidad de ocurrencia tiene cinco niveles: muy alta, alta, media, baja y muy baja.

- **Magnitud del impacto:** Es el resultado de la materialización de un riesgo, expresado cualitativa o cuantitativamente. Se definen rangos frente a los posibles resultados asociados a la materialización de un riesgo: catastrófico, mayor, moderado, menor e insignificante. La estimación del impacto se realiza evaluando el efecto de la posible materialización del riesgo.

  Los criterios de probabilidad e impacto deben ser presentados en escalas de 5 variables denominadas de la siguiente manera:

Probabilidad
• Muy Alta
• Alta
• Media
• Baja
• Muy Baja

Impacto
• Catastrófico
• Mayor
• Moderado
• Menor
• Insignificante

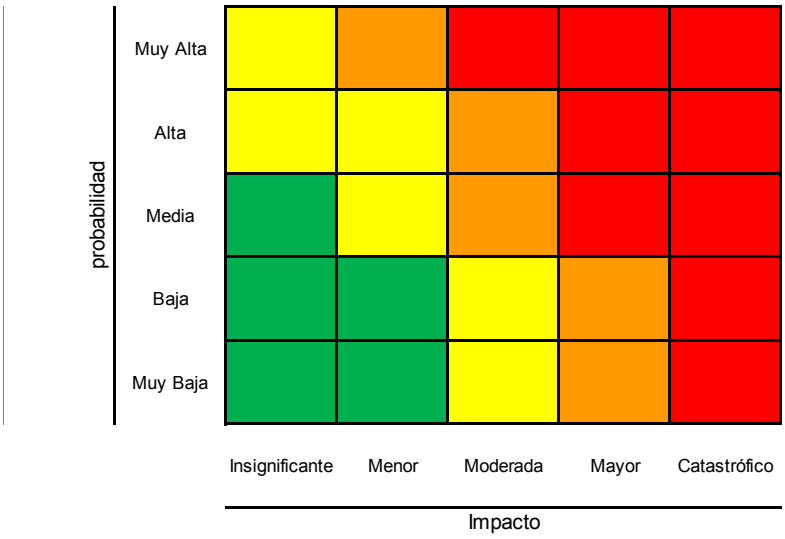
Una vez formalizados los criterios de probabilidad e impacto, se procede a definir el esquema del mapa de riesgos.

- La dimensión del mapa contiene niveles de 5 x 5 para brindar mayor flexibilidad en la determinación de riesgos intermedios.

- La combinación de probabilidad e impacto define las diferentes zonas que conforman el mapa. Se definen cuatro zonas llamadas **zonas de severidad del riesgo**.

- el **GECC** acoge el mapa de riesgo definido por las siguientes zonas:

Severidad del riesgo	Combinación de variables	
	Probabilidad (Eje X)	Impacto (Eje Y)
Crítico	Muy Alta	Catastrófico
	Muy Alta	Mayor
	Muy Alta	Moderado
	Alta	Mayor
	Alta	Catastrófico
	Media	Mayor
	Media	Catastrófico
	Baja	Catastrófico
Alto	Muy Alta	Menor
	Muy Alta	Insignificante
	Alta	Menor
	Alta	Moderado
	Media	Moderado
	Baja	Mayor
	Muy Baja	Mayor
	Muy Baja	Catastrófico
Moderado	Alta	Insignificante
	Media	Menor
	Baja	Moderado
	Muy Baja	Moderado
Bajo	Media	Insignificante
	Baja	Insignificante
	Baja	Menor
	Muy Baja	Insignificante
	Muy Baja	Menor



6.2.2.2 Estimar el nivel de riesgo inherente

Con base en el inventario de riesgos identificados en la etapa anterior (analizándolos sin tener en cuenta ninguna medida de control que se encuentre establecida), se determina la probabilidad de ocurrencia y el impacto del mismo. Teniendo en cuenta las ponderaciones establecidas por zonas, se obtiene la calificación de Probabilidad e Impacto para el Riesgo.

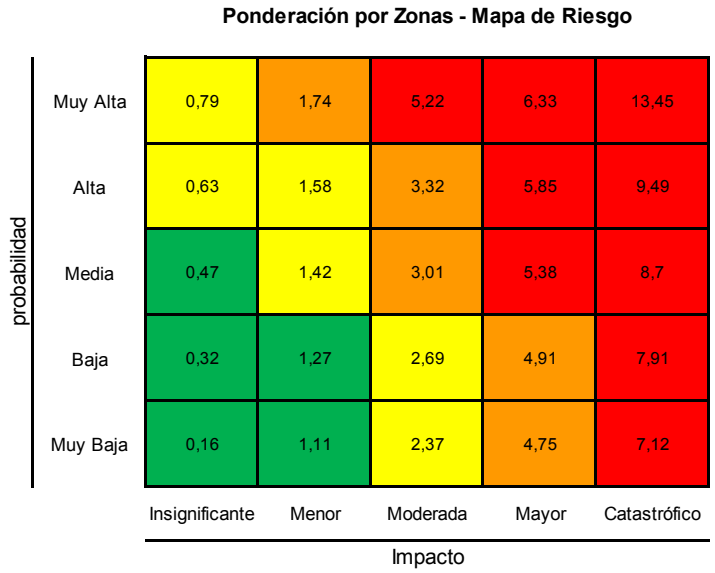


Gráfico x: Ponderación por Zonas – Mapa de Riesgo

6.2.2.3 Identificar y evaluar los controles existentes

Una vez establecidos y calificados los riesgos inherentes, se procede a identificar frente a cada uno de dichos riesgos los controles existentes al interior de la organización y a establecer la descripción para cada control. Posteriormente, se realiza su evaluación en relación con el diseño y la ejecución.

La evaluación de cada uno se realizará por medio de las siguientes variables:

6.2.2.3.1 Diseño de Controles

Para evaluar la forma como fue prescrito el control y la concepción de este, se realiza la calificación de 3 variables:

a) **Tipo de Control:**

Escala	Tipo
10	Preventivo
5	Detectivo
3	No Aplica
1	Correctivo

Los determinadores para la definición de los tipos de control aplicado son:

- **Preventivo:** Usado para prevenir irregularidades. Ej.: Backup de servidores o equipos de cómputo personal.
- **Detectivo:** Detección de ocurrencias irregulares o errores. Ej.: Validaciones de la recuperabilidad de los Backup- Log de errores en el cargue automático de información en los aplicativos- Mallas validadoras en procesos como la compensación.
- **Correctivo:** Recuperar, reparar el daño o minimizar el costo de irregularidades o errores Ej.: Conciliación de cuentas contables realizadas después del cierre – Atención de quejas y reclamos.

b) Naturaleza del Control:

Escala	Naturaleza
10	Automático
5	Semiautomático
3	Manual
1	No Aplica

Define la forma de aplicación de la acción del control. Estas pueden ser:

- **Automático:** Es todo aquel que valiéndose de una herramienta tecnológica es ejecutado automáticamente por el sistema - software.
- **Semiautomático:** Es aquel que se vale de una herramienta tecnológica y del trabajo humano, actuando ambos simultáneamente o en diferentes momentos.
- **Manual:** Es todo aquel que es desarrollado manualmente por parte de un funcionario.

c) Evidencia de ejecución:

Escala	Evidencia
10	Si
5	No
3	No Aplica
1	No Aplica

Los determinadores para la definición la evidencia son:

- **Sí:** Permite definir si actualmente existen evidencias que certifiquen su ejecución, o que en su próxima ejecución existirá trazabilidad
- **No:** No se evidenciará la ejecución del control por medio de elementos que permitan validar trazabilidad o historial.

6.2.2.3.2 Ejecución de Controles

Se realiza para evaluar si la definición de los controles propende por que estos sean operados como fueron prescritos por la administración y para determinar si efectivamente al ejecutarlos éstos contribuyen a disminuir la probabilidad o el impacto del riesgo. Para ello se califican 3 variables:

a) **Documentación/Madurez:**

Escala	Documentación / Madurez
10	Óptimo
8	Monitoreado
6	No Aplica
5	Estandar
4	No Aplica
2	No Aplica
1	Informal

Se utiliza para definir la calidad y efectividad planeada del control. Los determinadores a calificar son:

- **Optimo:** Está documentado, se supervisa sistemáticamente y se han realizado pruebas que demuestran su efectividad.
- **Monitoreado:** Esta documentado y se supervisa su aplicación
- **Estándar**: Está documentado el control
- **Informal:** No está documentado el control

b) Contribución:

Escala	Contribución
10	Alta
8	No Aplica
6	No Aplica
5	Media
4	No Aplica
2	No Aplica
1	Baja

Se utiliza para determinar el impacto del control sobre la causa relacionada. Los determinadores a calificar son:

- **Alta:** El impacto del control es fuerte para mitigar la causa relacionada
- **Media:** El impacto del control es moderado para mitigar la causa relacionada
- **Baja:** El impacto del control es débil para mitigar la causa relacionada

c) Ejecución/Cobertura:

Escala	Ejecución /Cobertura
10	81% - 100%
8	61% - 80%
6	41% - 60%
5	No Aplica
4	21% - 40%
2	0% - 20%
1	No Aplica

Se utiliza para determinar el alcance porcentual del nivel de cobertura, con la aplicación del control sobre la causa identificada. Para calificar esta variable es fundamental reconocer el universo sobre el cual se aplica el control. Los

determinadores de esta variables son los siguientes rangos: (0-20%), (21-40%), (41-60%), (61-80%) y(81-100%).

Adicionalmente, los criterios de diseño tendrán un peso relativo del 40% y los de ejecución el 60%.

Las variables para evaluar el diseño y la ejecución, se ponderan conforme a la siguiente tabla:

EVALUACIÓN DE CONTROLES					
Diseño			Ejecución		
Tipo	15%	40%	Documentación/Madurez	15%	60%
Naturaleza	15%		Contribución	20%	
Evidencia	10%		Ejecución/Cobertura	25%	

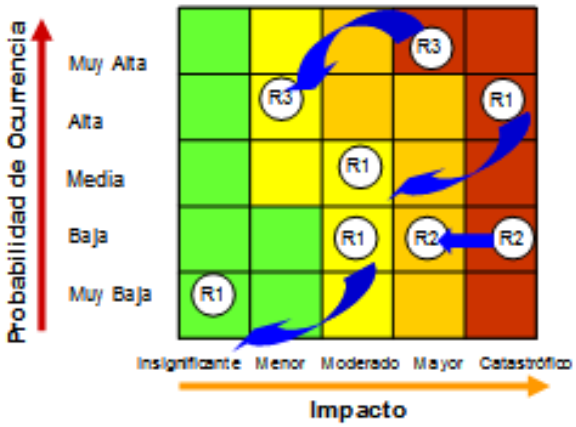
6.2.2.4 Estimar el nivel de riesgo residual

Como resultado final de la etapa de análisis de riesgos, a partir de la evaluación de los controles, se debe determinar el riesgo residual. El resultado de la evaluación de controles corresponde a la exposición final del riesgo.

Para determinar el número de cuadrantes que se desplazará la probabilidad y/o impacto inherente, se tiene en cuenta la siguiente tabla:

CALCULO DEL RIESGO RESIDUAL	
% MITIGACION CONTROL	No. CUADRANTES
81% - 100%	3
61% - 80%	2
41% - 60%	1
21% - 40%	0
0% - 20%	0

El riesgo residual es el resultado del desplazamiento del riesgo inherente por la aplicación de los controles:



6.2.3 Evaluar los riesgos

El propósito de la evaluación del riesgo es facilitar la toma de decisiones basadas en los resultados de dicho análisis, decidir acerca de cuáles riesgos necesitan tratamiento y sobre la prioridad para la implementación del tratamiento.

La evaluación del riesgo implica la comparación del nivel de riesgo observado durante el proceso de análisis y el de los criterios del riesgo establecidos al considerar el contexto. Con base en esta comparación, se puede considerar la necesidad de tratamiento.

La evaluación del riesgo también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente del mantenimiento de los controles existentes. Esta decisión estará influida por la actitud de la organización hacia el riesgo y por los criterios del riesgo que se han establecido.

6.2.3.1 Zonas no toleradas de riesgo

Las zonas no toleradas de riesgo son aquellas zonas en las que el riesgo residual es inaceptable y deben tomarse medidas adicionales para mitigar el riesgo y llevarlo a zonas toleradas (en blanco y negro).

En el **GECC**, las zonas no toleradas de riesgo son:

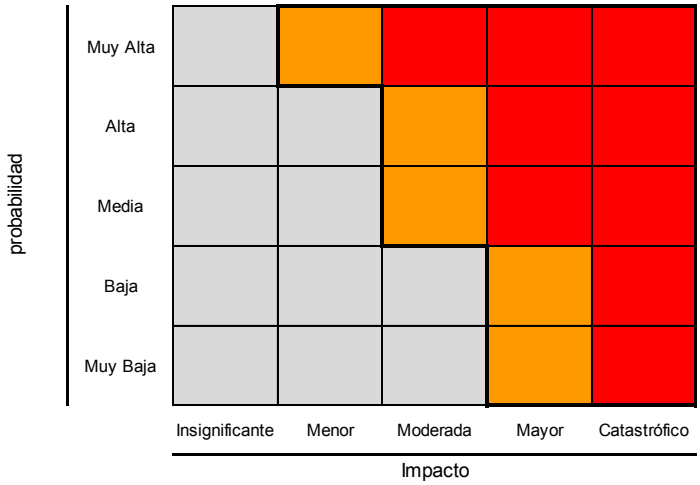
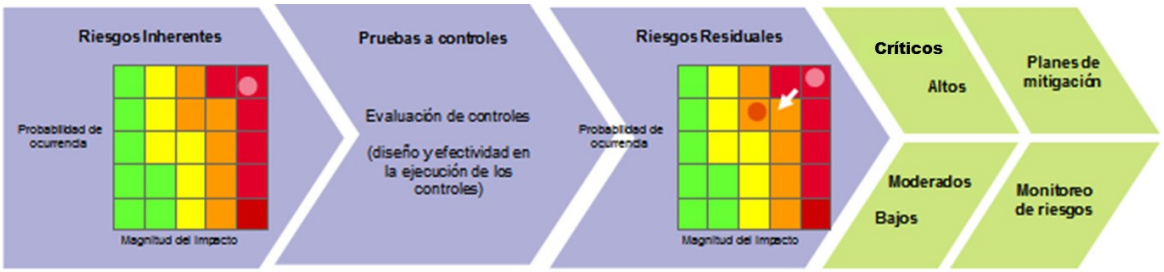


Gráfico x: Mapa de riesgos residuales – Perfil de riesgo

6.2.3.2 Acciones frente al nivel de exposición (severidad) del riesgo

- **Bajo:** Un riesgo situado en esta región del mapa significa que la combinación probabilidad - impacto no implica una gravedad significativa, por lo que no amerita la inversión de recursos y no requiere acciones adicionales para su gestión diferentes a las ya aplicadas.
- **Moderado:** Un riesgo situado en esta región del mapa significa que aunque deben desarrollarse actividades para la gestión sobre el riesgo, estas tienen una prioridad de segundo nivel, pudiendo ser desarrolladas a mediano plazo; estas actividades son de responsabilidad del Líder del Proceso según corresponda y de la Presidencia Ejecutiva, Presidentes o Gerentes Generales.
- **Alto:** Un riesgo situado en esta región del mapa significa que se requiere siempre desarrollar acciones prioritarias a corto plazo para su gestión, debido al alto impacto que tendrían sobre el sistema y la organización. Estas actividades son de responsabilidad del Líder del Proceso según corresponda, de la Presidencia Ejecutiva, Presidentes o Gerentes Generales y del Consejo de Administración o Juntas Directivas. A partir de este nivel, el riesgo no es aceptable por la organización.
- **Crítico:** Un riesgo situado en esta región del mapa significa que bajo ninguna circunstancia se deberá mantener un escenario con esa capacidad potencial de afectar la estabilidad del sistema y la organización. Por ello, estos riesgos requieren una atención de alta prioridad para buscar disminuir en forma inmediata su medida. Las acciones que se definan son de responsabilidad del

Líder del Proceso según corresponda, de la Presidencia Ejecutiva, Presidentes o Gerentes Generales y del Consejo de Administración o Juntas Directivas.



6.3 Tratar los riesgos

El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

6.3.1 Selección de métodos para la administración del riesgo

Se deben determinar las políticas y las acciones tendientes a gestionar los riesgos a los que se ve expuesta la entidad, de acuerdo con los niveles de riesgo determinados. Para el efecto, se contemplan cuatro métodos fundamentales:

d) **Evitar el riesgo:** Decidir no iniciar o continuar la actividad que lo originó

e) **Mitigar el riesgo:** Desarrollar acciones de control para prevenir la materialización del riesgo (atacando la probabilidad de ocurrencia) o adoptar medidas que eviten pérdidas cuando ocurra un evento (mitigando el efecto o el impacto).

f) **Aceptar o retener el riesgo:** tomar o incrementar el riesgo para perseguir una oportunidad

g) **Transferir o compartir el riesgo.** Trasladar las posibles pérdidas a través de arreglos contractuales, tercerización de procesos y seguros, con el fin de compartir el riesgo.

Para aquellos procesos nuevos que están en etapa de definición, se recomienda a partir del riesgo inherente establecer los planes de tratamiento bajo los siguientes criterios:

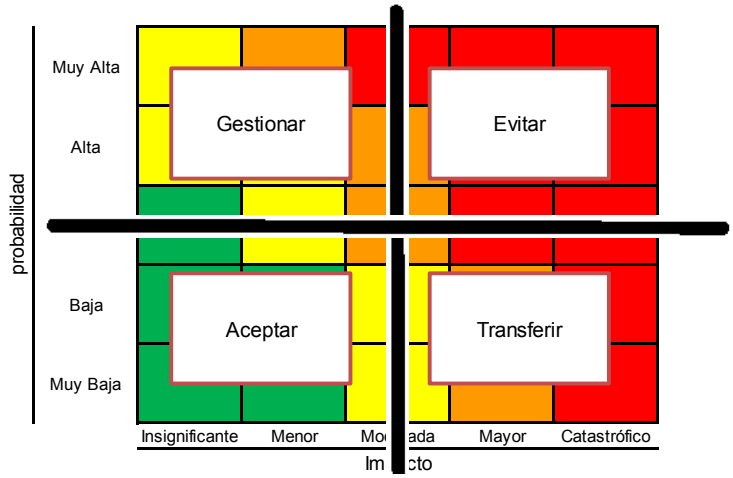


Gráfico X: Matriz de tratamiento de los riesgos inherentes

6.3.2 Controlar el riesgo

El control o tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

El tratamiento implica un proceso cíclico de:

- Valoración del tratamiento del riesgo
- Decisiones sobre si los niveles de riesgo residual son tolerables (apetito de riesgo)
- Cuando los niveles de riesgo residual no son tolerables, debe generarse un nuevo tratamiento para el riesgo.
- Valoración de la eficacia del tratamiento nuevamente aplicado.

La selección de las opciones más adecuadas para el tratamiento del riesgo implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios derivados con respecto a los requisitos legales, reglamentarios y otros, como por ejemplo la responsabilidad social y la protección del ambiente natural. También se deben considerar los valores y las percepciones de las partes involucradas, y las vías más adecuadas para comunicarse con ellos.

El tratamiento también puede introducir riesgos secundarios que es necesario identificar, valorar, tratar, monitorear y revisar.

El propósito de los planes para el tratamiento del riesgo es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas, por lo tanto la información suministrada en los planes de tratamiento debe incluir: las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener; el orden de prioridad en el cual se deben implementar los tratamientos individuales para el riesgo; identificar si surgen riesgos secundarios a causa de la implementación del plan y una clara identificación de aquellos que son responsables de aprobar el plan y los responsables de implementarlo.

Los planes de tratamiento deben integrarse con los procesos de gestión de la organización y se deben construir junto con las partes involucradas pertinentes.

Los encargados de tomar las decisiones y otras partes involucradas deben conocer la naturaleza y la extensión del riesgo residual después del tratamiento del riesgo. El riesgo residual se debe documentar y someter a monitoreo, revisión y, cuando así corresponda, a tratamiento adicional.

El propósito de los planes para el tratamiento del riesgo es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas.

6.3.3 Análisis Costo-Beneficio

Como resultado del análisis costo/beneficio, las empresas y unidades de negocio del **GECC** definirán su apetito de riesgo, conforme a su situación interna y a las propias del entorno que la afecten.

6.4 Monitoreo y Revisión

Debe ser una parte planificada del proceso para la gestión del riesgo e incluir verificación o vigilancia regular. Cada empresa y unidad de negocio del **GECC** definirá de acuerdo con el core de su negocio, cuáles pueden ser periódicos y cuáles no.

El monitoreo debe comprender todos los aspectos del proceso para la gestión del riesgo con el fin de:

- Garantizar la efectividad de los controles.
- Obtener información adicional para valoración del riesgo
- Analizar y documentar las lecciones aprendidas.
- Detectar cambios en el Contexto (parámetros internos y externos)
- Identificar riesgos emergentes

Los resultados del monitoreo y la revisión se deben registrar y reporta interna y externamente según corresponda.

6.5 Comunicación y Consulta

Son procesos continuos y reiterativos que la organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un dialogo con las partes involucradas con respecto a la gestión del riesgo, los cuales deben realizarse garantizando la transparencia.

7. MONITOREO Y REVISIÓN DEL MARCO DE REFERENCIA

Se deberá garantizar que las actividades y planes para llevar a cabo la gestión de los riesgos son adecuados, efectivos y que se estén cumpliendo apropiadamente, para lo cual, como mínimo una vez al año se deberán examinar y evaluar:

- Criterios de evaluación del riesgo e impacto
- Criterios de aceptación de riesgos
- Enfoque para la evaluación del riesgo
- Herramientas y recursos utilizados para la gestión
- Alineación con las políticas corporativas
- Alineación frente a cambios en el plan estratégico y objetivos del **GECC**
- Contexto regulatorio
- Alcance de la gestión y su planificación
- Administración de recursos
- Indicadores de gestión de riesgos
- Costos de la gestión
- Resultados de auditorías internas, externas, revisoría fiscal y/o entes de control sobre la gestión de riesgos
- Cambios en normas que proponen mejores prácticas para la gestión de riesgos

8. MEJORA CONTINUA DEL MARCO DE REFERENCIA

El resultado de la evaluación de los factores expuestos pueden representar la necesidad de implementar cambios sobre la metodología y/o enfoque de la gestión de riesgos, por lo cual, cualquier mejora acordada sobre las etapas/actividades de gestión deberán ser notificadas a la alta dirección y a las partes involucradas a fin de que no sea omitido ningún elemento y se tomen las acciones pertinentes para la comprensión y capacidad de adaptación sobre los cambios propuestos.

Acorde con las falencias detectadas, cada entidad integrante del **GECC** debe definir los planes de acción encaminados a la actualización y mejora del **SGR**, utilizando las herramientas definidas a nivel interno.

9. GRADUALIDAD DE LA IMPLEMENTACIÓN

El marco, las políticas y metodologías establecidas en el presente Manual serán desarrolladas e implementadas acogiendo el principio de gradualidad, ello teniendo en cuenta la naturaleza, normatividad, tipo de negocio y características de cada entidad integrante del **GECC** y basados en el entendimiento de la gestión del riesgo como un proceso, el cual implica sucesivos avances de madurez a lo largo del tiempo.

Cada entidad integrante del **GECC**, según el grado de desarrollo y madurez alcanzado, puede adelantar la implementación de su **SGR,** estructurando un proyecto, basándose para ello en la metodología de Gestión de Proyectos vigente en el **GECC**, con el fin de permitir la visualización del alcance, tiempo y costos que ello implica.

En todo caso, durante los siguientes dieciocho (18) meses a partir de la aprobación del presente Manual, cada una de las entidades integrantes del G**ECC** deberán elaborar y presentar para aprobación de los representantes legales, Consejo de Administración y Juntas Directivas, según el caso, el Proyecto de Implementación del **SGR** a desarrollar hasta el 2018.

El Proyecto de implementación será elaborado con el apoyo de sus respectivas áreas de riesgos y deberá contar con el concepto técnico del Comité Corporativo de Riesgo, quien interactuará con el apoyo de la Unidad Corporativa de Gestión del Riesgo. El Proyecto plan debe contener como mínimo el alcance, el cronograma y el presupuesto requerido para la implementación del **SGR**.

Dado el grado de madurez alcanzado por Bancoomeva en cuanto al desarrollo de su propio Sistema de Administración de Riesgos, y sin perjuicio de las normas especiales que le son aplicables y de acoger lo pertinente a la gestión de riesgos de conglomerado, éste revisará cuales elementos del Sistema Corporativo de Gestión del Riesgo son susceptibles de ser adoptados, por cuanto alinean, complementan o fortalecen su propio Sistema, de lo cual informará a su Junta Directiva, a la Presidencia Ejecutiva del GECC y a la Unidad Corporativa de Gestión del Riesgo, presentando el respectivo Proyecto de implementación. De igual manera procederá Coomeva Corredores de Seguros y Coomeva EPS.