



# POSITIVA

COMPañÍA DE SEGUROS

## MANUAL PARA LA GESTIÓN DE RIESGOS DEL NEGOCIO

Aprobó:  <b>Junta Directiva Acta</b>	Revisó:  <b>Alexander Ruiz Ceballos Jefe Oficina de Gestión Integral de Riesgos</b>	Elaboró:  <b>Andrés Puentes Andrés Ruiz Profesionales OGIR</b>	Código: <b>EST-3-1-MA01</b>
			Fecha: <b>09/01/2020</b>
			<b>Versión: 13</b>

## TABLA DE CONTENIDO

INTRODUCCIÓN.....	7
OBJETIVO .....	8
ALCANCE.....	8
DEFINICIONES.....	8
DIRECTRICES Y PREMISAS PARA EL MANEJO DEL DOCUMENTO.....	8
CAPITULO I.....	9
1. CONSIDERACIONES GENERALES PARA LA GESTIÓN DE RIESGOS DEL NEGOCIO .....	9
1.1 OBJETIVO GENERAL .....	9
1.2 OBJETIVOS ESPECÍFICOS .....	9
1.3 ALCANCE DE LA GESTIÓN DE RIESGOS DEL NEGOCIO .....	9
1.4 MARCO LEGAL APLICABLE .....	10
1.5 PRINCIPIOS DE LA GESTIÓN DE RIESGOS DEL NEGOCIO .....	10
1.5.1 Principio de estandarización .....	10
1.5.2 Principio de independencia .....	10
1.5.3 Principio de calidad.....	10
1.5.4 Principio de información.....	11
1.5.5 Principio de gestión.....	11
1.6 SISTEMAS DE GESTIÓN DE RIESGOS DEL NEGOCIO EN POSITIVA COMPAÑÍA DE SEGUROS S.A. ....	11
1.7 ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS DEL NEGOCIO .....	12
1.7.1 Establecer el contexto.....	12
1.7.2 Identificación de riesgos.....	12
1.7.3 Medición y Control de riesgos.....	12
1.7.4 Evaluación de riesgos.....	13
1.7.5 Tratamiento de riesgos .....	13
1.7.6 Monitoreo y revisión.....	13
1.7.7 Comunicación y Consulta.....	14
1.8 NIVEL DE RIESGO ACEPTABLE.....	14
1.9 ESTRUCTURA ORGANIZACIONAL- FUNCIONES Y RESPONSABILIDADES	
14	
1.9.1 Junta Directiva.....	14

1.9.2	Comité de Auditoria.....	15
1.9.3	Presidente .....	16
1.9.4	Comité de Riesgos del Negocio .....	17
1.9.5	Oficina de Gestión Integral de Riesgos.....	19
1.9.6	Gestores de Riesgos .....	20
1.9.7	Todos los Funcionarios de Positiva Compañía de Seguros.....	21
1.9.8	Órganos de Control .....	21
1.10	DIVULGACIÓN DE INFORMACIÓN.....	22
1.11	CAPACITACIÓN .....	22
1.11.1	Alcance del programa de capacitación:.....	23
1.11.2	Objetivos del programa de capacitación: .....	23
1.11.3	Herramientas.....	23
1.11.4	Control y Evaluación .....	23
1.12	PREVENCIÓN Y RESOLUCIÓN DE CONFLICTOS DE INTERES .....	23
1.13	PROCEDIMIENTOS .....	24
1.14	DOCUMENTACIÓN.....	24
1.15	PLATAFORMA TECNOLÓGICA.....	24
<b>CAPITULO II.....</b>		<b>25</b>
<b>2. SISTEMA ESPECIAL DE ADMINISTRACION DE RIESGOS EN SEGUROS SEARS</b>		<b>25</b>
2.1	DEFINICIONES .....	25
2.1.1	Sistema de Administración de Riesgos en Seguros (SEARS).....	25
2.1.2	Riesgo de crédito en seguros .....	25
2.1.3	Riesgo de mercado en seguros .....	25
2.1.4	Riesgo de liquidez en seguros.....	25
2.1.5	Riesgo de suscripción.....	25
2.1.6	Riesgo de Insuficiencia de Reservas .....	26
2.1.7	Riesgo legal en seguros.....	26
2.1.8	Riesgo operacional en seguros .....	26
2.1.9	Riesgo estratégico en seguros .....	26
2.1.10	Riesgo reputacional en Seguros .....	26
2.2	CARACTERÍSTICAS DEL SEARS .....	26
2.2.1	Cuantificación del Riesgo .....	27
2.2.2	Cubrimiento de Riesgo.....	27

2.2.3	Control de Riesgos .....	27
2.3	<b>ELEMENTOS DEL SISTEMA DE ADMINISTRACIÓN DE RIESGOS DE SEGUROS .....</b>	<b>27</b>
2.3.1	Políticas sobre asunción de riesgos .....	27
2.3.2	Metodologías especiales para la medición de los riesgos de seguros .....	27
2.3.3	Procesos y mecanismos de control .....	28
2.3.4	Riesgo de crédito.....	28
2.3.5	Riesgo de mercado.....	28
2.3.6	Riesgo de Liquidez .....	28
2.3.7	Riesgo de suscripción.....	28
2.3.8	Riesgo de insuficiencia de reservas.....	29
2.3.9	Riesgo legal en seguros.....	29
2.3.10	Riesgo operacional en seguros .....	29
2.3.11	Riesgo estratégico en seguros .....	29
2.3.12	Riesgo reputacional.....	29
	<b>CAPITULO III .....</b>	<b>30</b>
3.	<b>SISTEMA DE ADMINISTRACION DE RIESGO OPERATIVO SARO .....</b>	<b>30</b>
3.1	<b>DEFINICIONES .....</b>	<b>30</b>
3.1.1.	Riesgo .....	30
3.1.2.	Causas del riesgo operativo .....	30
3.1.2.1.	Recurso Humano.....	30
3.1.2.2.	Procesos .....	30
3.1.2.3.	Tecnología .....	31
3.1.2.4.	Infraestructura .....	31
3.1.2.5.	Factores externos.....	31
3.1.3.	Consecuencia del riesgo.....	31
3.1.4.	Control.....	31
3.1.4.1.	Control Preventivo .....	31
3.1.4.2.	Control Detectivo.....	31
3.1.5.	Nivel de Riesgo .....	31
3.1.6.	Plan de tratamiento .....	31
3.1.7.	Evento de Riesgo.....	32
3.1.8.	Frecuencia o probabilidad de ocurrencia .....	32
3.1.9.	Impacto.....	32

3.1.10.	Sistema de Administración de Riesgo Operativo (SARO) .....	32
3.1.11.	Recursos Inembargables .....	32
3.2	<b>POLÍTICA PARTICULAR DEL SARO</b> .....	33
3.2.1	Estandarización .....	33
3.2.2	Gestión de Calidad .....	33
3.2.3	Gobernabilidad de los mapas de riesgos operativos.....	33
3.2.4	Continuidad del Negocio.....	33
3.2.5	Modificación y/o inclusión de riesgos y controles.....	33
3.3	<b>ETAPAS DE LA GESTIÓN DE RIESGO OPERATIVO</b> .....	33
3.3.1	Establecimiento del contexto estratégico.....	33
3.3.2	Entendimiento de proceso .....	34
3.3.3	Levantamiento de riesgos operativos .....	34
3.3.4	Identificación del riesgo .....	35
3.3.4.1	Identificación de causas de riesgo.....	35
3.3.4.2	Medición y Control de riesgo.....	36
3.3.4.3	Calificación de riesgos.....	36
3.3.4.4	Criterios para la calificación de la probabilidad de ocurrencia .....	36
3.3.4.5	Criterios para la calificación del impacto de materialización .....	38
3.3.4.6	Estimación del nivel de riesgo inherente.....	40
3.3.4.7	Identificación de controles.....	40
3.3.4.8	Calificación de la eficacia de los controles .....	41
3.3.4.9	Estimación del Nivel de riesgo controlado .....	43
3.3.5	Matriz de riesgos .....	43
3.3.6	Evaluación de riesgos .....	44
3.3.7	Tratamiento de riesgos .....	44
3.3.8	Monitoreo y revisión.....	45
3.3.9	Comunicación y consulta.....	46
3.4	<b>REGISTRO DE EVENTOS DE RIESGO (RER)</b> .....	46
3.4.1	Clase o clasificación de los eventos riesgo operativo.....	46
3.4.2	Tipo de pérdida de los eventos riesgo operativo .....	48
3.5	<b>ÓRDENES DE EMBARGO</b> .....	49
3.6	<b>MEDIDAS ANTE EL INCUMPLIMIENTO DEL SARO</b> .....	49
	<b>CAPITULO IV</b> .....	51
4	<b>SISTEMA DE ADMINISTRACIÓN DEL RIESGO CREDITICIO (SARC)</b> .....	51

<b>4.1</b>	<b>MARCO CONCEPTUAL Y NORMATIVO.....</b>	<b>51</b>
<b>4.1.1</b>	<b>Definición riesgo de crédito (RC) .....</b>	<b>51</b>
<b>4.1.2</b>	<b>Sistema de Administración del Riesgo Crediticio - SARC .....</b>	<b>51</b>
<b>4.2</b>	<b>ALCANCE DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO CREDITICIO.....</b>	<b>51</b>
<b>4.3</b>	<b>POLÍTICAS PARTICULARES AL SARC .....</b>	<b>51</b>
<b>4.4</b>	<b>ESTRUCTURA ORGANIZACIONAL PARTICULAR AL SARC .....</b>	<b>52</b>
<b>4.5</b>	<b>ETAPAS DE LA ADMINISTRACION DE RIESGO CREDITICIO.....</b>	<b>52</b>
<b>4.5.1</b>	<b>Otorgamiento de crédito .....</b>	<b>53</b>
<b>4.5.2</b>	<b>Criterios de validación de la capacidad de endeudamiento de los servidores de Positiva Compañía de Seguros en caso de Libranza o descuentos directos .....</b>	<b>53</b>
<b>4.5.3</b>	<b>Seguimiento y control del riesgo de crédito.....</b>	<b>54</b>
<b>4.5.4</b>	<b>Recaudo y recuperación de los créditos .....</b>	<b>55</b>
<b>4.6</b>	<b>MONITOREO DE LA GESTIÓN DE RIESGO DE CRÉDITO.....</b>	<b>55</b>
<b>5.</b>	<b>ANEXOS .....</b>	<b>56</b>
<b>5.1.</b>	<b>ANEXO I.....</b>	<b>56</b>
<b>5.2.</b>	<b>ANEXO II.....</b>	<b>57</b>

## INTRODUCCIÓN

Positiva Compañía de Seguros es una entidad aseguradora, organizada como sociedad anónima que, como consecuencia de la participación mayoritaria del estado colombiano en su capital, a través del Ministerio de Hacienda y Crédito Público, tiene el carácter de entidad descentralizada indirecta del nivel nacional, con personería jurídica, autonomía administrativa y capital independiente. Está vigilada por la Superintendencia Financiera de Colombia

La conciencia que hay de los numerosos aspectos que comprometen la competitividad y la rentabilidad de las entidades es cada vez mayor, situaciones como escándalos financieros, volatilidad en los mercados financieros, deficiencias en el servicio a los clientes, inseguridad ante las nuevas tecnologías, catástrofes naturales, terrorismo, cambios normativos, son aspectos que se convierten en riesgos potenciales y amenazan la estabilidad de las entidades.

Es por esto, que se estructura el proceso de administración de riesgos para identificar y evaluar los mismos que afectan las compañías, a fin de determinar planes, acciones y tratamientos que permitan minimizar y controlar el impacto de dichas circunstancias en las empresas.

Las recomendaciones planteadas por el comité de supervisión Bancaria de Basilea en el documento conocido como "Acuerdo de Basilea" y su adaptación para el sector asegurador a través del proyecto "Solvencia II", buscan establecer un esquema sólido, fundamentado en los pilares de estadística y medición, el de supervisión y el de transparencia de mercado para contribuir a establecer políticas, criterios y parámetros para la gestión de sus diferentes tipos de Riesgo, en aras de aportar a la eficiencia de los procesos, como naturaleza del negocio y como herramienta de gestión, para el cumplimiento de los objetivos planteados.

## **OBJETIVO**

El objetivo del presente documento es compilar las políticas y directrices aprobadas por Junta Directiva para la gestión de los riesgos del negocio en Positiva Compañía de Seguros S.A.

## **ALCANCE**

El alcance del presente documento son las políticas y directrices que rigen el Sistema Especial de Administración de Riesgos en Seguros – SEARS, el Sistema de Gestión de Riesgo Operativo - SARO, el Sistema de Gestión de Riesgo de Crédito - SARC y el Esquema de Prevención de Fraude y Corrupción en Positiva Compañía de Seguros S.A.

## **DEFINICIONES**

Dado que cada tema tiene definiciones propias, en cada capítulo se irán desarrollando.

## **DIRECTRICES Y PREMISAS PARA EL MANEJO DEL DOCUMENTO**

- Este documento es para consulta de todos los funcionarios de Positiva Compañía de Seguros S.A
- Está prohibida la reproducción total del documento sin la previa autorización de la Oficina de Gestión Integral de Riesgos.
- El uso de fragmentos o párrafos de este manual deben ser debidamente referenciados.

## **CAPITULO I**

### **1. CONSIDERACIONES GENERALES PARA LA GESTIÓN DE RIESGOS DEL NEGOCIO**

#### **1.1 OBJETIVO GENERAL**

La Gestión de Riesgos del Negocio en Positiva Compañía de Seguros S.A. tiene como objetivo que la Entidad cuente con un proceso sistemático, ejecutado por todos los niveles de la Compañía (a partir de la Junta Directiva y de forma descendente) que permita identificar eventos potenciales que puedan afectarla y gestionar sus riesgos dentro de niveles permitidos y aceptables.

#### **1.2 OBJETIVOS ESPECÍFICOS**

Teniendo como marco general el objetivo mencionado, se puede afirmar que la Gestión de Riesgos del Negocio en Positiva Compañía de Seguros S.A. tiene los siguientes objetivos específicos:

- Alinear el nivel de riesgo aceptado con la estrategia de negocio.
- Reducir los eventos sorpresivos y las pérdidas operativas.
- Mejorar la respuesta de la Compañía ante la materialización de riesgos.
- Fomentar la Cultura de Gestión de riesgos.
- Cumplir con los requerimientos normativos de la Superintendencia Financiera de Colombia y demás órganos de control.
- Generar información útil para la toma de decisiones basada en riesgos.
- Brindar a los funcionarios, así como a los terceros contratados; el conocimiento y las herramientas para gestionar los riesgos, facilitando el mejoramiento continuo de los procesos.
- Soportar el desarrollo y operación de nuevos productos y/o servicios.
- Mejorar continuamente los procesos y los sistemas de control para minimizar los riesgos.

#### **1.3 ALCANCE DE LA GESTIÓN DE RIESGOS DEL NEGOCIO**

La Gestión de riesgos tiene un alcance Institucional, abarca todos los procesos de la Compañía y es una obligación de todos los funcionarios.

La Oficina de Gestión Integral de Riesgos tiene bajo su responsabilidad dirigir la gestión y evaluación de los riesgos del negocio, incluyendo:

Riesgo Operacional

Riesgo de crédito

Riesgos especiales del negocio asegurador.

Así mismo, la Oficina de Gestión Integral de Riesgos también se ocupa del análisis y evaluación del riesgo asociado a la administración del portafolio de Inversiones de la Compañía, aspecto que se rige por lo establecido en el Manual de Políticas y Riesgos para la Administración del Portafolio de Inversiones.

## **1.4 MARCO LEGAL APLICABLE**

Las actividades que deben desarrollarse para cumplir con las disposiciones de ley relacionadas a los riesgos del negocio, se encuentran reglamentadas en los siguientes documentos:

- a. Constitución Política de Colombia. Art. 209 y 269, referentes a los Sistemas de Control Interno de las Entidades Públicas.
- b. Ley 872 de 2003, referente a la creación del Sistema de Gestión de la Calidad.
- c. Decreto 1537 de 2001, referente a la reglamentación de algunos elementos técnicos y administrativos que fortalecen el sistema de control interno de las entidades y organismos del Estado.
- d. Decreto 1599 de 2005, referente a la adopción del MECI por parte de las entidades públicas.
- e. Decreto 943 de 2014, referente a la actualización del MECI.
- f. Artículo 73 de la Ley 1474 de 2011, referente al mapa de riesgos de corrupción de las entidades públicas.
- g. Capítulo V del Título de la Circular Básica Jurídica (C.E. 029 de 2014), referente a SEARS.
- h. Capítulos II y XXIII de la Circular Básica Contable y Financiera (C.E. 100 de 1995), referentes al SARC y SARO, respectivamente
- i. Numeral 7, Capítulo IX del Título I de la Circular Básica Jurídica (C.E. 007 de 1996), referente al Sistema de Control Interno.

## **1.5 PRINCIPIOS DE LA GESTIÓN DE RIESGOS DEL NEGOCIO**

La Gestión de Riesgos del Negocio en Positiva está sustentada en los siguientes principios:

### **1.5.1 Principio de estandarización**

La gestión de riesgos cumple con los lineamientos generales y particulares dados por la Superintendencia Financiera de Colombia y busca alinearse con las mejores prácticas y estándares nacionales e internacionales.

### **1.5.2 Principio de independencia**

La Oficina de Gestión Integral de Riesgos, y sus funcionarios son independientes, tanto a nivel funcional como organizacional, de las áreas encargadas de las funciones comerciales, de operaciones, financieras, administrativas y de las técnicas en seguros.

### **1.5.3 Principio de calidad**

Positiva Compañía de Seguros S.A. está organizada por procesos. Por lo anterior, todas las funciones y actividades realizadas por sus funcionarios son ejecutadas con estricta sujeción a los documentos que soportan las políticas, procesos y procedimientos previamente definidos y divulgados.

Bajo este principio, se contará con la participación de los gestores, dueños o responsables de los procesos para desarrollar la gestión de riesgos en toda la Compañía.

#### **1.5.4 Principio de información**

El proceso de gestión de riesgos garantiza que los resultados de la calificación y/o medición de riesgos del negocio de la entidad serán conocidos por los grupos de interés de la Compañía.

#### **1.5.5 Principio de gestión**

La gestión de riesgos se basa en la auto-gestión, lo que significa que cada funcionario tiene un rol dentro de los procesos que se ejecutan, siendo responsable directo de la adecuada gestión de los riesgos que asume en su labor diaria.

### **1.6 SISTEMAS DE GESTIÓN DE RIESGOS DEL NEGOCIO EN POSITIVA COMPAÑÍA DE SEGUROS S.A.**

Con base en el alcance mencionado, la gestión riesgos del negocio en la Compañía se compone de los siguientes sistemas:

- Sistema de Administración de Riesgo Operativo (SARO)
- Sistema de Administración de Riesgo de Crédito (SARC)
- Sistema Especial de Administración de Riesgos de Seguros (SEARS)

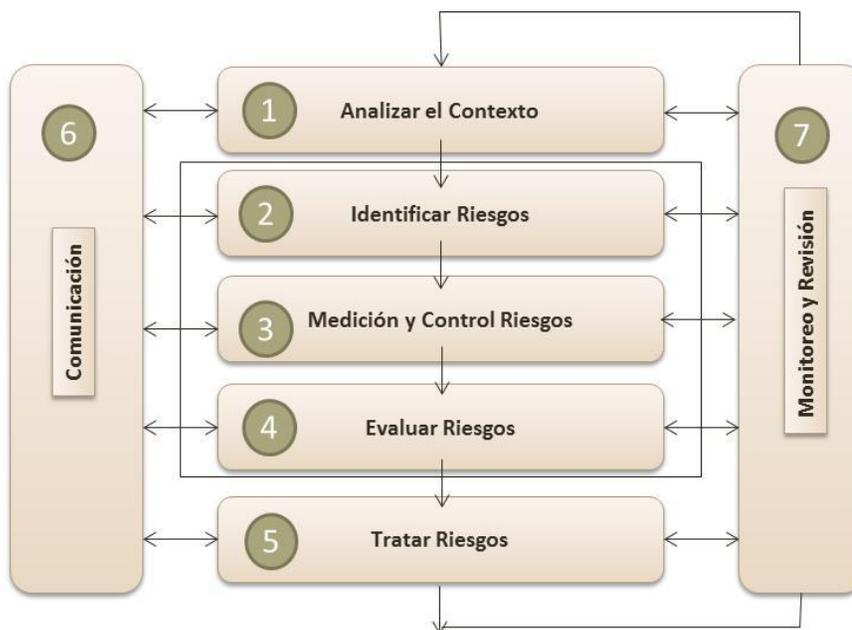
Cada uno de los Sistemas mencionados contemplan el conjunto de políticas, procedimientos, documentación, estructura organizacional, órganos de control, infraestructura tecnológica, herramientas de divulgación de información y herramientas de capacitación, mediante los cuales se cumple con cada una de las etapas del proceso de gestión de riesgos.

En Positiva Compañía de Seguros S.A., de los anteriores elementos que componen un sistema; la estructura organizacional, los órganos de control, la infraestructura tecnológica, las herramientas de divulgación de información y las herramientas de capacitación son comunes a los cuatro subsistemas mencionados. Por lo anterior, de acuerdo al riesgo, se cuenta con políticas, procedimientos de medición y seguimiento y documentos específicos por tipo de riesgo.

## 1.7 ETAPAS DEL PROCESO DE GESTIÓN DE RIESGOS DEL NEGOCIO

La gestión de riesgos del negocio se desarrolla considerando 7 etapas tal como se muestra a continuación:

**FIGURA N° 1.** Etapas de la Gestión de Riesgos



La Oficina de Gestión Integral de riesgos comenzará la ejecución de las etapas del sistema de administración del riesgo, una vez la Oficina de Estrategia y desarrollo y los dueños del proceso notifiquen que el proceso se encuentra debidamente documentado

### 1.7.1 Establecer el contexto

Esta etapa tiene como objetivo alinear la gestión de riesgos del negocio con la estrategia corporativa (misión, visión, objetivos estratégicos, estrategias y líneas de negocio).

### 1.7.2 Identificación de riesgos

El propósito de esta fase es generar una lista exhaustiva de riesgos a través de las respuestas a cuatro preguntas: ¿QUE?, ¿COMO?, ¿PORQUE? Y ¿DONDE? se originan o se pueden originar eventos de riesgo que afecten negativamente el cumplimiento de los objetivos de la Compañía, de un proceso, de un área, un producto, un nuevo producto, un contrato o un proyecto.

### 1.7.3 Medición y Control de riesgos

En esta etapa se establece la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, así como los controles existentes y su calificación en términos de su eficiencia como mitigadores del riesgo.

La calificación del impacto y de la probabilidad de ocurrencia se combinan para producir un nivel de riesgo estimado.

#### **1.7.4 Evaluación de riesgos**

Esta etapa comprende la comparación del nivel de riesgo estimado con el nivel de riesgo aceptado, con el fin de priorizar y asignar recursos de manera eficiente para la gestión de riesgos.

#### **1.7.5 Tratamiento de riesgos**

Esta etapa tiene como fin identificar, registrar, evaluar y elegir el conjunto de actividades a ejecutarse para mitigar el riesgo y ajustar de esta manera el nivel de riesgo al máximo aceptable.

#### **1.7.6 Monitoreo y revisión**

El objetivo de esta etapa es asegurar la retroalimentación requerida para garantizar la mejora continua del proceso de gestión de riesgos, considerando que los riesgos no son estáticos, por lo que éstos y la efectividad de sus controles necesitan ser monitoreados continuamente.

Así las cosas, para asegurar el monitoreo y revisión de la gestión de riesgos se tendrá en cuenta el siguiente esquema de asignación y responsabilidades de cada una de las líneas de defensa<sup>1</sup>:

##### **1ª Línea de Defensa**

- Controles de las áreas Operativas (Líderes de proceso y sus equipos).
- La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de gestión de riesgos y sus controles como parte del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.

##### **2ª Línea de Defensa**

- Media y Alta Dirección: jefes de área, comité de riesgos, áreas financieras, de contratación, de TIC, entre otros que generen información para el aseguramiento de la operación.
- Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente y supervisan la implementación de prácticas de gestión de riesgo eficaces.

##### **3ª Línea de Defensa**

- A cargo de la Oficina de Control Interno, Revisoría Fiscal.
- La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporcionará aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad, incluidas la efectividad en que funciona la primera y segunda línea de defensa.

---

<sup>1</sup> Fuente: Modelo Integrado de Planeación y Gestión (MIPG). Función Pública

### **1.7.7 Comunicación y Consulta**

El objetivo de esta etapa es proveer y compartir información, así como comprometer a los grupos de interés de la Compañía en relación con la administración de riesgos.

### **1.8 NIVEL DE RIESGO ACEPTABLE**

El nivel de riesgo aceptable por Positiva Compañía de Seguros S.A. está definido como aquel nivel de riesgo que puede seguir siendo administrado por cada líder de proceso. Así, los riesgos que después del control se ubiquen en los niveles bajo y/o moderado, harán parte del nivel de riesgo aceptable. Para los riesgos que después del control se ubiquen en los niveles distintos a los mencionados deberán implementarse planes de tratamiento dirigidos a reducir su nivel de riesgo.

### **1.9 ESTRUCTURA ORGANIZACIONAL- FUNCIONES Y RESPONSABILIDADES**

Con el fin de garantizar la independencia y un adecuado esquema de Gobierno Corporativo, la Gestión de riesgos del negocio en Positiva Compañía de Seguros S.A. cuenta con la siguiente estructura organizacional:

#### **1.9.1 Junta Directiva**

La Junta Directiva sin perjuicio de las funciones asignadas en otras disposiciones, debe asegurar la existencia de los recursos e infraestructura necesaria para garantizar la eficaz administración y gestión del riesgo, acorde a la naturaleza, complejidad y volumen de los negocios, operaciones y actividades.

En referencia a la gestión del riesgo sus funciones son:

- a. Conocer y comprender los riesgos que asume la entidad.
- b. Definir y aprobar las políticas relativas a la Gestión del Riesgo del Negocio de la entidad.
- c. Aprobar los manuales, procedimientos, metodologías y disposiciones en materia de Gestión de Riesgo y sus actualizaciones.
- d. Emitir un concepto frente al perfil de riesgo consolidado de la Compañía y por clase de riesgo.
- e. Establecer el nivel de riesgo aceptable.
- f. Establecer las medidas relativas al perfil de riesgo v/s el nivel de riesgo aceptable.
- g. Emitir un concepto frente a las evaluaciones e informes que presente el Representante Legal y los órganos de control relacionados con la Gestión de Riesgos del Negocio.
- h. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que se le presenten en materia de Gestión del Riesgos del Negocio.
- i. Aprobar los recursos técnicos y humanos y el presupuesto necesario para implementar y mantener en funcionamiento los Sistemas de Gestión de Riesgos.
- j. Pronunciarse sobre los informes presentados por la Revisoría Fiscal y la Oficina de Control Interno o quien ejecute funciones similares o haga sus veces acerca del funcionamiento de los Sistemas de Administración de Riesgos, y hacer seguimiento a las observaciones o recomendaciones adoptadas, dejando la expresa constancia en la respectiva acta.

- k. Analizar el proceso de gestión de riesgo existente y adoptar las medidas necesarias para fortalecerlo en aquellos aspectos que así lo requieran.
- l. Efectuar seguimiento en sus reuniones ordinarias a través de informes periódicos que le presente el Comité de Auditoría, sobre la gestión de riesgos en la entidad y las medidas adoptadas para el control o mitigación de los riesgos más relevantes, por lo menos cada seis meses, o con una frecuencia mayor si así resulta procedente.
- m. Exigir de la administración, para su evaluación, reportes periódicos sobre los niveles de exposición al RC, sus implicaciones y las actividades relevantes para su mitigación y/o adecuada administración.
- n. Señalar las responsabilidades y atribuciones asignadas a los cargos y áreas encargadas de gestionar el RC.

### **1.9.2 Comité de Auditoría**

El Comité de Auditoría, en materia de Gestión de Riesgo, tendrá como mínimo las siguientes funciones, sin perjuicio de lo dispuesto en la normatividad aplicable al mismo:

- a. Proponer a la Junta directiva programas y controles para prevenir, detectar y responder adecuadamente a los riesgos de fraude y mala conducta.
- b. Efectuar seguimiento sobre los niveles de exposición de riesgo, sus implicaciones para la Compañía y las medidas adoptadas para su control o mitigación, por lo menos cada seis (6) meses, o con una frecuencia mayor si así resulta procedente, y presentar a la Junta Directiva un informe sobre los aspectos más importantes de la gestión realizada.

### 1.9.3 Presidente

El Presidente de Positiva Compañía de Seguros, sin perjuicio de las funciones asignadas en otras disposiciones, es responsable de:

- a. Dirigir el proceso de identificación, medición y control de los riesgos operativos<sup>2</sup>
- b. Desarrollar y velar por que se implementen las estrategias, con el fin de fortalecer el cambio cultural de la gestión del riesgo al interior de la Compañía.
- c. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente los Sistemas de Gestión de Riesgos del Negocio.
- d. Velar por el cumplimiento efectivo de las políticas aprobadas por la Junta Directiva frente a la implementación de los sistemas de administración de los riesgos del negocio.
- e. Adelantar un seguimiento permanente de las etapas y elementos que constituyen los Sistemas de Gestión de Riesgos del Negocio.
- f. Designar el área o cargo que actuará como responsable de la implementación y seguimiento de los Sistemas de Gestión de Riesgos del Negocio.
- g. Adoptar las medidas adecuadas, relativas al perfil de riesgo de la entidad, como resultado de la medición al mismo y de su seguimiento.
- h. Velar por la correcta aplicación de los controles de riesgo inherente.
- i. Recibir los informes presentados por la Oficina de Gestión Integral de Riesgos, así como pronunciarse en relación con los mismos.
- j. Velar porque las etapas y elementos de los Sistemas de Gestión de Riesgos del Negocio cumplan con las disposiciones legales pertinentes.
- k. Velar porque se implementen los procedimientos para la adecuada administración del riesgo a que se vea expuesta la entidad en desarrollo de su actividad.
- l. Aprobar los planes de contingencia y de continuidad del Negocio y disponer de los recursos necesarios para su oportuna ejecución.
- m. Adelantar un seguimiento permanente del cumplimiento de las funciones del área o unidad de gestión de riesgo y de sus funcionarios y mantener informada a la junta directiva.
- n. Realizar monitoreo y revisión de las funciones del auditor interno.
- o. Hacer seguimiento y pronunciarse respecto de los informes que presente el revisor fiscal.
- p. Establecer un procedimiento para alimentar el Registro de Eventos de Riesgo Operativo y velar porque el registro de eventos del riesgo operativo cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.
- q. Presentar un informe periódico, como mínimo semestral, a la Junta Directiva sobre la evolución y aspectos relevantes de los sistemas de Gestión de Riesgos del Negocio, incluyendo acciones preventivas y correctivas implementadas o por implementar y el área responsable.
- v. Garantizar que las bases de datos y la plataforma tecnológica cumplan los criterios y requisitos establecidos en la Norma.
- w. Reportar los casos de fraude al Comité de Auditoría.

---

<sup>2</sup> Función asignada al Presidente por el decreto 1678 de 2016

#### **1.9.4 Comité de Riesgos del Negocio**

Teniendo en cuenta que la gestión de riesgos del negocio requiere una atención especial por parte de la Alta Dirección de la Compañía se crea el Comité de Riesgos del Negocio, el cual funcionará con base en los siguientes parámetros:

##### **1.9.4.1 Naturaleza del Comité**

El Comité de Riesgos del Negocio de Positiva Compañía de Seguros S.A. tendrá como función asesorar al Presidente en la formulación de políticas y la gestión de los riesgos del negocio que debe administrar la empresa.

##### **1.9.4.2 Alcance del Comité**

El Comité de Riesgos del Negocio de Positiva Compañía de Seguros S.A. tendrá como alcance los siguientes sistemas de administración de riesgos:

- Sistema de Administración de Riesgo Operativo
- Sistema de Especial de Administración de Riesgos en Seguros
- Sistema de Administración de Riesgo de Crédito

##### **1.9.4.3 Conformación del Comité**

El Comité de Riesgos del Negocio de Positiva Compañía de Seguros S.A. estará integrado por los funcionarios que ocupen los siguientes cargos, quienes concurrirán con voz y voto y serán miembros permanentes:

- ✓ Presidencia de Positiva Compañía de Seguros S.A
- ✓ Secretaría General
- ✓ Vicepresidencia de Inversiones
- ✓ Vicepresidencia Financiera y Administrativa
- ✓ Vicepresidencia Técnica
- ✓ Vicepresidencia de Negocios
- ✓ Vicepresidencia de Promoción y Prevención
- ✓ Vicepresidencia de Operaciones
- ✓ Jefe de Oficina de Estrategia y Desarrollo
- ✓ Jefe de Oficina de Gestión Integral de Riesgos
- ✓ Jefe de Oficina de Tecnologías de la Información

El Jefe de la Oficina de Control Interno será invitado permanente al Comité con voz pero sin voto. Adicionalmente podrá asistir como invitado cualquier funcionario de la Compañía, quien participará con voz pero sin voto.

##### **1.9.4.4 Presidente del Comité**

Actuará en calidad de Presidente del Comité, la Presidencia de Positiva Compañía de Seguros S.A. Para la sesión donde no pueda participar la Presidencia de Positiva, el Jefe de la Oficina de Gestión Integral de Riesgos asumirá el rol de Presidente del Comité de Riesgos de Negocio.

En caso que ninguno de los dos se encuentre, será el encargado de la Presidencia o el encargado de la Oficina de Gestión Integral de Riesgos, respetando el orden jerárquico, quien ejercerá la presidencia del comité.

#### **1.9.4.5 Secretario del Comité**

El Secretario del Comité será el Jefe de la Oficina de Gestión Integral de Riesgos, o quien éste delegue para dicha función.

Tendrá como función principal organizar, asistir y velar por el cumplimiento de las decisiones adoptadas por el Comité, conforme a las siguientes funciones específicas:

- Convocar y citar a los miembros e invitados.
- Elaborar el orden del día para cada sesión.
- Elaborar las actas de cada sesión
- Verificar el cumplimiento de las decisiones adoptadas por el Comité.
- Las demás que les sean asignadas por el Comité.

#### **1.9.4.6 Sesiones del Comité**

El Comité de Riesgos del Negocio de Positiva Compañía de Seguros S.A. sesionará de manera ordinaria una vez cada dos (2) meses, en los siguientes meses febrero, mayo julio, septiembre y noviembre.

Adicionalmente, el Comité podrá sesionar de manera extraordinaria en el lugar, día y hora que informe el Presidente de la Compañía o la Oficina de Gestión Integral de Riesgos, cuando a juicio de dichas instancias, las circunstancias así lo ameriten.

#### **1.9.4.7 Quorum del Comité**

Para deliberar sobre cualquier asunto, se requiere la asistencia de siete de sus miembros permanentes.

Para decidir sobre cualquier asunto se requiere mayoría simple, esto es, la mayoría de los votos de los miembros presentes en la sesión.

#### **1.9.4.8 Funciones del Comité**

Siempre dentro de los sistemas de administración de riesgos mencionados en el numeral 1.9.4.2 del presente capítulo, serán funciones del Comité de Riesgos del Negocio de Positiva Compañía de Seguros S.A. las siguientes:

- a. Evaluar las propuestas de políticas, metodologías y modelos para identificar, analizar, medir, controlar y monitorear los distintos tipos de riesgo, que serán sometidas a aprobación de la Junta Directiva.
- b. Conocer y evaluar los niveles de tolerancia o aceptación de los distintos riesgos que se pondrán a consideración del Comité de Auditoría, para su evaluación y recomendación a Junta Directiva para su aprobación.

- c. Evaluar los cambios o modificaciones al Manual de Gestión de Riesgos que se someterán a consideración del Comité de Auditoría, para su análisis y recomendación a Junta Directiva para su aprobación.
- d. Conocer los perfiles de riesgo sobre los cuales se pronunciará el Comité de Auditoría y la Junta Directiva.
- e. Conocer el informe periódico a presentar al Comité de Auditoría y la Junta Directiva sobre la evolución del perfil de riesgo de la Compañía, así como los aspectos relevantes de los sistemas de riesgos mencionados en el alcance.
- f. Revisar y recomendar acciones respecto al perfil de riesgo de la entidad.
- g. Sugerir mecanismos de generación de cultura de gestión de riesgo corporativo a nivel nacional.
- h. Realizar seguimiento a la implementación de los planes de tratamiento de los riesgos que se encuentren fuera de los niveles de tolerancia definidos por la Junta Directiva.
- i. Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.
- j. Conocer el comportamiento y efectividad de los controles definidos en los procesos para la mitigación de riesgos.
- k. Asegurar que las áreas de negocio o dueños de procesos ejecuten correctamente la estrategia de gestión de riesgo aprobada.
- l. Velar por la implementación efectiva y oportuna de las acciones correctivas para subsanar las deficiencias de la administración de riesgos en la Compañía.
- m. Adelantar un seguimiento permanente de las etapas y elementos constitutivos de los sistemas de gestión de riesgos mencionados en el alcance.
- n. Evaluar las estrategias y los planes relacionados con la Continuidad del Negocio.
- o. Aprobar el plan anual de ejercicios relacionados con el esquema de continuidad del negocio.
- p. Aprobar el plan de sensibilización, divulgación y capacitación en gestión de riesgos y continuidad del negocio; así como conocer los resultados de dichos planes de forma periódica con el fin de implementar las medidas que sean requeridas.
- q. Velar porque el registro de eventos de riesgo operativo cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida, así como su efectiva alineación con el SARO.
- r. Las demás que por su naturaleza le sean afines.

### **1.9.5 Oficina de Gestión Integral de Riesgos**

La Oficina de Gestión Integral de Riesgos es la líder funcional de la gestión de riesgos en Positiva Compañía de Seguros.

Independientemente de sus demás funciones, es responsable de:

- a. Dirigir la identificación, medición y control de los Riesgos de Negocio.
- b. Proponer y presentar los manuales de administración de riesgos para aprobación de la Junta Directiva de la Compañía
- c. Orientar la evaluación de riesgos para la participación de la Compañía en nuevos productos.
- d. Coordinar la elaboración y publicación de informes para dar a conocer la evolución de los riesgos y rendir los informes de gestión y los que le sean solicitados por organismos externos con la oportunidad y periodicidad requerida.

- e. Proponer los instrumentos, políticas, límites, metodologías y procedimientos para que la Compañía administre efectivamente los diferentes tipos de riesgo, en concordancia con los lineamientos normativos previstos en el sistema de administración de riesgos.
- f. Establecer y monitorear el perfil de riesgo de la entidad e informarlo al órgano correspondiente. (Comité de Riesgos de Negocio, Comité de Auditoría, Junta Directiva)
- g. Identificar las áreas de riesgo sobre las cuales se debe priorizar tratamiento, atendiendo a los mapas de riesgos de cada proceso de la Compañía.
- h. Hacer seguimiento y control a la administración de la información de eventos de riesgo, no conformidades y acciones correctivas, de acuerdo con las disposiciones establecidas por los entes reguladores
- i. Participar en el proceso de identificación, medición y control de riesgos relacionados con los procesos que se desarrollan en el área.
- j. Garantizar que los procesos de la Oficina respondan a los lineamientos establecidos en el sistema integrado de gestión.
- k. Formular y ejecutar en coordinación con la Gerencia de Talento Humano, el programa de capacitación para todas las áreas de la compañía relacionado con los sistemas de riesgo de la operación del negocio y los demás requeridos para adelantar los procedimientos de la gerencia.
- l. Apoyar el desarrollo y sostenimiento del Sistema Integrado de Gestión Institucional
- m. Adelantar el diseño, implementación y evaluación de los programas destinados a desarrollar una cultura de prevención de los riesgos del negocio involucrando a todos los niveles de la Compañía.
- n. Coordinar la identificación, análisis y evaluación de los riesgos existentes en los procesos y su impacto, atendiendo la metodología establecida y la información recolectada.
- o. Administrar los sistemas de riesgo de la operación del negocio (SARO), continuidad del negocio (SGCN), esquema antifraude, especial de la administración del riesgo asociado al negocio de seguros (SEARS).
- p. Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos operativos medidos.
- q. Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.
- r. Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
- s. Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo.
- t. Las demás funciones asignadas por la autoridad competente de acuerdo con el nivel jerárquico y la naturaleza de la dependencia

#### **1.9.6 Gestores de Riesgos**

La gestión del riesgo cuenta con delegados, dueños de los procesos que participan en los diferentes sistemas, quienes estarán encargados de describir, analizar, evaluar, autoevaluar y monitorear los diferentes tipos de riesgos que se presentan en los procesos de Positiva Compañía de Seguros.

Sin perjuicio de las funciones asignadas en otras disposiciones los designados como gestores o representantes de los procesos dentro del sistema deberán:

- a. Participar y representar el proceso que desarrolla a nivel Nacional, en la implementación y mantenimiento del Sistema de Gestión de Riesgos del Negocio a través de todas sus etapas.
- b. Generar la información necesaria para desarrollar, implementar y mantener el Sistema de Gestión de Riesgos de Negocio con las contribuciones necesarias de los procesos que representa.
- c. Desarrollar las diferentes etapas del sistema al interior del proceso, abarcándolo en su totalidad y representando el proceso a nivel nacional y sucursal.
- d. Sustentar la aplicación metodológica del Sistema de Gestión de Riesgos del Negocio en su proceso, en caso de requerirlo.
- e. Asistir a las capacitaciones relacionadas con el tema en la Compañía.
- f. Cumplir con las directrices dispuestas por la Oficina de Gestión Integral de Riesgos

### **1.9.7 Todos los Funcionarios de Positiva Compañía de Seguros**

Sin perjuicio de las funciones asignadas en otras disposiciones, los funcionarios de la Compañía deberán:

- a. Participar activamente del Sistema Integral de Gestión del Riesgo, en torno a las actividades desarrolladas que lo involucren.
- b. Cumplir con la directriz de identificar medir y controlar los riesgos relacionados en el área a la que pertenece y los procesos en los que participa.
- c. Asistir a las capacitaciones relacionadas con el tema, que sean coordinadas por la Oficina de Gestión Integral de Riesgos o por la Gerencia de Recursos Humanos.
- d. Ajustar los mapas de riesgo del negocio con las sugerencias dadas por la Oficina de Gestión Integral de Riesgos.
- e. Ejecutar los controles dispuestos por la Oficina de Gestión Integral de Riesgos, así como suministrar al Oficial de Cumplimiento información susceptible de análisis.

### **1.9.8 Órganos de Control**

#### **1.9.8.1 Revisoría Fiscal**

La Revisoría Fiscal tiene por función frente a los Sistemas de Administración de Riesgo del Negocio elaborar reportes de cumplimiento e informar a la Presidencia y a la Junta Directiva los incumplimientos.

Sin perjuicio de las funciones asignadas en otras disposiciones la Revisoría Fiscal deberá:

- a. Elaborar un reporte al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre los diferentes Sistemas de Administración del Riesgo implementados al interior de Positiva Compañía de Seguros.
- b. -
- c. Poner en conocimiento del Representante Legal los incumplimientos del SARO, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva.

#### **1.9.8.2 Oficina de Control Interno**

La oficina de Control Interno tiene por función evaluar periódicamente el cumplimiento y efectividad de los Sistemas de Administración del Riesgo a través de las etapas y elementos definidos para los mismos, determinando las oportunidades de mejora y

posibles soluciones. Así mismo, debe informar los resultados al Presidente de la Compañía, al Oficial de Cumplimiento y a la Oficina de Gestión Integral de Riesgos.

Sin perjuicio de las funciones asignadas en otras disposiciones la Oficina de Control Interno deberá:

- a. Evaluar anualmente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del Sistema de Gestión Integral del Riesgo con el fin de determinar las deficiencias y posibles soluciones.
- b. Informar los resultados de la evaluación a la Oficina de Gestión Integral de Riesgos, al Oficial de Cumplimiento, al Representante Legal y a la Junta Directiva.
- c. Evaluar el cumplimiento en la implementación de los diferentes reportes relacionados y en el Registro de Eventos de Riesgo RER.
- d. Velar por la correcta implementación de todas las metodologías y procedimientos, así como por el cumplimiento de todos los límites y controles adoptados por la junta directiva.
- e. Informar al Representante Legal sobre el incumplimiento del Registro de Eventos de Riesgo Operativo.

## **1.10 DIVULGACIÓN DE INFORMACIÓN**

Positiva Compañía de Seguros S.A. utiliza comunicados, reportes e informes de interés general y particular permitiendo mantener a los colaboradores informados en lo referente los sistemas de Gestión de Riesgos, perfiles de riesgo, mapas de riesgo e informes y reportes internos y externos.

De acuerdo a lo anterior, la Compañía implementa una serie de reportes por cada sistema de riesgos, de tal forma que se garantice el funcionamiento adecuado de sus procedimientos, su cumplimiento de requisitos normativos y el adecuado conocimiento de las políticas, sus límites, los excesos presentados a los mismos, el nivel de exposición y su perfil de riesgo.

Así mismo, implementa la publicación a través de la intranet de la información correspondiente a los procedimientos y procesos desarrollados en la organización, y sus mapas de riesgo correspondientes; reportes, como mínimo semestrales, que permitan establecer el perfil de riesgo de la entidad; la publicación en el Informe de gestión anual de los avances obtenidos en materia de riesgos en los diferentes sistemas de administración de riesgos y reportes periódicos de la Oficina de Gestión Integral de Riesgos sobre el cumplimiento de las políticas, límites y nivel de exposición a los distintos riesgos asumidos.

## **1.11 CAPACITACIÓN**

Positiva Compañía de Seguros, a través de la Oficina de Gestión Integral de Riesgos y la Gerencia de Talento Humano diseña y coordina anualmente los programas de capacitación referentes a los sistemas de Administración de Riesgos de Negocio. Estos planes están dirigidos a todos los colaboradores de la organización, incluyendo terceros que presten servicios críticos a la Compañía.

### **1.11.1 Alcance del programa de capacitación:**

El programa de capacitación tiene un cubrimiento nacional y está dirigido a todos los funcionarios y colaboradores de la Compañía.

### **1.11.2 Objetivos del programa de capacitación:**

- Contribuir a la construcción de cultura frente a la administración de riesgos a través de la generación de conciencia en los colaboradores haciendo énfasis en el autocontrol y la autogestión.
- Servir de herramienta de gestión para el mejoramiento continuo de Positiva Compañía de Seguros.
- Fortalecer la imagen y solidez de la Compañía frente al mercado.
- Garantizar el cumplimiento de los objetivos institucionales para cada uno de los procesos.
- Formar colaboradores capaces de identificar y resolver los retos de la Gestión de riesgos.
- Asegurar un conocimiento amplio y suficiente por parte de todos los colaboradores.

### **1.11.3 Herramientas**

El programa de capacitación diseñado para cada año podrá contar con las siguientes herramientas:

- ✓ Sesiones presenciales o virtuales.
- ✓ Ayudas audiovisuales que son compartidas como material de consulta.
- ✓ Cuestionarios de medición de conocimientos y percepciones del tema.
- ✓ Envío de correo electrónico, videos, presentaciones entre otros.

### **1.11.4 Control y Evaluación**

Positiva implementará un esquema de evaluación obligatorio para sus colaboradores, que tendrá una calificación mínima del 85%. En caso de que la evaluación sea reprobada, el colaborador deberá presentar nuevamente su evaluación.

## **1.12 PREVENCIÓN Y RESOLUCIÓN DE CONFLICTOS DE INTERES**

En cuanto a la prevención y resolución de conflictos de interés, en la recolección de información en las diferentes etapas del SARO, especialmente para el registro de eventos de riesgo operativo; Positiva Compañía de Seguros S.A. cuenta con un Código de Ética y Buen Gobierno, donde se establecen las políticas frente a los grupos de interés; y el compromiso frente a los Conflictos de Interés, los deberes del equipo humano relacionados con los Conflictos de Interés, las prohibiciones para los servidores sobre Conflictos de Interés y el procedimiento de resolución y divulgación de Conflictos de Intereses. El código se encuentra publicado en el manual de calidad en la herramienta SIMPLE.

Por lo anterior, Positiva Compañía de Seguros S.A. declara que los conflictos de interés que se presenten dentro del proceso de gestión de riesgos serán solucionados siguiendo los lineamientos mencionados en el Código de Ética y Buen Gobierno.

Adicionalmente, los programas de capacitación implementados, en lo referente al Registro de Eventos de Riesgo Operativo, harán énfasis en los potenciales conflictos y la manera como deben prevenirse y solucionarse.

### **1.13 PROCEDIMIENTOS**

Para cada uno de los Sistemas de Administración del Riesgos, se desarrolla de forma particular en el Capítulo correspondiente la descripción de los procedimientos aplicables a cada sistema, con el respectivo desarrollo de sus etapas y elementos.

### **1.14 DOCUMENTACIÓN**

A partir del desarrollo de las etapas de los diferentes Sistemas de Administración de Riesgos, la Oficina de Gestión Integral de Riesgos documentará y custodiará la información que soporta su implementación. Los cambios o modificaciones de esta información estructural deben ser solicitados formalmente a esta oficina.

La documentación de los Sistemas de Administración de Riesgo tiene por objetivo:

- Demostrar que el proceso se realiza en forma apropiada.
- Proporcionar evidencia de un enfoque sistemático.
- Ofrecer un registro de los eventos de riesgo, y desarrollar la base de datos del conocimiento de Positiva Compañía de Seguros.
- Facilitar el monitoreo continuo y la revisión.
- Ofrecer un rastro o registro de auditoría.
- Compartir y comunicar la información.

Los informes para la Junta Directiva, para el Representante Legal, el Oficial de Cumplimiento y los órganos de control con referencia a los Sistemas de Administración de riesgos, tienen los mismos criterios de guarda y conservación establecidos por la Compañía para los documentos en las tablas de retención documental, de cada una de las áreas que intervienen en dichos sistemas.

### **1.15 PLATAFORMA TECNOLÓGICA**

Es el conjunto de herramientas tecnológicas o Software que permiten a Positiva Compañía de Seguros S.A. administrar la información relacionada con los sistemas de administración de riesgos.

A través del aplicativo ERA (Enterprise Risk Assessor), la Oficina de Gestión Integral de Riesgos administra la información generada en el desarrollo de las etapas y elementos de los sistemas de administración de riesgos del negocio.

## CAPITULO II

### 2. SISTEMA ESPECIAL DE ADMINISTRACION DE RIESGOS EN SEGUROS SEARS

#### 2.1 DEFINICIONES

##### 2.1.1 Sistema de Administración de Riesgos en Seguros (SEARS)

Conforme al numeral 1.1 del Capítulo IV del Título IV de la Parte II de la Circular Externa 029 de 2014 expedida por la Superintendencia Financiera de Colombia, el Sistema Especial de Administración de Riesgos de Seguros (SEARS) corresponde al sistema que toda entidad aseguradora debe diseñar y adoptar para realizar una adecuada gestión de los riesgos propios de su actividad.

##### 2.1.2 Riesgo de crédito en seguros

Se entiende por riesgo de crédito de las entidades aseguradoras a la posibilidad de incurrir en pérdidas por el no pago o pago inoportuno de las obligaciones a cargo de sus reaseguradores, asegurados, intermediarios de seguros y otras compañías de seguros con las cuales realiza operaciones de coaseguro. Incluye la exposición al riesgo de crédito indirecto, el cual se genera, por ejemplo, en la expedición de pólizas de cumplimiento.

##### 2.1.3 Riesgo de mercado en seguros

Se entiende por riesgo de mercado la posibilidad de incurrir en pérdidas derivadas del incremento no esperado en el monto de sus obligaciones con asegurados, reaseguradores, intermediarios y otros agentes externos a causa de variaciones en las tasas de interés, en la tasa de devaluación o cualquier otro parámetro de referencia.

##### 2.1.4 Riesgo de liquidez en seguros

Se entiende por riesgo de liquidez la imposibilidad de adquirir u obtener los fondos necesarios para atender el pago de obligaciones de corto plazo bien sea para el pago de siniestros o para el ajuste de reservas inadecuadamente calculadas.

##### 2.1.5 Riesgo de suscripción

Se entiende por riesgo de suscripción la posibilidad de incurrir en pérdidas como consecuencia de políticas y prácticas inadecuadas en el diseño de productos o en la colocación de los mismos. Dicha categoría de riesgo se puede clasificar en los siguientes tipos:

- **Riesgos de tarificación:** Corresponde a la probabilidad de pérdida como consecuencia de errores en el cálculo de primas al punto que resulten insuficientes para cubrir los siniestros actuales y futuros, los gastos administrativos y la rentabilidad esperada.
- **Riesgo de descuento sobre primas:** Corresponde a la probabilidad de pérdida en que puede incurrir una entidad como consecuencia del otorgamiento inadecuado de descuentos sobre primas.

- **Riesgo de concentración:** Corresponde a la probabilidad de pérdida en que puede incurrir una entidad como consecuencia de una inadecuada diversificación de los riesgos asumidos.
- **Riesgo de diferencia en condiciones:** Corresponde a la probabilidad de pérdida que se genera como consecuencia de diferencias entre las condiciones originalmente aceptadas de los tomadores de pólizas y las aceptadas a su vez por los reaseguradores de la entidad.

### **2.1.6 Riesgo de Insuficiencia de Reservas**

Corresponde a la probabilidad de pérdida como consecuencia de una subestimación en el cálculo de las reservas técnicas y otras obligaciones contractuales. (Participación de utilidades, pago de beneficios garantizados, etc.)

### **2.1.7 Riesgo legal en seguros**

Se entiende por riesgo legal en seguros a la posibilidad de incurrir en pérdidas derivadas del incumplimiento de normas legales, de la inobservancia de disposiciones reglamentarias, de códigos de conducta o normas éticas en cualquier jurisdicción en la cual opere la entidad aseguradora. Así mismo, el riesgo legal puede derivar de situaciones de orden legal que puedan afectar la titularidad de los activos o la efectiva recuperación de su valor.

### **2.1.8 Riesgo operacional en seguros**

Se entiende por riesgo operacional a la posibilidad de incurrir en pérdida derivadas de problemas en el desarrollo de las funciones del negocio o sus procesos. La exposición a este riesgo puede resultar de una deficiencia o ruptura en los controles internos o procesos de control, fallas tecnológicas, errores humanos o deshonestidad y catástrofes naturales.

### **2.1.9 Riesgo estratégico en seguros**

Corresponde a la probabilidad de pérdida como consecuencia de la imposibilidad de 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.

### **2.1.10 Riesgo reputacional en Seguros**

Corresponde a la probabilidad de pérdida como consecuencia de incurrir en pérdidas derivadas de la celebración de contratos de seguros y reaseguros con personas y entidades que generen un bajo nivel de confianza para sus asegurados por su nivel de solvencia o la conducta de sus funcionarios o por la celebración de acuerdos sobre los cuales recaiga una publicidad negativa, así como la realización de prácticas que puedan derivar en demandas legales y pérdida de credibilidad del público.

## **2.2 CARACTERÍSTICAS DEL SEARS**

Conforme a lo mencionado en el numeral 1.2 del Capítulo IV, Título IV de la Parte II de la CE 029 de 2014, el SEARS debe contar como mínimo con las siguientes características:

### **2.2.1 Cuantificación del Riesgo**

Teniendo en cuenta que la Superfinanciera no ha reglamentado los riesgos cuantificables ni los parámetros y características para su cuantificación, Positiva adopta las metodologías de medición de riesgos mencionadas en los numerales 1.7 y 3.3 del presente Manual, en lo que respecta a la determinación de la probabilidad e impacto de la materialización de los riesgos en la actividad aseguradora.

### **2.2.2 Cubrimiento de Riesgo**

Con el fin de mantener la exposición a riesgos de la actividad aseguradora dentro del nivel aceptable mencionado en el numeral 1.8 del presente Manual, Positiva adopta los mecanismos definidos en el numeral 3.3.3 del presente Manual.

### **2.2.3 Control de Riesgos**

El SEARS adopta los lineamientos generales mencionados en los numerales 1.7.6 y 3.3.2 del presente manual, con el fin de monitorear los riesgos existentes e identificar nuevos riesgos.

## **2.3 ELEMENTOS DEL SISTEMA DE ADMINISTRACIÓN DE RIESGOS DE SEGUROS**

Al igual que todo Sistema de Administración de Riesgos, el SEARS debe contar con los siguientes elementos, los cuales, en función de las características, tamaño y complejidad de las operaciones realizadas por cada entidad, pueden adoptarse independientemente o formar parte del sistema general:

- a. Políticas sobre asunción de riesgos
- b. Infraestructura adecuada para la gestión de los riesgos de seguros
- c. Metodologías especiales para la medición de los riesgos de seguros
- d. Procesos de Control de Riesgos
- e. Mecanismos de control de los procesos

Tal como se señala en el numeral 1.6 del presente manual, en Positiva Compañía de Seguros S.A. los siguientes elementos que componen un sistema: la estructura organizacional, los órganos de control, la infraestructura tecnológica, las herramientas de divulgación de información y las herramientas de capacitación; son comunes a los tres subsistemas de gestión de riesgos del negocio (SARO, SARC y SEARS).

A continuación, se encuentra la descripción de los demás elementos que componen el SEARS.

### **2.3.1 Políticas sobre asunción de riesgos**

La política de asunción de riesgos del SEARS está descrita en el numeral 1.8 del presente Manual.

### **2.3.2 Metodologías especiales para la medición de los riesgos de seguros**

Se siguen los lineamientos establecidos en el numeral 2.2.1 del presente Manual.

### 2.3.3 Procesos y mecanismos de control

A continuación, se hace una descripción general de los controles mínimos con que cuenta Positiva para la mitigación de los riesgos en la actividad aseguradora:

### 2.3.4 Riesgo de crédito

Para el cubrimiento del riesgo de crédito asumido con los reaseguradores, la compañía realiza seguimiento al REACOEX, así como al cumplimiento de las condiciones económicas pactadas en las notas de cobertura contratadas con dichas Compañías.

### 2.3.5 Riesgo de mercado

Los riesgos de mercado identificados en Positiva, relacionados con incrementos en el valor del Salario Mínimo Legal por encima del IPC, tienen como fuente factores externos fuera del control de la Compañía; debido a esto, son riesgos que serán asumidos.

### 2.3.6 Riesgo de Liquidez

Para efectos de evaluar y monitorear el riesgo de liquidez, la Junta Directiva de Positiva aprobó una metodología basada en la evaluación de la brecha de los flujos asociados al portafolio de inversiones y aquellos estimados para el pasivo de las reservas matemáticas de ARL y Conmutación Pensional. Las brechas de corto y largo plazo se calculan cada 3 meses con los cortes de marzo, junio, septiembre y diciembre. Su cálculo se encuentra reglamentado en el Capítulo XI del Manual de Políticas y Riesgos para la Administración del Portafolio de Inversiones.

### 2.3.7 Riesgo de suscripción

- **Riesgo de tarificación:** Para la mitigación de este riesgo, la compañía tiene implementados controles:
  - ✓ Controles automáticos en el aplicativo, los cuales validan el cumplimiento de las distintas políticas de suscripción definidas.
  - ✓ Para la fijación de la prima de un seguro, el área técnica evalúa los distintos aspectos que pueden hacer la misma insuficiente, tales como la siniestralidad histórica y los gastos asociados a la póliza entre otros.
- **Riesgo de descuento sobre primas:** Para el cubrimiento de este riesgo, el control definido corresponde a la autorización previa de la Gerencia Técnica de Vida de cualquier descuento.
- **Riesgo de concentración:** Para la mitigación de este riesgo, la compañía cuenta con una política de retención de riesgos y de utilización de reaseguradores.
- **Riesgo de diferencia en condiciones:** Para efectos de mitigar este riesgo, Positiva cuenta con procedimientos para el diseño y/o desarrollo de nuevos productos o modificaciones a los mismos, que aseguran que las condiciones ofrecidas a nuestros tomadores se encuentran dentro de la política de retención de riesgo o dentro de las coberturas de los contratos de reaseguros suscritos por la Compañía.

### **2.3.8 Riesgo de insuficiencia de reservas**

Positiva mitiga este riesgo garantizando que el cálculo de las reservas técnicas cumpla con la legislación vigente; para ello la Gerencia de Actuaría y el Actuario Responsable ejecutan en sus procesos los controles respectivos que aseguran el cálculo de la reserva.

Así mismo, las áreas de control (Revisoría Fiscal y Área de Control Interno) realizan una revisión objetiva de dicho cálculo como mínimo una vez al año.

Para el caso de la reserva matemática de ARL, adicionalmente, cada año solicita una revisión por parte de una Firma externa especializada en el tema.

### **2.3.9 Riesgo legal en seguros**

Para el cubrimiento de este riesgo, la compañía hace un seguimiento a la gestión y cumplimiento oportuno de las sentencias judiciales, análisis de los casos para dar respuestas adecuadas y oportunas a los requerimientos y cuenta con alertas automáticas de vencimientos de PQR.

La Secretaría General divulgará dentro de la Compañía, toda la normatividad aplicable a la actividad aseguradora, así como de la jurisprudencia sobre hechos conocidos en el mercado.

La Gerencia Jurídica mantendrá actualizado un normograma dentro del Manual de Calidad SIG, que será de consulta permanente. Se hará una evaluación de las contingencias que se originan en litigios, que no se encuentran respaldadas en los contratos de seguros, y un seguimiento de los procesos judiciales para la evaluación periódica de las contingencias.

### **2.3.10 Riesgo operacional en seguros**

Los controles definidos para los riesgos operacionales de la compañía se encuentran documentados en el Sistema de Administración de Riesgo Operacional (SARO).

### **2.3.11 Riesgo estratégico en seguros**

Para el monitoreo del riesgo estratégico la compañía realiza un seguimiento a la ejecución de la estrategia y al cumplimiento de los objetivos trazados.

### **2.3.12 Riesgo reputacional**

Para el cubrimiento del riesgo reputacional, el principal control definido en Positiva Compañía de Seguros S.A. es el adecuado conocimiento del cliente, siguiendo los lineamientos establecidos en el Capítulo IV del presente Manual (Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo).

## CAPITULO III

### 3. SISTEMA DE ADMINISTRACION DE RIESGO OPERATIVO SARO

#### 3.1 DEFINICIONES

##### 3.1.1. Riesgo

Cualquier situación o circunstancia que de llegar a ocurrir podría impedir el cumplimiento de los objetivos de Positiva, de uno de sus procesos o de una de sus áreas.

De acuerdo a lo anterior, y para efectos del presente capítulo, entendemos riesgo operativo como cualquier situación o circunstancia que de llegar a ocurrir podría impedir el cumplimiento de los objetivos de un proceso.

Por otro lado, se destaca que en el Capítulo XXIII de la Circular Básica Financiera expedida por la Superintendencia Financiera de Colombia, 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 los riesgos legal y reputacional, asociados a tales factores.

El riesgo se clasifica en inherente y residual. Como **RIESGO INHERENTE** debemos entender el riesgo que Positiva, uno de sus procesos o áreas asume en ausencia de cualquier acción que la gerencia pudiera tomar para cambiar la probabilidad o impacto del riesgo.

El **RIESGO RESIDUAL O CONTROLADO** se define como el riesgo remanente una vez aplicados los controles existentes.

##### 3.1.2. Causas del riesgo operativo

Son los medios, circunstancias y agentes generadores de riesgo. Los agentes generadores se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo. Las causas del riesgo se clasifican en: Recurso Humano, Procesos, Tecnología, Infraestructura y Factores Externos.

###### 3.1.2.1. Recurso Humano

Se clasifican como causas relacionadas con el recurso humano la falta de capacitación, el error al ingreso de datos, el incumplir procesos, los comportamientos inadecuados o en contra de las políticas de la organización, entre otros.

###### 3.1.2.2. Procesos

Se clasifican como causas relacionadas con los procesos las debilidades en los mismos, tales como falta de procesos, procesos mal definidos o no divulgados.

### **3.1.2.3. Tecnología**

Inadecuada asignación de perfiles, niveles de seguridad deficientes, ausencia de logs de auditoría en el software, instalación de software no permitido, debilidades en controles, daños en equipo de cómputo no generados por usuarios.

### **3.1.2.4. Infraestructura**

Inadecuados espacios de trabajo, conexiones eléctricas en mal estado, fallas en estudios en elaboración de planos, fallas estudios de terrenos para construcción de edificaciones.

### **3.1.2.5. Factores externos**

Fuerzas de la naturaleza (terremotos, inundaciones, incendios no provocados). Incumplimiento o mala calidad de servicios contratados con proveedores, terrorismo etc.

### **3.1.3. Consecuencia del riesgo**

Resultado de un evento que afecta los objetivos; o la afectación directa del objetivo de un proceso. También se pueden definir como las pérdidas en las que incurre la organización como producto de la materialización de un riesgo. Se clasifican en cuantitativas y cualitativas.

### **3.1.4. Control**

Se define control como cualquier acción que incremente la probabilidad que Positiva, uno de sus procesos o áreas logre sus objetivos, a través de la mitigación o administración de los riesgos. Se clasifican en preventivos y detectivos.

#### **3.1.4.1. Control Preventivo**

Es aquel que se desarrolla antes o durante las actividades con el fin de evitar la materialización de un riesgo.

#### **3.1.4.2. Control Detectivo**

Es aquel que detecta la aparición de un riesgo. Supone que éste ya se ha materializado, por lo que su aplicación no corrige o mitiga el riesgo.

### **3.1.5. Nivel de Riesgo**

Es el grado de exposición al riesgo (severidad). Surge como resultado de relacionar la probabilidad de ocurrencia de un riesgo y el impacto de su materialización. Permite establecer la importancia relativa del riesgo y de esa manera clasificarlo con el fin de priorizar su gestión a través de planes de tratamiento.

### **3.1.6. Plan de tratamiento**

Es el conjunto de actividades definidas cuyo objetivo es modificar el riesgo hasta reducirlo al nivel tolerable definido por la organización, el área o el proceso.

Existen diversas estrategias de tratamiento:

Frente a un riesgo; éste se puede EVITAR; es decir la estrategia consiste en NO realizar la actividad que genera el riesgo.

También se puede MITIGAR; esta estrategia consiste en implementar un plan de tratamiento que busque reducir o controlar su frecuencia o el impacto de su materialización. Generalmente, una vez implementados se convierten en CONTROLES.

Otra estrategia es TRANSFERIR su impacto financiero. Un ejemplo típico de esto es la contratación de un Seguro de daños; a través del cual, en caso de la materialización del riesgo, la pérdida financiera o patrimonial es asumida por la Compañía de Seguros.

Por último, podemos asumir una estrategia de RETENCIÓN del riesgo; la cual consiste en asumirlo. Generalmente esta estrategia es válida cuando el costo de implementar estrategias diferentes es mayor a la pérdida obtenida en caso de la materialización del riesgo.

### **3.1.7. Evento de Riesgo**

Un incidente o suceso REAL, que ocurrió en un determinado lugar, durante un determinado período y que tuvo una consecuencia negativa para la Compañía, proceso o área en términos del cumplimiento de sus objetivos. En otras palabras, se puede definir como la materialización de un riesgo.

### **3.1.8. Frecuencia o probabilidad de ocurrencia**

Número de veces que se repite un hecho, acción o actividad por unidad de tiempo.

### **3.1.9. Impacto**

Efecto del riesgo sobre la Compañía, un proceso o área, en términos de la afectación del objetivo trazado. El impacto puede adoptar varias formas: reducción de ingresos, pérdidas financieras, afectación de la reputación, reducción del número de clientes, entre otros.

### **3.1.10. Sistema de Administración de Riesgo Operativo (SARO)**

Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo.

### **3.1.11. Recursos Inembargables<sup>3</sup>**

Se entenderán como recursos inembargables los siguientes aspectos:

- Los recursos del Sistema de Seguridad Social, entre estos los que administra la entidad administradora de los recursos de Seguridad Social en Salud. (ADRES)
- Los ingresos por cotizaciones que recauden las EPS.
- Los recursos públicos que financian salud.
- Las rentas incorporadas en el presupuesto general de la nación, así como los bienes y derechos de los órganos que lo conforman.
- Los recursos del Sistema General de Participaciones.
- Regalías

---

<sup>3</sup> Art. 594 del Código General del Proceso, Carta Circular 65 de 2018 de la SFC, Circular Externa 022 de 2018 de la SFC.

- Y demás recursos que la constitución y la Ley les otorguen dicha condición

### **3.2 POLÍTICA PARTICULAR DEL SARO**

Además de las políticas, directrices y principios mencionados en el Capítulo I del presente manual, el Sistema de Administración de Riesgo Operativo de Positiva Compañía de Seguros S.A. se enmarca en las siguientes políticas:

#### **3.2.1 Estandarización**

El SARO, además de cumplir con los lineamientos dados por la Superintendencia Financiera en el capítulo XXIII de la Circular Básica Financiera, se implementa y desarrolla teniendo en cuenta la Norma Técnica Colombiana NTC ISO 31000.

#### **3.2.2 Gestión de Calidad**

El SARO se desarrolla por proceso, teniendo en cuenta los lineamientos y en particular el mapa de procesos vigente en Positiva.

#### **3.2.3 Gobernabilidad de los mapas de riesgos operativos**

La Oficina de Gestión Integral de Riesgos es el área encargada de la administración y custodia de los mapas de riesgo operativo de cada proceso. El líder de cada proceso es el dueño de la información que allí reposa.

La información contenida en el mapa de riesgos de un proceso puede ser modificada, eliminada o adicionada por decisión del Líder del Proceso o la Oficina de Gestión Integral de Riesgos.

#### **3.2.4 Continuidad del Negocio**

Positiva asegura la existencia de un proceso independiente, enmarcado dentro de la Gestión de Riesgos Operativos, que vele por la existencia e implementación de estrategias necesarias para proporcionar la continuidad al negocio.

#### **3.2.5 Modificación y/o inclusión de riesgos y controles**

Para la inclusión y/o modificación de riesgos y controles derivados de planes de acción definidos por control interno o cualquier otro ente regulatorio que lo requiera, deberá diligenciarse el formato definido y cargado en la herramienta SIMPLE, posteriormente debe ser enviado a la Oficina de Gestión Integral de Riesgos con mínimo 8 días hábiles de anticipación al vencimiento del plan o al requerimiento de publicación del mismo.

### **3.3 ETAPAS DE LA GESTIÓN DE RIESGO OPERATIVO**

Como se mencionó en el numeral 1.7 del Capítulo I del presente Manual, la gestión de riesgos operativos se desarrolla considerando 7 etapas, las cuales se describen a continuación:

#### **3.3.1 Establecimiento del contexto estratégico**

En esta etapa se busca contextualizar la gestión de riesgos desde 3 dimensiones:

**Contexto externo:** Se refiere a la definición del ambiente externo en el cual Positiva realiza su actividad y busca alcanzar los objetivos propuestos. Las partes interesadas (stakeholders), la forma como se interrelaciona Positiva con su ambiente externo, sus amenazas y oportunidades, son elementos importantes en esta definición.

**Contexto interno:** Se refiere a la definición del ambiente interno en el cual Positiva realiza su actividad y busca alcanzar los objetivos propuestos. Consiste en realizar un análisis de lo que se tiene en una organización o área determinada. Para ello es relevante tener claro con que se cuenta y en que se tienen deficiencias. En otras palabras, es el conocimiento que tenemos de la organización o proceso (estructura, capacidades, recursos), en el cual identificamos sus debilidades y fortalezas.

**Contexto específico:** Consiste en establecer el contexto de cada uno de los procesos de Positiva Compañía de Seguros S.A.

Teniendo en cuenta que la Compañía adelanta un enfoque de operación basado en procesos, para cada uno de ellos se deben tener en cuenta los siguientes aspectos:

- Nombre del proceso al cual se le van administrar los riesgos.
- Definir el responsable o los responsables del proceso.
- Establecer el objetivo general del proceso, de acuerdo a las definiciones contenidas en el manual del mismo.
- Indicadores de desempeño del proceso, metas.
- Delimitar el proceso a través de la identificación de la actividad en la que inicia y finaliza el proceso.

La etapa de establecimiento del contexto es ejecutada por la Junta Directiva y el Comité de Presidencia cada vez que modifica, cambia o define un nuevo plan estratégico.

### **3.3.2 Entendimiento de proceso**

Para efectuar una adecuada identificación de riesgos se debe partir de la definición y conocimiento claro del objetivo del proceso y de cada uno de sus procedimientos, por lo anterior es importante que la documentación se encuentre actualizada y sea conocida por los miembros del equipo de trabajo que llevarán a cabo la identificación de riesgos.

### **3.3.3 Levantamiento de riesgos operativos**

En esta etapa se identifican todas aquellas situaciones que se han materializado en el proceso o que podrían llegar a ocurrir afectando el logro de los objetivos del mismo.

Para hacer el levantamiento de riesgos operativos se deben tener en cuenta los siguientes parámetros:

- Si no afecta el objetivo, NO ES UN RIESGO.
- La ausencia de un control, NO ES UN RIESGO.
- El incumplimiento del objetivo, NO ES UN RIESGO.
- La redacción adecuada de un riesgo cumple con:
  - ✓ Verbo en infinitivo+ descripción de la acción.
  - ✓ Adjetivo + acción que se ve afectada.
- Evite las negaciones para describir el riesgo.

### **3.3.4 Identificación del riesgo**

El objetivo específico de esta etapa es identificar los riesgos inherentes a los procedimientos de cada proceso.

En caso de presentarse procesos de fusiones, adquisiciones, cesión de activos, pasivos y contratos; el grupo multidisciplinario designado para liderar este cambio tendrá la responsabilidad de identificar los riesgos asociados a dicha labor. En cualquier caso, contarán con el apoyo metodológico de la oficina de Gestión Integral de Riesgos.

Para la identificación de los riesgos se tendrá como criterio básico el aporte de los colaboradores involucrados en la ejecución de cada procedimiento, aporte que será generado a través de la realización de reuniones en las cuales participen un representante de la Oficina de Gestión Integral de Riesgos, el líder o dueño del proceso, el gestor de riesgo del proceso y opcionalmente el (los) colaborador(es) que el líder del proceso considere necesario(s).

Para la adecuada identificación de los riesgos de un proceso, la Oficina de Gestión Integral de Riesgos, aparte de la experiencia de los colaboradores, se apoya en la regulación aplicable, los soportes documentales que proporcionen el área de Control Interno y la Revisoría Fiscal a través de sus informes y la información histórica consignada en el registro de eventos de riesgo operativo.

La revisión periódica de riesgos se organizará teniendo en cuenta los siguientes lineamientos:

#### **Componente Fijo**

Lineamiento para procesos asociados a los macroprocesos misionales: se revisarán como mínimo una vez al año conforme al modelo operacional vigente en la Entidad y acorde con el cronograma anual de trabajo definido por la Oficina de Gestión Integral de Riesgos.

#### **Componente Flexible**

Lineamiento para procesos asociados a los macroprocesos de tipo Estratégicos, de Apoyo y Evaluación: se revisarán en un periodo no mayor a 2 años bajo los siguientes criterios.

- Acorde al cronograma anual definido por la Oficina de Gestión Integral de Riesgos.
- A solicitud del proceso por actualización del mismo.
- Cuando la Oficina de Gestión Integral de Riesgos lo considere necesario.

Esta etapa de identificación de riesgos comprende los siguientes pasos:

#### **3.3.4.1 Identificación de causas de riesgo**

A continuación, para cada riesgo identificado y clasificado, se procede a su respectivo análisis de causas. Para tal fin, es válido el uso de cualquier de las distintas metodologías conocidas, tales como lluvia de ideas, espina de pescado o causa-efecto, 5 por qué's, 5W2H<sup>4</sup> o cualquier otra metodología

---

<sup>4</sup> 5W2H: Nombre dado a una metodología de identificación de causas por sus siglas en inglés: 5W + 2H. Las "W" hacen referencia a: What, When, Who, Where y Why. Las "H" hacen referencia a: How y How much.

La(s) causa(s) raíz(es) identificada(s) debe ser descrita y clasificada en una de las siguientes categorías, conforme a las definiciones mencionadas en el numeral 3.1.2 del presente Manual:

**Factores de Riesgos:**

- Recurso Humano
- Procesos
- Tecnología
- Infraestructura
- Factores externos

**3.3.4.2 Medición y Control de riesgo**

El análisis del riesgo busca establecer la calificación del riesgo en términos de su probabilidad de ocurrencia y el impacto de sus consecuencias, con el fin de estimar el nivel de riesgo inherente, así como determinar los controles existentes y su eficiencia para estimar el nivel de riesgo residual.

Como nivel de riesgo inherente debemos entender el nivel de riesgo que Positiva, uno de sus procesos o áreas asume en ausencia de cualquier acción que la gerencia pudiera tomar para cambiar la probabilidad o impacto del riesgo.

El nivel de riesgo residual se define como el nivel de riesgo remanente una vez aplicados los controles existentes.

Para efectos de realizar el análisis del riesgo, se deben seguir los siguientes pasos:

**3.3.4.3 Calificación de riesgos**

Al igual que en la etapa de identificación, la calificación de riesgos tiene como criterio básico para su ejecución, el aporte de los colaboradores involucrados en el proceso y/o procedimiento analizado, por lo que la determinación de la probabilidad o frecuencia del riesgo y su impacto se realiza a través de las mismas reuniones mencionadas en el numeral 3.3.2.

La calificación riesgos de cada proceso se debe llevar a cabo conforme a los componentes definidos en el numeral 3.3.4 Identificación de Riesgos y de acuerdo al modelo operacional vigente para la Compañía.

Es importante mencionar que, para riesgos ya identificados, el Comité de Riesgos y la Oficina de Gestión Integral de Riesgos tienen la potestad de modificar su probabilidad de ocurrencia y su impacto si evidencian argumentos suficientes para hacerlo. De igual forma dichos criterios pueden ser modificados por sugerencia de los Órganos de Control Interno (Oficina de Control Interno o Revisoría Fiscal).

**3.3.4.4 Criterios para la calificación de la probabilidad de ocurrencia**

Positiva utiliza una metodología que combina aspectos cuantitativos y cualitativos para calificar la probabilidad de ocurrencia de los riesgos, éstos se deben aplicar en virtud de la disponibilidad de información. Los dos posibles criterios son:

**Probabilidad matemática:** Número de casos en los que se materializa el riesgo dividido por el número de casos posibles en los que se puede materializar el riesgo. Utilizar este criterio exige la existencia de una base de datos de eventos de riesgo materializados. Es la primera opción para calificar la probabilidad de un riesgo.

**Posibilidad:** Corresponde a una definición basada en la experiencia del equipo de trabajo que lleva a cabo la calificación. Supone la inexistencia de datos que soporten la calificación otorgada o en el mejor de los casos, la existencia de algunos datos e información cuantitativa no verificable o estadísticamente no válida para el cálculo de una probabilidad.

En la siguiente tabla se describen los niveles de probabilidad aplicables en Positiva y sus criterios de calificación:

**TABLA N° 1.** Niveles de Probabilidad y Criterios de Calificación.

NIVEL	PROBABILIDAD MATEMATICA	POSIBILIDAD	VALOR
CASI CIERTO	Mayor al 80%	En el último año, el riesgo ha ocurrido la mayoría de las veces que se ejecuta el proceso o la actividad. La información existente indica que se presenta máximo cada 2 operaciones.	5
PROBABLE	Mayor que 60% y menor que 80%	En el último año, el riesgo se ha materializado en varias ocasiones. La información existente permite señalar que se presenta máximo cada 10 operaciones.	4
POSIBLE	Mayor que 40% y menor que 60%	En el último año, el riesgo se ha materializado en contadas ocasiones, bajo circunstancias normales. La información existente permite señalar que se presenta máximo cada 100 operaciones.	3
IMPROBABLE	Mayor que 20% y menor que 40%	En el último año, el riesgo se ha materializado en contadas ocasiones, bajo circunstancias excepcionales. La información disponible permite inferir que se puede presentar máximo cada 1000 operaciones.	2
RARO	Menor que 20%	En el último año, el riesgo NO se ha materializado. No existe información al respecto.	1

### 3.3.4.5 Criterios para la calificación del impacto de materialización

La determinación del impacto de la materialización de un riesgo en Positiva se realiza mediante dos tipos de evaluaciones:

**Evaluación cuantitativa:** a través de la definición del impacto financiero de la materialización del riesgo.

Por impacto financiero se entiende el valor histórico de la máxima pérdida financiera que haya tenido la compañía por efecto de la materialización de un riesgo. Por pérdida financiera debemos entender: multas, sanciones, indemnizaciones, reducción de ingresos o cualquier afectación del estado de pérdidas y ganancias atribuible a la materialización de un riesgo.

En la siguiente tabla se describen los niveles de impacto aplicables en Positiva en caso de utilizar la evaluación cuantitativa y sus criterios de calificación:

**TABLA N° 2.** Niveles de Impacto y Criterios de Calificación.

EVALUACIÓN CUANTITATIVA		
TIPO DE IMPACTO	PERDIDAS ECONOMICAS	VALOR
CATASTROFICO	Pérdidas > 1.000 SMLV	5
MAYOR	700 SMLV < Pérdidas <=1.000 SMLV	4
MODERADO	400 SMLV < Pérdidas <= 700 SMLV	3
MENOR	100 SMLV < Pérdidas <= 400 SMLV	2
INSIGNIFICANTE	Pérdidas <100 SMLV	1

**Evaluación cualitativa:** Basada en el conocimiento de los expertos en el proceso o procedimiento para el cual se esté analizando riesgos.

La calificación obtenida a través de esta metodología combina la evaluación de los siguientes impactos:

- ✓ **IMPACTO LEGAL** entendido como la actuación del Supervisor, de cualquier otra entidad reguladora o una rama del poder judicial, a través de una posible sanción, multa, llamado de atención, acción administrativa o sentencia judicial entre otros.
- ✓ **IMPACTO REPUTACIONAL** entendido como el desprestigio, mala imagen o publicidad negativa para la Compañía.
- ✓ **IMPACTO OPERATIVO** entendido como la afectación en los niveles de servicio o atención al cliente por requerir de un tiempo de reparación o recuperación.

- ✓ IMPACTO DE GOBERNABILIDAD entendido como la necesidad de escalar la atención y búsqueda de una solución exitosa a la situación presentada.
- ✓ IMPACTO COMERCIAL entendido como la reducción del número de clientes de la Compañía y su efecto sobre variables de participación en mercado.

En la siguiente tabla se describen los niveles de impacto aplicables en Positiva en caso de utilizar la evaluación cualitativa y sus criterios de calificación:

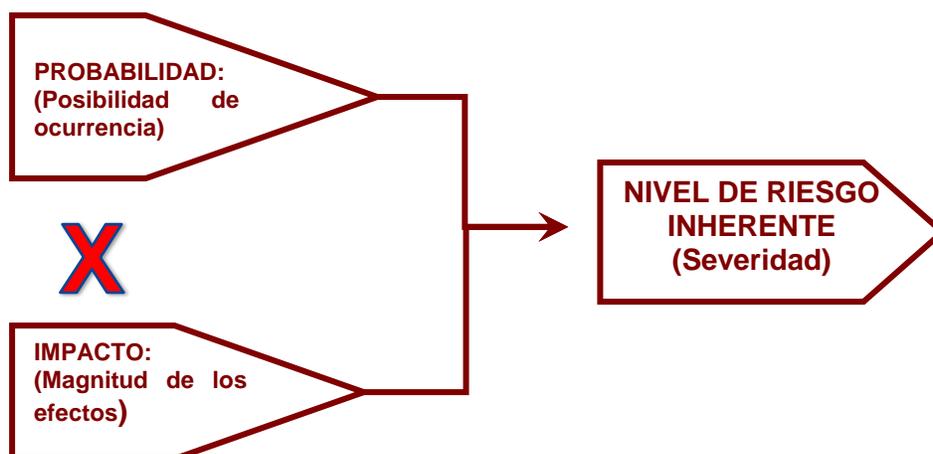
**TABLA N° 3.** Niveles de Impacto Evaluación Cualitativa y Criterios de Calificación.

EVALUACIÓN CUALITATIVA						
TIPO DE IMPACTO	IMPACTO LEGAL	IMPACTO REPUTACIONAL	IMPACTO OPERATIVO	IMPACTO DE GOBERNABILIDAD	IMPACTO COMERCIAL	VALOR
<b>CATASTROFICO</b>	La materialización del riesgo genera la Intervención de la Compañía por parte de la Superintendencia Financiera	La materialización del riesgo Afecta la Imagen de Positiva a nivel Nacional e Internacional	La materialización del riesgo implica un retraso de más de 3 horas en la prestación del servicio al cliente final	La materialización del riesgo implica la intervención de la Junta Directiva en la búsqueda de una solución	La materialización del riesgo implica una reducción en el número de clientes mayor al 10%	5
<b>MAYOR</b>	La materialización del riesgo genera el pago de multas o sanciones institucionales y/o posibles indemnizaciones	La materialización del riesgo afecta la Imagen a nivel de Nacional	La materialización del riesgo implica un retraso entre 2 y 3 horas en la prestación del servicio al cliente final	La materialización del riesgo implica la intervención de la Presidencia de la Compañía en la búsqueda de una solución	La materialización del riesgo implica una reducción en el número de clientes entre el 7% y el 10%	4
<b>MODERADO</b>	La materialización del riesgo genera acciones administrativas, apertura de pliego de cargos o investigaciones de la Superintendencia Financiera o cualquier otro órgano de control	La materialización del riesgo afecta de la Imagen a nivel de una sucursal	La materialización del riesgo implica un retraso entre 1 y 2 horas en la prestación del servicio al cliente final	La materialización del riesgo implica la intervención de alguna o algunas de las Vicepresidencias	La materialización del riesgo implica una reducción en el número entre el 3% y el 7%	3
<b>MENOR</b>	La materialización del riesgo genera glosas en los informes de visita de los Órganos de Control y Vigilancia	La materialización del riesgo afecta la Imagen a nivel de una vicepresidencia.	La materialización del riesgo implica un retraso de menos de 1 hora en la prestación del servicio al cliente final	La materialización del riesgo obliga a la toma de decisiones a nivel de las Gerencias, en busca de una solución	La materialización del riesgo implica una reducción en el número de clientes menor al 3%	2
<b>INSIGNIFICANTE</b>	La materialización del riesgo genera solicitudes de información preliminar por parte de los Órganos de Control y Vigilancia	La materialización del riesgo afecta la Imagen a Nivel de un Área o Gerencia	La materialización del riesgo NO afecta el nivel de servicio prestado al cliente final	La materialización del riesgo implica ajustar actividades del día a día que no necesitan aprobación de niveles superiores	La materialización del riesgo NO genera la pérdida de clientes.	1

### 3.3.4.6 Estimación del nivel de riesgo inherente

Una vez definida la probabilidad y el impacto se procede a calcular el nivel de riesgo inherente, multiplicando el valor asignado a la probabilidad por el valor asignado al impacto.

FIGURA N° 2. Obtención de Riesgo Inherente.



### 3.3.4.7 Identificación de controles

Como se mencionó al comienzo del presente capítulo, se define como control cualquier acción encaminada a mitigar o administrar el riesgo e incrementar la probabilidad de que la compañía o un proceso logren sus metas y objetivos. De esta forma los controles se pueden entender como los procesos, dispositivos, prácticas u otras acciones que actúan para eliminar o minimizar los riesgos.

En esta sub-etapa de medición y control de riesgo se busca conocer todos y cada uno de los controles con que cuenta el proceso o procedimiento analizado para mitigar los riesgos que asume.

La identificación de controles tiene como criterio básico para su ejecución, el aporte de los colaboradores involucrados en el proceso y/o procedimiento analizado, por lo que se realiza a través de las reuniones mencionadas en el numeral 3.3.2.

Para la adecuada identificación de los controles de un proceso, la Oficina de Gestión Integral de Riesgos, aparte de la experiencia de los colaboradores, se apoya en los soportes documentales que proporcionen el área de Control Interno y la Revisoría Fiscal a través de sus informes.

La identificación de controles se debe llevar a cabo de igual manera con lo definido en el numeral 3.3.4 Identificación de Riesgos.

### 3.3.4.8 Calificación de la eficacia de los controles

Corresponde a la determinación del nivel de eficacia del control o controles establecidos para mitigar un riesgo.

Para la calificación de los controles, Positiva utiliza un esquema que combina la autoevaluación de la eficacia en el diseño del control, a cargo de cada uno de los líderes o dueños de proceso, y una evaluación independiente de su ejecución, tal como se observa en la siguiente gráfica.

**FIGURA N° 3.** Obtención Eficacia del Control.



### Autoevaluación de Controles

Para evaluar la eficacia de los controles a través de la herramienta de gestión de riesgos, se generarán los cuestionarios de controles, donde los dueños de proceso deben responder las preguntas de la siguiente tabla:

**TABLA N° 4.** Atributos de Control.

No	Criterios	Preguntas y posibles repuestas
1	<b>FUNCIONABILIDAD (CLASE)</b>	Qué clase de control es? * Preventivo * Detectivo
2	<b>APLICACIÓN (TIPO)</b>	Qué <u>tipo de Control</u> es? * Automático * Semiautomático * Manual
3	<b>DOCUMENTACIÓN</b>	El control se encuentra debidamente documentado en manuales o flujogramas? * Si * No

No	Criterios	Preguntas y posibles repuestas
4	<b>RESPONSABLE</b>	El control cuenta con un responsable <u>independiente</u> asignado para su aplicación? * Si * No
5	<b>COBERTURA (SUBJETIVIDAD)</b>	Que cobertura tiene el control? * Total * Parcial * Baja
6	<b>FRECUENCIA (SUBJETIVIDAD)</b>	El control se ejecuta cada vez que se requiera? * Si * Algunas Veces * No

La autoevaluación de controles se debe llevar **a cabo mínimo una vez al año**, acorde con el cronograma anual de trabajo definido por la Oficina de Gestión Integral de Riesgos, y abarca los procesos y sus procedimientos, que no hayan sido objeto de revisión o actualización en los tres meses anteriores a fecha de inicio de la autoevaluación.

#### **Evaluación Independiente (Prueba de Recorrido)**

La eficacia de la ejecución será evaluada por el equipo de la Oficina de Gestión Integral de Riesgos, mediante la metodología definida (*Véase Anexo II del presente Manual*), la muestra a evaluar será aleatoria y estará en función del número de controles que tenga el proceso; es decir es posible que no todos los controles cuenten con esta evaluación, caso en el cual la eficacia de un control corresponde a la eficacia de su diseño.

La calificación de controles estará coordinada por la Oficina de Gestión Integral de Riesgos, con el apoyo de todos los funcionarios de la Compañía, a través del proceso de captura de información definido para tal fin.

Para determinar si un control se considera eficaz, la Oficina de Gestión Integral de Riesgos determino los siguientes criterios:

- Eficacia Alta: El riesgo que mitiga el control evaluado No presenta eventos de riesgos durante el periodo de evaluación.
- Eficacia Moderada: El riesgo que mitiga el control evaluado presenta eventos de riesgos considerados de impacto leve o moderado para el proceso.
- Eficacia Baja: El riesgo que mitiga el control evaluado presenta eventos de riesgos considerados de alto impacto para la entidad.

Para determinar la escala de impacto de un evento de riesgo (alto, moderado, leve) véase numeral 3.4.1 Clase o clasificación de los eventos riesgo operativo.

Es importante mencionar que el Comité de Riesgos y la Oficina de Gestión Integral de Riesgos tienen la potestad de modificar la calificación de un control si evidencian argumentos suficientes para hacerlo. De igual forma dicha calificación puede ser modificada por sugerencia de los Órganos de Control Interno (Oficina de Control Interno o Revisoría Fiscal).

La evaluación independiente de los controles se debe llevar a cabo conforme a los lineamientos definidos en el numeral 3.3.4 Identificación de Riesgos.

#### **3.3.4.9 Estimación del Nivel de riesgo controlado**

El Nivel de riesgo inherente afectado por la eficacia del control(es) identificado(s) se denomina Nivel de Riesgo Controlado.

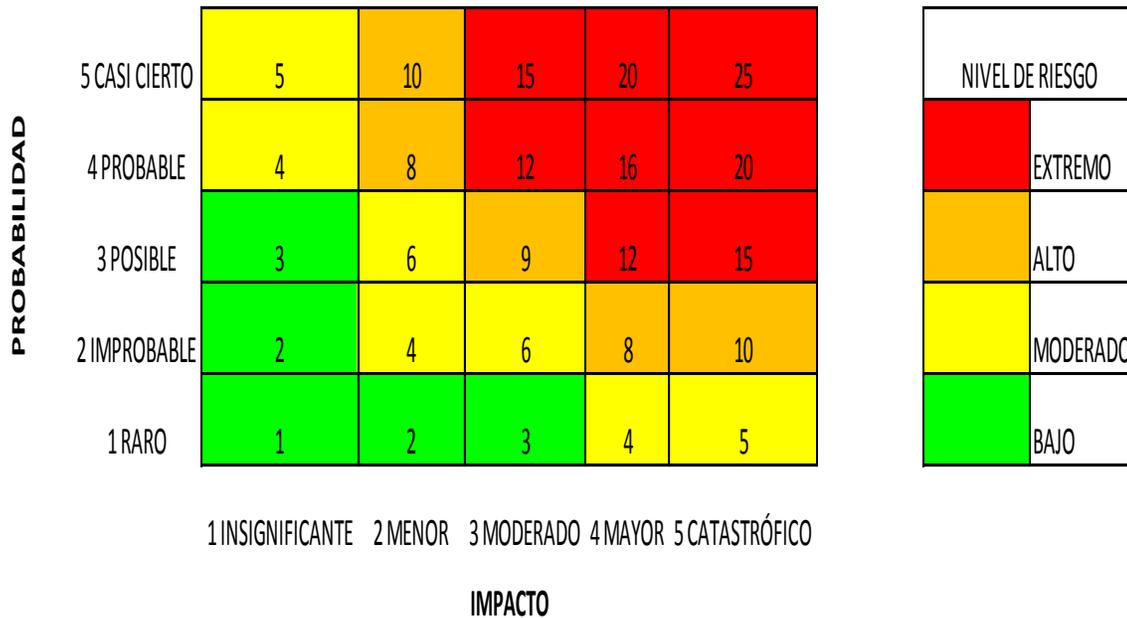
**FIGURA N° 4.** Obtención Nivel de Riesgo Controlado.



#### **3.3.5 Matriz de riesgos**

El nivel de riesgo o severidad, tanto inherente como residual, se representa gráficamente en una matriz de riesgos, tal como se muestra en la siguiente gráfica.

**FIGURA N° 5. Niveles Matriz de Severidad.**



### 3.3.6 Evaluación de riesgos

Esta etapa comprende la comparación del nivel de riesgo residual o controlado contra el apetito de riesgo establecido por la Junta Directiva de la compañía, con el fin de determinar el grado de exposición de Positiva al riesgo operativo.

La evaluación permite establecer los riesgos a los que se les debe dar prioridad para efecto de definir los planes de tratamiento respectivos.

El grado de exposición de Positiva al riesgo operativo y su comparación con el apetito de riesgo definido se realizará como mínimo trimestralmente y será una responsabilidad de la Oficina de Gestión Integral de Riesgos.

### 3.3.7 Tratamiento de riesgos

Esta etapa comprende identificar, registrar, evaluar y elegir el conjunto de opciones para mitigar el riesgo o mejorar el control existente, hasta llevarlo al nivel de riesgo aceptable. Todos aquellos riesgos cuyo nivel de riesgo residual o controlado se encuentre ubicado en los niveles ALTO Y EXTREMO, según la matriz de riesgos explicada en el numeral 3.3.5 del presente capítulo, requieren obligatoriamente el diseño e implementación de un plan de tratamiento.

Para el caso de los niveles de riesgo MODERADO Y BAJO es decisión de los líderes o dueños de proceso, así como de los gestores de riesgo, la implementación de planes de tratamiento.

A continuación, se encuentran las opciones de tratamiento de riesgos:

**TABLA N° 5. Opciones de Tratamiento de Riesgos.**

<b>EVITAR</b>	No realizar la actividad que genera el riesgo
<b>REDUCIR</b>	<p>Implica tomar medidas encaminadas a disminuir la probabilidad y/o el impacto del riesgo a través del tratamiento de las causas que lo generan. A nivel de ejemplo se encuentran las siguientes posibilidades:</p> <p><b>Para disminuir la probabilidad:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Auditoría o programas de verificación de cumplimiento.</li> <li><input type="checkbox"/> Cambio de condiciones contractuales.</li> <li><input type="checkbox"/> Revisión formal de especificaciones, requerimientos y diseño.</li> <li><input type="checkbox"/> Inspección y procesos de control.</li> <li><input type="checkbox"/> Mantenimiento Correctivo.</li> <li><input type="checkbox"/> Aseguramiento de Calidad, Gestión y normalización.</li> <li><input type="checkbox"/> Investigación y desarrollo Tecnológico.</li> <li><input type="checkbox"/> Supervisión.</li> <li><input type="checkbox"/> Ensayos.</li> <li><input type="checkbox"/> Disposiciones organizacionales.</li> <li><input type="checkbox"/> Técnicas de control.</li> </ul> <p><b>Para disminuir el impacto:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Planes de contingencia.</li> <li><input type="checkbox"/> Arreglos contractuales.</li> <li><input type="checkbox"/> Condiciones contractuales.</li> <li><input type="checkbox"/> Planes de recuperación de desastres.</li> <li><input type="checkbox"/> Planes de control de fraudes.</li> <li><input type="checkbox"/> Reducción de exposición a causas de riesgo.</li> <li><input type="checkbox"/> Políticas de control de precios.</li> <li><input type="checkbox"/> Separación o reubicación de una actividad o de recursos.</li> </ul>
<b>TRANSFERIR</b>	Reduce el impacto de la materialización del riesgo, a través del traspaso de las pérdidas a otras organizaciones; como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los Contratos de riesgo compartido.
<b>RETENER</b>	Después de reducir o transferir el riesgo, hay parte del riesgo que se ha retenido. Deben implementarse planes para manejar sus consecuencias e identificar la fuente de financiación. La retención de un riesgo también puede ocurrir, si se ha fallado en su identificación.

Los planes de tratamiento definidos para ajustar el nivel de riesgo residual o controlado se constituyen en ACCIONES PREVENTIVAS Y/O CORRECTIVAS del Sistema Integral de Gestión (SIG), por lo que su seguimiento y monitoreo se regirá por las directrices dadas en el SIG.

### 3.3.8 Monitoreo y revisión

Pocos riesgos permanecen estáticos, por lo tanto, los riesgos y la efectividad de sus medidas de control necesitan ser monitoreados continuamente, para asegurar que circunstancias cambiantes del entorno no generan nuevos riesgos o los modifican.

Por lo anterior, Positiva monitorea trimestralmente su perfil de riesgo a través del indicador denominado “Nivel de Riesgos controlado SARO”. Dicho indicador hace parte del Balance Scorecard de la Compañía como un indicador corporativo. Su objetivo es monitorear el cumplimiento del nivel de riesgo operativo establecido por la Junta Directiva a nivel institucional.

De igual manera, y para algunos riesgos identificados en procesos críticos (definidos dentro del documento Análisis de Impacto al Negocio– BIA identificado en el aplicativo SIMPLE con el código EST\_3\_2\_1\_OD01), la Oficina de Gestión Integral de Riesgos establecerá indicadores descriptivos que le faciliten al dueño del proceso el seguimiento efectivo de los riesgos.

La metodología para gestionar los indicadores del Sistema de Administración de Riesgo Operativo se encuentra alineada a las directrices definidas en el instructivo de Construcción de Indicadores que define la Oficina de Estrategia y Desarrollo.

El Comité de riesgos, en sus reuniones periódicas, monitorea la evolución del nivel de riesgo de la Compañía y de los procesos.

### **3.3.9 Comunicación y consulta**

En cumplimiento del lineamiento general establecido sobre la divulgación de información en el numeral 1.10 del presente Manual, Positiva ha diseñado un sistema de reportes que garantiza el funcionamiento de sus propios procedimientos y el cumplimiento de sus obligaciones.

Para cumplir con lo anterior, como mínimo se implementará:

- Publicación a través de la intranet de la información correspondiente a los procedimientos y procesos desarrollados en la organización, así como los mapas de riesgo operativos correspondientes.
- Reportes a la Junta Directiva, como mínimo semestrales, que permitan dar a conocer el perfil de riesgo de Positiva.
- Publicación en el Informe de gestión anual de la gestión adelantada en materia de administración de riesgos operativos.
- Reportes periódicos de la Oficina de Gestión Integral de Riesgos sobre el cumplimiento de las políticas, límites y nivel de exposición a los distintos riesgos del negocio asumidos.

## **3.4 REGISTRO DE EVENTOS DE RIESGO (RER)**

El Registro de Eventos de Riesgo (RER) es un mecanismo a través del cual se registran y administran ordenadamente todos los eventos de riesgo operativo materializados en la Compañía:

### **3.4.1 Clase o clasificación de los eventos riesgo operativo**

Una vez identificado y descrito el riesgo, se procede a su clasificación. Para tal fin, todos los riesgos operativos deben encontrarse en una de las siguientes categorías:

- **Fraude Interno:** Cualquier tipo de actuación orientada a defraudar, apropiarse indebidamente de bienes o incumplir normas, leyes o políticas empresariales en las que se encuentra implicado, al menos, un empleado o administrador de la entidad, en beneficio propio o de un tercero.
- **Fraude Externo:** Cualquier tipo de actuación o situación orientada a defraudar, apropiarse indebidamente de bienes o incumplir normas, leyes o políticas

empresariales por parte de una persona externa a la entidad, en beneficio propio o de un tercero.

- **Relaciones Laborales y Seguridad en el puesto de trabajo:** Actuaciones o situaciones incompatibles con la legislación laboral, los acuerdos internos de trabajo en general, la legislación vigente sobre la materia o el pago de reclamaciones por daños personales.
- **Prácticas con clientes, productos y negocios:** actuaciones que conlleven el incumplimiento negligente o involuntario de las obligaciones frente a los clientes, de prácticas comerciales o de obligaciones relacionadas con el diseño de un producto o servicio.
- **Daños a Activos físicos:** actuaciones que conlleven daños o perjuicios a activos físicos de la entidad.
- **Ejecución y administración de procesos:** Actuaciones o situaciones que impliquen errores en la ejecución y administración de los procesos.
- **Fallos en sistemas y/o Tecnología:** Actuaciones o situaciones asociadas con la capacidad de la compañía para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporte el cumplimiento de la misión.
- **Cumplimiento o Conformidad Legal:** Actuaciones o situaciones que impliquen que la compañía pueda ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales; de igual forma se entiende por riesgo legal actuaciones o situaciones que afecten la formalización o ejecución de contratos o transacciones.
- **Afectación de la reputación o buen nombre:** Cualquier actuación o situación que conlleve al desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la Compañía y sus prácticas de negocio.

Adicional se consideran los siguientes criterios de **referencia**<sup>5</sup> para determinar la escala de impacto de un evento de riesgo así:

- **Eventos de riesgos de Impacto Alto:** todos aquellos relacionados con conductas asociadas a fraude, corrupción, lavado de activos o financiación del terrorismo al interior de la entidad. Eventos de fraude externo que involucren a Positiva de forma directa (riesgo de contagio). Eventos que detengan la operación de la entidad o de proveedores críticos por tiempos superiores a los RTO asociados a los procesos críticos. Eventos que generen una interrupción de procesos o proveedores críticos a nivel nacional o regional con duración superior a su RTO. Eventos relacionados con crisis que afecten a nivel nacional la reputación de la entidad. Eventos relacionados con pago de multas o sanciones por entes de

---

<sup>5</sup> Criterios de referencia, de cualquier forma, **eventos que salgan de esta categorización** serán clasificados por los profesionales de la OGIR bajo su **juicio de expertos**.

control y que han llegado a su última instancia. Eventos relacionados con desastres naturales o actos de vandalismo que afecten de forma significativa los activos de la entidad o presenten muertes o lesiones de personas. Eventos asociados con ataque cibernéticos que impidan la operación de la entidad o alguno de sus procesos.

- **Eventos de riesgos de Impacto Moderado:** eventos relacionados con fraude externo que puedan relacionar indirectamente a Positiva o alguno de sus empleados. Eventos que detengan de forma parcial la operación de alguna de las sucursales de la entidad pero que no tengan involucrados lesionados o heridos. Eventos que generen la detención de procesos críticos en sucursales o proveedores que no superen los RTO. Eventos relacionados con crisis que afectan la reputación de la entidad en una sucursal. Eventos que generen hallazgos de entes de control internos o externos, pero que no implican multas o sanciones. Eventos que generen insatisfacción justificada de clientes que no estén relacionados con servicios vitales. Eventos relacionados con daño a activos de la entidad que no sean cubiertos por seguros. Eventos asociados con ataque cibernéticos que afecten gravemente los principios de seguridad de la información pero que no detienen la operación.
- **Eventos de riesgos de Impacto leve:** todos aquellos relacionados con conductas asociadas a error humano, incumplimientos o inoportunidad en la generación o entrega de información en aspectos puntuales asociados a lineamientos, políticas o procedimientos internos, y que, por ende, generen llamados de atención verbales o escritos. Eventos que detengan la operación de algún proceso no crítico de la entidad por un tiempo superior a 48 horas. Eventos relacionados con afectación o pérdida de activos de la entidad inferiores a ½ salario mínimo legal vigente y que sea cubierto por seguros. Eventos asociados con incidencias puntuales que impidan la operación de un o un grupo de funcionarios pero que no detengan totalmente el proceso.

### 3.4.2 Tipo de pérdida de los eventos riesgo operativo

- Tipo A: Generen pérdidas y afecten el estado de resultados.
- Tipo B: Generen pérdidas y NO afecten el estado de resultados
- Tipo C: No generen pérdidas y por lo tanto no afecten el estado de resultados.

El objetivo de este registro es construir una base de eventos de riesgo que permita adelantar un análisis cualitativo y cuantitativo acerca de la probabilidad e impacto de la materialización de los riesgos.

El RER será construido a partir de la información recibida por parte de los Vicepresidentes, Jefes de Oficina, Gerentes y/o delegados, quienes serán los responsables de reportar de forma mensual los eventos presentados en su área o sucursal, el último día hábil de cada mes. De no presentarse eventos durante el mes a reportar, se deberá informar tal hecho a través de comunicación formal por correo electrónico.

El análisis y depuración previos a la consolidación y cargue de los eventos de riesgo está a cargo de los profesionales de la, Oficina de Gestión Integral de Riesgos área que podrá

sugerir las medidas de control inmediatas a que haya lugar.

La información contenida en el RER, está sujeta a la aplicación integral de las políticas aprobadas en la Compañía relacionadas con seguridad de la información.

La Oficina de Gestión Integral de Riesgos podrá consultar y obtener de fuentes alternas de información; datos que le permitan identificar eventos de riesgo no reportados por las áreas de la compañía. Posterior a estas indagaciones, y previo análisis de la relevancia en los datos obtenidos, procederá a levantar el respectivo evento de riesgo, el cual será cargado en la base de información consolidada de eventos de riesgo.

Se entenderá como fuentes de información alternas, para la detección de eventos de riesgo, todos aquellos informes generados por parte de los entes de control, tanto internos como externos; las bases de información administradas o generadas por los aplicativos que utilizan las áreas de la compañía, el reporte de provisiones administrativas realizadas para procesos judiciales, las sanciones impuestas a la compañía por las diferentes instancias que la vigilan, entre otras.

Los campos mínimos del RER en Positiva serán los mencionados en el numeral 3.2.5.1 del Capítulo XXIII de la Circular Básica Financiera expedida por la Superintendencia Financiera de Colombia.

### **3.5 ÓRDENES DE EMBARGO**

Una vez recibida la orden de embargo, el funcionario encargado de dar cumplimiento a la misma, deberá verificar si los recursos sobre los cuales recae esta orden no cuentan con condición de “Recurso Inembargable”, tal y como se encuentra definido en este Manual. En aquellos casos en los que se logre establecer la inembargabilidad de los recursos, la Compañía dará cumplimiento a lo establecido en el artículo 594 del Código General del Proceso, para lo cual el funcionario responsable deberá notificar al día hábil siguiente a la autoridad que decretó la medida, sobre el no acatamiento de la medida por cuanto dichos recursos ostentan la calidad de inembargables.

Así mismo, la Compañía cuenta con las medidas, controles y sistemas de información necesarios para que sus funcionarios de los respectivos procesos (Gestión Jurídica, Gestión de Canales, Gestión Humana y Gestión de Reconocimiento de Prestaciones Asistenciales y Económicas) reciban, procesen, acaten, atiendan y den respuesta a los mandatos judiciales y administrativos de forma completa, oportuna y conforme al procedimiento establecido en la ley.

De otra parte, la Compañía ha establecido los controles necesarios para verificar que se atiendan de forma completa y oportuna las solicitudes de sus clientes, intermediarios, proveedores, funcionarios, y terceros, relacionadas con las órdenes de desembargo.

### **3.6 MEDIDAS ANTE EL INCUMPLIMIENTO DEL SARO**

En caso de identificarse posibles omisiones por parte de las áreas de la organización respecto a las siguientes directrices del Sistema de Administración de Riesgo Operativo - SARO:

- Reporte de Eventos de Riesgo – RER
- Autoevaluación de Controles
- Aprobación de Mapas de Riesgos y Reporte Controles
- Capacitación Anual Obligatoria en Riesgos

El Jefe de Oficina de Gestión Integral de Riesgos, en primera instancia, remitirá comunicación informando de la omisión al Gerente, Jefe de Oficina o Vicepresidente del área infractora con el fin de que subsanen la situación y/o establezcan el plan de mejoramiento respectivo.

Si después de hacer seguimiento al caso, no se obtiene una solución a la situación o se vuelve a repetir, después de haber agotado lo descrito anteriormente, el Jefe de la Oficina de Gestión Integral de Riesgo procederá a informar a la Oficina de Control Disciplinario para que evalúe el grado de incumplimiento y/o impacto sobre la Compañía y tome las medidas correspondientes.

Nota: Todos los directivos y trabajadores de Positiva Compañía de Seguros S.A. deben reportar los eventos de riesgo – RER – que evidencien conductas fraudulentas o corruptas. En caso de identificarse que dichas situaciones no fueron reportadas a la OGIR de forma oportuna, el caso sería remitido al área de Control Disciplinario.

## **CAPITULO IV**

### **4 SISTEMA DE ADMINISTRACIÓN DEL RIESGO CREDITICIO (SARC)**

#### **4.1 MARCO CONCEPTUAL Y NORMATIVO**

##### **4.1.1 Definición riesgo de crédito (RC)**

El RC es la posibilidad de que una entidad incurra en pérdidas y se disminuya el valor de sus activos, como consecuencia de que un deudor incumpla sus obligaciones.

##### **4.1.2 Sistema de Administración del Riesgo Crediticio - SARC**

Siguiendo los lineamientos contenidos en el numeral 2.5.3 del Capítulo II de la Circular Básica Contable y Financiera de la Superintendencia Financiera de Colombia, las aseguradoras y las sociedades de capitalización deben mantener una adecuada administración del RC mediante la adopción de un SARC que contenga los elementos definidos en dicho capítulo, salvo la adopción de la metodología para el cálculo de las pérdidas esperadas.

El presente capítulo del Manual para la Gestión de Riesgos del Negocio contiene los elementos necesarios para conocer los criterios y la forma mediante la cual Positiva evalúa, asume, controla y cubre el RC.

#### **4.2 ALCANCE DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO CREDITICIO**

Conforme a lo establecido en el numeral 2.5.3 del Capítulo II de la Circular Básica Contable y Financiera de la Superintendencia Financiera de Colombia, el SARC de una Aseguradora se debe desarrollar únicamente sobre operaciones que generan RC, que a su vez, originan partidas contables correspondientes a cartera de créditos (exceptuando los préstamos sobre títulos de capitalización y sobre pólizas de seguros), cuentas por cobrar correspondientes a remuneración de intermediación y créditos a empleados y agentes

Dentro de los términos señalados en el Capítulo II de la Circular Básica Contable y Financiera, y considerando las actividades y estrategias diseñadas para el desarrollo del objeto social, en Positiva solo se asume RC en los créditos otorgados a los Trabajadores Oficiales, a través de operaciones de mutuo que se originan en los acuerdos firmados, entre la Compañía y dichos Trabajadores, en virtud del Pacto Colectivo vigente.

#### **4.3 POLÍTICAS PARTICULARES AL SARC**

Con el fin de realizar una adecuada gestión del riesgo de crédito descrito, Positiva Compañía de Seguros S.A. ha adoptado las siguientes políticas:

- Los empleados sujetos de crédito serán aquellos que ostenten la calidad de Trabajadores Oficiales.

- Las condiciones para el otorgamiento de los créditos están contenidas en el Pacto Colectivo y el reglamento de crédito vigentes.
- La Gerencia de Talento Humano es el área responsable de evaluar la capacidad de pago de los Trabajadores Oficiales que soliciten crédito; y en general de que se cumplan las condiciones necesarias para el otorgamiento de un crédito.
- La Gerencia de Talento Humano es la encargada de las condonaciones a los créditos educativos.
- La Gerencia de Talento Humano es la encargada del seguimiento y recaudo de la cartera.
- La Oficina de Gestión Integral de Riesgos es la responsable de realizar el seguimiento a los riesgos y controles involucrados en los respectivos procesos, con el fin de mitigar la probabilidad e impacto de las situaciones que se puedan presentar, las cuales disminuyan el valor de los activos de Positiva.

#### **4.4 ESTRUCTURA ORGANIZACIONAL PARTICULAR AL SARC**

En el numeral 1.9 del presente Manual se encuentran descritas las funciones y responsabilidades que tienen la Junta Directiva, La Presidencia, La Oficina de Gestión Integral de Riesgos, Los Órganos de Control y en general todos los colaboradores de Positiva Compañía de Seguros S.A., a la luz de la Gestión de riesgos.

La Gerencia de Talento Humano tendrá las siguientes responsabilidades a la luz del Sistema de Administración de Riesgo de Crédito:

- Analizar las solicitudes de créditos educativos.
- Evaluar la capacidad de pago del trabajador.
- Mantener un registro actualizado del comportamiento histórico de los créditos.
- Realizar la liquidación de los créditos educativos de los Trabajadores Oficiales.
- Estudiar y evaluar el cumplimiento de requisitos necesarios para la condonación de créditos educativos; de acuerdo a las condiciones previstas en el Pacto Colectivo y el Reglamento de Crédito vigentes.
- Presentar un informe semestral a la Presidencia acerca del comportamiento de los créditos a Trabajadores Oficiales.
- Asegurar el cumplimiento de los límites de riesgo establecidos en el Pacto Colectivo y el Reglamento de Crédito vigentes.

#### **4.5 ETAPAS DE LA ADMINISTRACION DE RIESGO CREDITICIO**

Para la adecuada gestión del riesgo de crédito se identifican tres grandes etapas:

Otorgamiento: Esta etapa consiste en la presentación, estudio, aprobación y desembolso de una solicitud de crédito presentada por un Trabajador Oficial.

Seguimiento y control: Esta etapa corresponde al seguimiento periódico que realiza la Gerencia de Talento Humano sobre los créditos desembolsados. De igual manera, incluye las actividades desarrolladas para controlar el cumplimiento de los límites máximos e individuales previstos en el Pacto Colectivo y el Reglamento de Crédito vigentes.

Recaudo y recuperación: Esta etapa incluye las actividades que desarrolla la Gerencia de Talento Humano para el recaudo a través del descuento por nómina de las cuotas

acordadas para el pago de los créditos desembolsados, así como el monitoreo de los requisitos necesarios para la condonación de la deuda.

La Gerencia de Talento Humano garantiza que dentro del Sistema Integral de Gestión se encuentre la documentación detallada y necesaria para cada una de las etapas aquí mencionadas.

#### **4.5.1 Otorgamiento de crédito**

En esta etapa, la Gerencia de Talento Humano realiza una evaluación de la capacidad de pago de los trabajadores, de acuerdo a lo establecido en el Artículo 59 del código sustantivo del trabajo y en el artículo 3 de la ley 1527 del 27 de abril de 2012, normas según las cuales el descuento de nómina mensual que se haga al trabajador, una vez aprobado el crédito, no debe superar el 50% del neto del salario, después de los descuentos de ley.

En los casos en que se evidencie que el trabajador no cuenta con la capacidad de pago necesaria para acceder al monto de crédito solicitado, la Gerencia de Talento Humano podrá aprobar un monto inferior, acorde a la capacidad de pago del empleado.

Una vez evaluada la capacidad de pago del trabajador, la Gerencia de Talento Humano verifica que se cumplan las políticas y requisitos mencionados en el Pacto Colectivo; así como, el cumplimiento del reglamento de crédito.

#### **4.5.2 Criterios de validación de la capacidad de endeudamiento de los servidores de Positiva Compañía de Seguros en caso de Libranza o descuentos directos**

Positiva Compañía de Seguros en su calidad de empleador podrá, realizar descuentos directos a sus servidores con el fin de posibilitar la adquisición de productos y servicios financieros o bienes y servicios de cualquier naturaleza, acreditados con el salario, siempre que medie autorización expresa de descuento otorgada por el servidor o funcionario.

Ahora bien, la posibilidad de este servicio estará sujeto a la capacidad de endeudamiento del solicitante.

En efecto, los artículos 149 y siguientes del Código Sustantivo del Trabajo, y la Ley 1527 de 2012 modificada por la Ley 1902 de 2018; por medio de la cual se establece un marco general para la libranza o descuento directo que dispone:

*“CONDICIONES DEL CRÉDITO A TRAVÉS DE LIBRANZA O DESCUENTO DIRECTO. Para poder acceder a cualquier tipo de producto, bien o servicio a través de la modalidad de libranza o descuento directo se deben cumplir las siguientes condiciones:*

*...*

*5. Que la libranza o descuento directo se efectúe, siempre y cuando el asalarado o pensionado no reciba menos del cincuenta por ciento (50%) del neto de su salario o pensión, después de los descuentos de ley. Las deducciones o retenciones que realice el*

*empleador o entidad pagadora, que tengan por objeto operaciones de libranza o descuento directo, quedarán exceptuadas de la restricción contemplada en el numeral segundo del artículo 149 del Código Sustantivo del Trabajo.” (subrayado fuera del texto)*

Ahora bien, con el fin de dar cumplimiento a lo anterior, Positiva garantizará que sus trabajadores no perciban menos del 50% del neto de su salario, de conformidad con el procedimiento que se describe a continuación:

Para estos efectos, el 50% del neto se tomará luego de realizar los descuentos de ley como aporte a salud, pensión, fondo de solidaridad pensional, retención en la fuente, así como los descuentos por orden judicial.

Dentro del cálculo a tener en cuenta para cumplir con el límite legal de descuentos por libranza o descuentos directos, se tomarán los realizados a la fecha de la solicitud por concepto de créditos de libranzas, descuentos por créditos con el Fondo de Empleados, descuentos por seguros, descuentos por los diversos planes complementarios en salud y servicios en salud, así como cualquier otro que haya sido autorizado por el trabajador; lo anterior significa que la suma de todos los descuentos autorizados por el trabajador no podrán en ningún caso exceder el 50% del neto que percibe.

Dentro de los criterios de validación de capacidad de endeudamiento se excluyen los realizados por concepto de ahorros al fondo de empleados, ahorros en cuentas AFC y cualquier otro ahorro que el trabajador realice a través de la nómina; no obstante en caso que la libranza o descuento directo solicitado por el trabajador supere el 50% del neto que perciba en los términos de las normas citadas, deberá autorizar a la compañía reducir o eliminar el descuento que por ahorro venga realizando.

La formulación del cálculo de la capacidad de endeudamiento se encuentra parametrizada en formato Excel diseñado por la Gerencia de Talento Humano de acuerdo con los criterios definidos archivo controlado por esta dependencia.

Finalmente, y en el evento de presentarse embargos a las cuentas de los funcionarios de nuestra compañía, se deberá dar aplicación a lo dispuesto en los artículos 2495 y Sigüientes del Código Civil y artículo 134 del Decreto 2737 de 1989 (Código del Menor) en cuanto a la prelación de créditos.

Los lineamientos anteriormente descritos serán aplicados por la Gerencia de Talento Humano y se encuentran contenidos en el Manual de Gestión Humano, publicado en la herramienta SIMPLE en el Macroproceso de Gestión, lo anterior teniendo en cuenta que estos descuentos se hacen en caso de Libranza o descuentos directos .

### **4.5.3 Seguimiento y control del riesgo de crédito**

#### **4.5.3.1 Límites de exposición crediticia para créditos educativos**

Los límites de exposición crediticia están determinados en el Pacto Colectivo y en el reglamento de crédito vigentes.

#### **4.5.3.2 Garantías para créditos educativos**

La garantía de los créditos educativos está conformada por las prestaciones sociales del trabajador producto de su contrato laboral con Positiva Compañía de Seguros S.A.

#### **4.5.4 Recaudo y recuperación de los créditos**

##### **4.5.4.1 Recaudo de la cartera**

El recaudo de las cuotas periódicas de la cartera de crédito educativo para Trabajadores Oficiales de Positiva Compañía de Seguros S.A. se realiza mediante el descuento directo de nómina.

Si por algún motivo excepcional, la cuota mensual no se puede descontar en un 100% a través del descuento de nómina, la Gerencia de Talento Humano debe solicitar al trabajador que el pago faltante sea realizado en efectivo a través de consignación en la cuenta corriente y/o de ahorros que la Gerencia de Talento humano indique.

##### **4.5.4.2 Recalificación de cartera y constitución de provisión**

Positiva Compañía de Seguros S.A. otorga créditos educativos a los trabajadores oficiales vinculados a la compañía y descuenta directamente de nómina las cuotas pactadas, por lo anterior no hay lugar a cartera pendiente y los créditos concedidos tienen una calificación crediticia A, no obstante si por algún motivo excepcional, la cuota mensual no se puede descontar en un 100% o el trabajador se desvincula de la compañía y su liquidación no es suficiente para subsanar la deuda, se constituirá un acuerdo de pago entre las partes, el cual hará parte integral de la documentación en el contrato de mutuo, si se llegase a presentar incumplimiento de dicho acuerdo generando mora en la cartera se procederá a realizar la recalificación crediticia y se actuará según lo consignado en el anexo I del capítulo II de la Circula Básica Contable de la Superintendencia Financiera. *(Véase Anexo I del presente Manual)*

##### **4.5.4.3 Condonación de créditos educativos**

Positiva Compañía de Seguros S.A. condonará el valor de los préstamos de acuerdo con las condiciones establecidas en el Pacto Colectivo y el Reglamento de Crédito vigentes. El Trabajador Oficial debe presentar a la Gerencia de Talento Humano la solicitud formal de la condonación del crédito junto con la certificación original del promedio de notas obtenido en el semestre cursado.

#### **4.6 MONITOREO DE LA GESTIÓN DE RIESGO DE CRÉDITO.**

La Oficina de Gestión Integral de Riesgos verifica, de acuerdo a las condiciones del Pacto Colectivo vigente, que los valores de los créditos aprobados estén en función de la capacidad de pago del Trabajador Oficial.

Adicionalmente verificará el cumplimiento de las condiciones requeridas para la condonación de créditos educativos.

## 5. ANEXOS

### 5.1. ANEXO I

Si bien el Capítulo II de la Circular Externa 100 de 1995 ordena a las entidades aseguradoras la implementación de un SARC, dicha norma establece unas reglas especiales para ello, particularmente en lo aplicable a la metodología de cálculo de la pérdida esperada. Así, el subnumeral 2.5.3.2 de la norma señalada refiere que “Toda vez que las entidades a las que se refiere el presente numeral no están obligadas a adoptar metodologías para el cálculo de pérdidas esperadas, las provisiones individuales se realizarán de acuerdo con lo previsto en el Anexo 1 del presente capítulo”, el cual establece la siguiente tabla de provisiones a partir de la calificación de crédito:

CALIFICACIÓN DE CREDITO	PORCENTAJE MÍNIMO DE PROVISIÓN
A	0%
B	1%
C	20%
D	50%
E	100%

Si la totalidad de la cartera crediticia de la Compañía se encuentra calificada como A, la provisión individual corresponde al 0%.

En relación con la provisión general, la cual corresponde como mínimo al 1% sobre el total de la cartera de créditos bruta, la Circular Básica Contable y Financiera (Circular Externa 100 de 1995) establece reglas especiales para su establecimiento, razón por la cual no resulta aplicable para todos los casos. En general, la provisión general es obligatoria para (i) Entidades o portafolios cuyo modelo interno no incorpore componentes contracíclicos; (ii) Entidades o portafolios para los que no se empleen ni los modelos internos que incorporen componentes contracíclicos y hayan obtenido un pronunciamiento de no objeción por parte de la SFC, ni los de referencia adoptados por la SFC; (iii) Las entidades descritas en el numeral 1 del Anexo 6 que no incorporen componentes contracíclicos en su metodología de estimación de provisiones. Ya que la Compañía no cumple ninguna de las condiciones anteriormente señaladas, es necesario remitirnos nuevamente al numeral 2.5.3 de la Circular, el cual describe la provisión general para las entidades aseguradoras de la siguiente forma:

“La provisión general de las entidades aseguradoras y las sociedades de capitalización debe corresponder como mínimo al uno por ciento (1%) sobre el total de la cartera de créditos bruta registrada en la cuenta PUC 14, con excepción de los créditos garantizados con pólizas de vida y los créditos garantizados con títulos de capitalización.”

En el PUC, que corresponde al 2013, la cuenta 14 “registra las diferentes clases de créditos otorgados por la Entidad bajo las distintas modalidades autorizadas, en desarrollo

del giro especializado de cada una de ellas.” Con la entrada en vigencia de las Niif, dicho PUC fue modificado y ahora corresponde a la cuenta 1406 “cartera de créditos - actividad aseguradora” del Catalogo Único de Información Financiera con Fines de Supervisión.

Por ser créditos a corto plazo, Positiva clasifica sus créditos educativos como “beneficios a empleados a corto plazo”, los cuales corresponden a una cuenta distinta a la señalada por la normatividad, siendo aplicable la NIC 19. Bajo dicha norma, la contabilización de los beneficios a corto plazo a los empleados es generalmente inmediata, y por tanto no existe posibilidad alguna de ganancias o pérdidas, y como consecuencia, no hay lugar a la provisión de la cartera. No obstante, lo anterior, las provisiones individuales derivadas de la calificación del cliente sí resultan aplicables. Para el caso de la Compañía, y dado que la totalidad de la cartera está calificada en A, la provisión corresponde al 0%.

## 5.2. ANEXO II

### Metodología Eficacia de Controles

#### Política

Los controles a evaluar de cada proceso será una muestra aleatoria con un mínimo a evaluar según la siguiente tabla.

Rango	Intervalo	Controles a Evaluar
1	1-19 controles	4
2	20-39 controles	8
3	40-59 controles	12
4	60-79 controles	16
5	80 o más controles	20

1. Los controles vinculados a riesgos materializados tendrán prioridad a la hora de elegir la muestra que será objeto de evaluación.
2. Los procesos que tengan un número de controles a evaluar, igual o inferior a 4, deberán ser evaluados al 100% de sus controles.
3. Los resultados obtenidos por la metodología son un insumo al momento de realizar la revisión anual de riesgos y controles, la eficacia del control en la herramienta ERA se verán reflejada hasta la actualización anual de Riesgos y Controles.

#### Criterios definidos para dar respuesta a la primera pregunta

##### PRIMERA PREGUNTA

¿El diseño del control mitiga el riesgo?

Atributos	%	
Clase	13.33%	<b>80%</b>
Tipo	13.33%	
Documentado	13.33%	
Responsable	13.33%	
Cobertura	13.33%	
Frecuencia	13.33%	
Preguntas	%	
¿El procedimiento del control se realiza según lo descrito?	20.00%	<b>20%</b>

Política: Para dar como respuesta SI a la pregunta el total debe ser igual o superior al 70%

### Criterios definidos para dar respuesta a la segunda pregunta

#### SEGUNDA PREGUNTA

**¿Conforme a la muestra seleccionada o auditada el control se considera eficaz?**

Preguntas	%	
¿Considera que el control tiene una eficacia Alta, Moderada o Baja?	Alta	<b>50%</b>
	Moderada	<b>25%</b>
	Baja	<b>0%</b>
¿En control tiene vinculados riesgos que presentaron eventos en el último año?	NO	<b>50%</b>

Política: Para dar como respuesta SI a la pregunta el total debe ser igual o superior al 75%

Macro-proceso: Gestión de Riesgos

Proceso: Gestión de Riesgos de Negocio

Subproceso: Gestión de Riesgo Operativo  
Gestión de Riesgo de Crédito

### Responsable

Para despejar cualquier inquietud sobre el contenido del presente documento, por favor comuníquese con el Jefe de la Oficina de Gestión Integral de Riesgos.

<b>Documentos y/o Formatos Asociados</b>		
<b>N°</b>	<b>Nombre del Documento y/o Formato asociado</b>	<b>Código del Documento sin versión</b>
1	Plantilla RER	EST-3-1-1-FR02
2	Guía Diligenciamiento de la Plantilla de Eventos de Riesgo Operativo	EST-3-1-GU01
3	Formato Riesgo y Controles	EST-3-1-1-RF03
4	Formato Plantilla Consolidada de Eventos de Riesgo	EST-3-1-1-RF04

<b>Control de Cambios</b>				
<b>N°</b>	<b>Descripción del Cambio</b>	<b>Fecha del Cambio</b>	<b>Quien Aprueba el Cambio</b>	<b>Versión Anterior</b>
1	Exclusión del capítulo SARM, por el proceso de reestructuración de Positiva, en el cual se involucra la creación de la Vicepresidencia de Inversiones.	15/11/2013	Junta Directiva	10
2	<p>El Manual para la Gestión de Riesgos del Negocio sustituye el anterior Manual para la Gestión Integral de Riesgo.</p> <p>A los capítulos I, II, III, IV y VI se les realiza ajustes de forma, actualizándolos a la estructura organizacional vigente.</p> <p>Modificación del Capítulo V SARC, re-definición del riesgo de crédito, ajustándolo a los requerimientos del Capítulo II de la Circular Básica Contable. Se limitó a crédito a trabajadores oficiales.</p> <p>Modificación del Capítulo I; se adiciona al numeral 1.6.1 ajustando la política de prevención y solución de conflictos de interés.</p>	30/04/2014	Junta Directiva	11
3	Modificación del Capítulo VI: "ESQUEMA DE PREVENCIÓN DE FRAUDE Y CORRUPCIÓN", incluyendo la creación del Comité de Ética.	28/05/2014	Junta Directiva	12
4	<p>Modificación del Capítulo I: "CONSIDERACIONES GENERALES PARA LA GESTIÓN DE RIESGOS DEL NEGOCIO. Se incluye: Alcance, Nivel de riesgo aceptable, consolidación de funciones, modificación del Comité de Riesgos</p> <p>Modificación del Capítulo III: "SISTEMA DE ADMINISTRACION DE RIESGO OPERATIVO SARO. Se incluye: modificación de metodología de valoración de impacto, ajuste de colorimetría de la matriz de riesgos.</p>	27/06/2014	Junta Directiva Acta 550	13
5	Modificación del Capítulo IV: "SARLAFT", Se incluye: modificación de metodología de segmentación.	04/12/2014	Junta Directiva Acta 557	14

6	<p>Modificación del Capítulo III: "SARO", Se modifica el numeral 3.3.3.4. Calificación de la eficacia de los controles.</p> <p>Modificación del Capítulo IV: "SARLAFT", Se modifican los numerales 4.4.2, 4.6.1.1.1, 4.7.1.1, 4.7.1.2, 4.7.1.4 y 4.7.2.</p> <p>Modificación del Capítulo VI: "ESQUEMA DE PREVENCIÓN DE FRAUDE Y CORRUPCIÓN", Se modifica el numeral 6.10.5.</p> <p>Se retira el anexo 3 "Indicadores SARO"</p>	06/11/2015 02/12/2015	Junta Directiva Actas 575 y 576	15
7	Modificación del capítulo I: "CONSIDERACIONES GENERALES PARA LA GESTIÓN DEL RIESGO DEL NEGOCIO", se modifican los numerales 1.9.4.3 y 1.9.4.6	04/02/2016	Junta Directiva Acta 579	16
8	Modificación del capítulo VI: "ESQUEMA DE PREVENCIÓN DE FRAUDE Y CORRUPCIÓN".	05/04/2016	Junta Directiva Acta 581	17
9	Modificación del capítulo V: "SISTEMA DE ADMINISTRACIÓN DEL RIESGO CREDITICIO (SARC)"	29/04/2016	Junta Directiva Acta 582	01
10	Modificación del capítulo II: "SISTEMA ESPECIAL DE ADMINISTRACIÓN DE RIESGOS EN SEGUROS SEARS"	29/07/2016	Junta Directiva Acta 587	02
11	<p>Cambios de forma por la nueva estructura organizacional de Positiva, acorde al decreto 1678 del 21 de octubre de 2016.</p> <p>Incluye ajustes conformación Comité de Riesgos de Negocio, Conformación de Comité de Ética y eliminación funciones de las antiguas Vicepresidencia de Riesgos y Gerencia de Riesgos de Negocio e inclusión de las funciones de la Oficina de Gestión Integral de Riesgos Decreto 1678 de 2016 artículo 6)</p>	06-02-2017	Junta Directiva Acta No.595	03
12	Modificación numeral 1.7, 1.7.3 y 3.3.3 por cambio en el nombre de la etapa.		Junta Directiva Acta No.601	04
	Modificación numeral 5.4, por error en la referencia del Manual de acuerdo a revisión del SARC.		-	
13	Modificación del capítulo IV "SARLAFT"	02-08-2017	Junta Directiva Acta No.603	04

14	<p>Incluir en el numeral 1.9.1 dos funciones de Junta directiva:</p> <ul style="list-style-type: none"> <li>- Exigir de la administración, para su evaluación, reportes periódicos sobre los niveles de exposición al RC, sus implicaciones y las actividades relevantes para su mitigación y/o adecuada administración.</li> <li>- Señalar las responsabilidades y atribuciones asignadas a los cargos y áreas encargadas de gestionar el RC.</li> </ul>	25-09-2017	Junta Directiva Acta No.607	05
15	<p>Incluir in el numeral 1.7 el siguiente texto: La Oficina de Gestión Integral de riesgos comenzará la ejecución de las etapas del sistema de administración del riesgo, una vez la Oficina de Estrategia y desarrollo y los dueños del proceso notifiquen que el proceso se encuentra debidamente documentado</p>	27/11/2017	Junta Directiva Acta No.610	06
16	<p>Se extrajo del manual de Riesgos del Negocio el capítulo IV Sistema de administración del riesgo de lavado de activos y financiación del terrorismo SARLAFT, como todo lo correspondiente a este sistema de administración de riesgos contenido a lo largo del Manual de Riesgos de Negocio, incluidos los anexos I y II. Modificación Capítulo III inclusión de la evaluación del equipo de la Oficina de Gestión Integral de Riesgos en la calificación de la eficacia de controles.</p>	23/02/2018	Junta Directiva Acta No.615	07
17	<p>Modificaciones al capítulo III SISTEMA DE ADMINISTRACION DE RIESGO OPERATIVO SARO numeral 3.3.3.4</p>	27/04/2018	Junta Directiva Acta No.618	08
18	<p>Modificaciones al capítulo IV 4 SISTEMA DE ADMINISTRACIÓN DEL RIESGO CREDITICIO (SARC) Inclusión numeral 4.5.3.2 Recalificación de cartera y constitución de provisión. Inclusión numeral 4.5.1.1 Criterios de validación de la capacidad de endeudamiento de los servidores de Positiva Compañía de Seguros en caso de Libranza o descuentos directos. Inclusión Anexo I</p>	30/10/2018	Junta Directiva Acta No.626	09

19	<p>Modificación del Capítulo I: “ESTRUCTURA ORGANIZACIONAL – FUNCIONES Y RESPONSABILIDADES. Se incluye: Funciones del Presidente y Secretario del Comité de Riesgos, así como funciones de la OGIR y del mismo Comité de Riesgos.</p> <p>Modificación del Capítulo III: “SISTEMA DE ADMINISTRACION DE RIESGO OPERATIVO SARO. Se incluye: definición de riesgos inembargables, así como las medidas y controles para las órdenes de embargo.</p> <p>Se incluye modificación a la revisión periódica para la identificación de riesgos, de calificación de controles, de la autoevaluación de controles, de la eficacia de controles (Prueba de Recorrido).</p> <p>Se incluye las responsabilidades de la identificación de riesgos en caso de fusiones, adquisiciones, etc.</p> <p>Se incluye los criterios para determinar si un control se considera eficaz, así mismo se relaciona el documento donde se identifican los procesos críticos.</p> <p>La clasificación de eventos se incorpora al numeral de Registro de Eventos de Riesgos.</p>	27/03/2019	Junta Directiva Acta No.632	10
20	<p>Se modifica el Capitulo I. “ESTRUCTURA ORGANIZACIONAL – FUNCIONES Y RESPONSABILIDADES. Se excluye la siguiente función de la Junta Directiva que corresponde SARLAFT: Establecer y hacer seguimiento a las metodologías para la realización de entrevistas no presenciales y/o la realización de entrevistas por personal que no tenga la condición de empleado de la entidad.</p> <p>Se excluye la siguiente función del Presidente ya que la hace la Oficina de Gestión Integral de Riesgos: Presentar y someter a aprobación de la Junta Directiva el Manual para la Gestión de riesgos del negocio, así como sus actualizaciones.</p> <p>Se modifica la fecha límite para el reporte de eventos de riesgo por parte de las áreas.</p> <p>Se ingresa al Capítulo III. MEDIDAS ANTE EL INCUMPLIMIENTO DEL SARO.</p> <p>Se retira el Capitulo V. ESQUEMA DE PREVENCIÓN DE FRAUDE Y CORRUPCIÓN al Manual para la Gestión de Riesgos del Negocio.</p>	15/05/2019	Junta Directiva Acta No. 635	11

21	<p>Se incluyen responsabilidades dentro del numeral 1.9.5 Oficina de Gestión Integral de Riesgos.</p> <p>Se incluye en el numeral 3.3.8 Monitoreo y revisión que la metodología para gestionar los indicadores del Sistema de Administración de Riesgo Operativo se encuentra alineada a las directrices definidas en el instructivo de Construcción de Indicadores que define la Oficina de Estrategia y Desarrollo.</p> <p>Se da claridad en el numeral 3.4.2 Tipo de pérdida de los eventos riesgo operativo que el reporte de eventos de riesgo puede ser informado por un delegado.</p> <p>En el numeral 1.7.6 Monitoreo y Revisión se incluye el esquema de asignación y responsabilidades de cada una de las líneas de defensa.</p> <p>Creación del ANEXO II - Metodología para la medición a la eficacia de controles.</p> <p>Se incluyen en el numeral 3.4.1 Clase o clasificación de los eventos riesgo operativo los criterios para calificar el impacto: alto, moderado o leve de los eventos de riesgo. Y se referencia en el numeral 3.3.4.8 Calificación de la eficacia de los controles la definición de la escala de impacto de un evento de riesgo.</p> <p>Se incluye en el numeral 2.3.8 Riesgo de insuficiencia de reservas que la Gerencia de Actuaría y el Actuario Responsable ejecutan en sus procesos los controles respectivos que aseguran el cálculo de la reserva.</p>	09/01/2020	Junta Directiva Acta No. 648	12
----	---	------------	------------------------------	----