

GESTIÓN INTEGRAL DE RIESGOS

ASSA Compañía de Seguros S.A. y ASSA Vida, S.A., Seguro de Personas. Consientes que el desarrollo comercial de sus actividades se encuentra naturalmente expuesta a situaciones eventuales que de materializarse pueden comprometer, impedir o entorpecer el logro de sus objetivos. Por tal motivo nuestra Junta Directiva mantiene un alto compromiso con la Gestión Integral de Riesgos en la operación y cuenta con metodologías, políticas y procedimientos enfocados a la mitigación de los riesgos. La Junta Directiva, como ente superior de Dirección, comparte la responsabilidad con todos los empleados de la Gestión de los Riesgos ejerciendo una permanente labor de dirección en el proceso de Gestión Integral de Riesgos.

Estructura organizativa para la Gestión Integral de Riesgos

En cumplimiento del compromiso antes mencionado, el Comité de Riesgos que asiste a la Junta Directiva en el seguimiento y evaluación de las Metodologías, Políticas y Procedimientos de la Gestión Integral de Riesgos implementados por la Aseguradora, desarrolló una función de monitoreo y comunicación de los distintos niveles de exposición de la misma, a los riesgos inherentes a su actividad, sesionando de forma trimestral y reportando a la Junta Directiva el resultado de la gestión de la Unidad de Riesgos.

El Comité de Riesgos tiene una estructura, conformada por dos funcionarios designados por la Junta Directiva para la Gestión Integral de Riesgos, el Gerente General de la Aseguradora, el vicepresidente de Negocios Internacionales, el vicepresidente de Riesgos, dos miembros de Junta Directiva, uno de los cuales ostenta el cargo de director Externo, y es quien preside el Comité.

Además, la compañía cuenta con la Unidad de Riesgos, encargada de la administración del modelo de Gestión Integral de Riesgos, que incluye la matriz de riesgos de la aseguradora, de la cual es responsable. Su principal función es la de garantizar, por parte de todos los empleados involucrados en la gestión de riesgos y de la compañía en general, un nivel adecuado de comprensión de los estándares mínimos y de la implementación de las mejores prácticas, durante el periodo reportado se impartió una capacitación a todos los empleados sobre el modelo de gestión de riesgos que desarrolla la compañía, haciendo énfasis en la importancia del involucramiento de todos los empleados en la mitigación de los riesgos.

La Unidad de Riesgos, liderada por una Coordinación y un Oficial de Riesgos, tienen la responsabilidad primordial de dirigir este ámbito. No obstante, la gestión efectiva de riesgos constituye un compromiso que involucra a toda la compañía.

Riesgos asumidos por las actividades de las Aseguradoras.

Riesgo de Crédito: Es la posibilidad de incurrir en pérdidas, debido al incumplimiento de las obligaciones contractuales asumidas por una contraparte.

Al gestionar este riesgo se pretende controlar las pérdidas sufridas como consecuencias de impagos por parte de los deudores de la entidad, así como de activos que ésta posea y que den derecho a la percepción de flujos económicos. Por ende, la evaluación del riesgo de crédito se extiende a los contratos de seguros: primas por cobrar, coaseguros por cobrar, otras cuentas por cobrar, reaseguros; e inversiones.

El proceso de gestión de riesgo crédito comprende las actividades para identificar, medir, gestionar y controlar las exposiciones actuales y sus probabilidades de incumplimiento, contribuyendo a:

- Detectar riesgos de incumplimientos de pago, actuales y potenciales, para tomar decisiones sobre su tratamiento; y
- Mejorar continuamente los procesos y sistemas de gestión de cobros.

Riesgo de Mercado: Es la posibilidad de pérdida, producto de movimientos en los precios de mercado que generan un deterioro de valor en las posiciones dentro y fuera del balance o en los resultados Financieros de la Aseguradora.

La gestión del riesgo de mercado se enfoca principalmente en el monitoreo de la variabilidad del valor razonable de los instrumentos financieros y sus efectos en los resultados integrales de la compañía. Se reporta a Junta Directiva y al Comité de Riesgos la exposición de la Aseguradora al Riesgo de Tasa de Interés, Liquidez del Portafolio como de Spread de Crédito. El apetito de riesgo de la Aseguradora está orientado a inversiones en títulos Valores de renta fija, reduciendo de esta manera la exposición al riesgo de fluctuación de tasas de interés.

Riesgo de Liquidez: Es la posibilidad de incurrir en pérdidas por no disponer de los recursos suficientes para cumplir con las obligaciones asumidas, incurrir en costos excesivos y no poder desarrollar el negocio en las condiciones previstas.

La gestión del riesgo de liquidez tiene como objetivo, en el corto plazo, evitar tener dificultades para atender los compromisos de pago en el tiempo y forma previstos o que, para atenderlos, la compañía requiera recurrir a la obtención de fondos en condiciones gravosas deteriorando la situación financiera y la imagen o reputación de la entidad. En el mediano plazo, tiene como objetivo velar por la idoneidad de la estructura financiera de la Compañía y su evolución, en el marco de la situación económica, de los mercados y de los cambios regulatorios.

La gestión del riesgo de liquidez también permite aprovechar adecuadamente los excesos de liquidez de La Compañía estableciendo un plan de calce entre el vencimiento de los activos y pasivos a corto y mediano plazo.

Riesgo Operacional: Es la posibilidad de incurrir en pérdidas, debido a las fallas en los procesos, personas, los sistemas de información y a causa de acontecimientos externos; incluye el riesgo legal, riesgo de fraude, riesgo tecnológico y riesgo estratégico.

Con el fin de asegurar que los riesgos operativos se miden de una manera integrada y homogénea, la Compañía realiza actividades para el levantamiento de Matrices de Riesgo Operativo. La Aseguradora cuenta con los procedimientos y controles para gestionar y mitigar los riesgos inherentes a las actividades relacionadas por medio de: Documentación de procesos, políticas, procedimientos y controles.

Se cuenta además con la Recopilación de Datos sobre Pérdidas por Riesgo Operacional, la cual permite un monitoreo de los eventos reportados por los Propietarios de Riesgos de cada área, además de crear una base histórica que permite administrar la Gestión del Riesgo Operacional en el futuro.

Riesgo Reputacional: Es la posibilidad de incurrir en pérdidas, producto del deterioro de imagen de la entidad, debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros.

El Riesgo Reputacional es Gestionado a través de un adecuada Política de Gobierno Corporativo y la implementación de Políticas que definen los lineamientos éticos y los valores de la Aseguradora, como el Código de Ética Empresarial, Política de Conflicto de Intereses y Operaciones Vinculadas, además existen controles implementados, identificados y monitoreados a través de las Matrices de Riesgo Operativo, para garantizar el cumplimiento a los requerimientos Legales y a la Prevención del Lavado de Dinero y Activos y Financiamiento al Terrorismo.

Riesgo Técnico: Es la posibilidad de pérdidas generadas por incrementos inesperados en la siniestralidad y gastos, debido a inadecuadas bases técnicas o actuariales empleadas para: establecer la tasa pura de riesgo para cada ramo de seguro, determinar la tasa comercial o primas, la evaluación y aceptación de los riesgos asegurados o políticas de suscripción, la cobertura de reaseguros y el cálculo de las reservas técnicas.

La gestión del riesgo técnico se enfoca principalmente en el monitoreo de una serie de indicadores financieros, como el índice combinado, el ratio de siniestralidad, Reservas

suficientes para pago de siniestros presentados y el indicador de Riesgo de Continuidad de Cobertura de Reaseguro, con el objetivo de evaluar la salud financiera de la compañía y la capacidad para cumplir las obligaciones con los asegurados. Midiendo la rentabilidad de la suscripción, que es esencial para que la aseguradora sea financieramente sólida y capaz de resistir posibles fluctuaciones del mercado o eventos catastróficos.

Listado de Políticas, manuales y procedimientos para la Gestión de Riesgos

Para garantizar la adecuada gestión de los riesgos, la Aseguradora cuenta con las siguientes políticas:

- Política de Gestión Integral de Riesgos.
- Política de Gestión de Riesgo de Liquidez.
- Política de Gestión de Riesgo de Mercado.
- Política de Gestión de Riesgo de Crédito.
- Política de Gestión de Riesgo de Contraparte
- Política de Gestión de Riesgo Técnico.
- Política de Gestión de Riesgo de Descalce.
- Política de Gestión de Riesgo Operativo.
- Política de Gestión de Riesgo Reputacional.
- Política de Gestión de Riesgo Legal.
- Plan de Continuidad de Negocios.
- Manual Operativo para la Identificación y Evaluación de Riesgos Operativos.
- Manual Operativo para la Gestión de Eventos de Pérdida de Riesgo Operativo.

Metodologías, sistemas y herramientas de Administración de Riesgos

Se cuenta con las siguientes metodologías para la evaluación de Riesgos:

- **Metodología para la Gestión de Riesgo de Liquidez:** Busca establecer un conjunto de procedimientos y actividades clave para una evaluación cualitativa y efectiva del riesgo de liquidez.

Su objetivo principal es garantizar que la compañía mantenga la liquidez suficiente para hacer frente a sus obligaciones financieras en todo momento, minimizando el riesgo de pérdidas o problemas de solvencia.

- **Metodología para la Gestión de Riesgo de Contraparte:** Analiza la concentración de reaseguradores para la Compañía examinando la distribución y dependencia de la aseguradora respecto a un número limitado de reaseguradoras.

Evalúa cuánto del riesgo asumido por la Compañía está respaldado por un grupo reducido de reaseguradoras y evitar una vulnerabilidad de la Compañía a la insolvencia o a problemas financieros si una o varias de esas reaseguradoras enfrentan dificultades.

- **Metodología para la Gestión de Riesgo Técnico:** Esto determina la capacidad de la Compañía para cumplir con sus obligaciones contractuales, asegurando que las reservas y los activos líquidos sean suficientes y adecuados para cubrir los pagos futuros requeridos.

Su objetivo principal es asegurar que la compañía cuente con las reservas financieras adecuadas y tome decisiones informadas en cuanto a la fijación de precios, la suscripción de riesgos y la gestión de siniestros, minimizando así la probabilidad de pérdidas inesperadas o insuficiencia de recursos para hacer frente a los compromisos contractuales.

- **Metodología para la Evaluación de Riesgo Operativo:** El proceso de medición de riesgos operativos forma parte del marco de Gestión de Riesgo, y tiene como propósito:
 - Establecer la probabilidad de ocurrencia del riesgo y su posible impacto dentro de la organización;
 - Evaluar el diseño de los controles para determinar qué tan acertada es la planeación y definición conceptual de los aspectos relevantes de dicho control.

El objetivo de esta metodología es establecer los procedimientos fundamentales y actividades mínimas requeridas para la evaluación cualitativa del riesgo operativo, incluyendo la evaluación del diseño de los controles, cuyos resultados serán consolidados utilizando las herramientas de Matriz de Riesgo e Inventario de Controles.

- **Metodología para la Valoración de Pérdidas en Eventos de Riesgo Operativo:** La Recopilación de Datos de Pérdidas es el proceso utilizado para recabar la información sobre las pérdidas experimentadas debido a fallas operativas, cuyo principal objetivo es proporcionar datos homogéneos y fiables para mejorar de manera continua las autoevaluaciones de riesgos operativos.

La presente metodología establece los procedimientos, roles, responsabilidades, y actividades mínimas requeridas para identificar, recopilar, validar, y reportar pérdidas sufridas como resultado de la ocurrencia de fallas operativas.

- **Metodología para Evaluación de Riesgos Tecnológicos:** Este documento describe la metodología que la aseguradora utiliza para llevar a cabo las actividades de medición de riesgos tecnológicos y evaluación de los controles, teniendo como referencia las mejores prácticas y marcos de referencia internacionales.

Tiene como objetivo, establecer los procedimientos fundamentales y actividades mínimas requeridas para la medición de los riesgos tecnológicos, utilizando la herramienta de Matriz de Riesgo de TI.

- **Metodología para el Análisis de Impacto al Negocio:** Está dirigida a identificar los procesos de negocios de ASSA que, ante una interrupción imprevista por alguna falla o siniestro, impactarían de manera crítica la continuidad de la operación y la garantía de prestación de servicios a los clientes y demás partes interesadas. Este estudio permite estimar el nivel de impacto y criticidad de los procesos a la continuidad de la operación tanto en aspectos cualitativos (imagen, clientes, relación y cumplimiento de compromisos con otras partes interesadas), como cuantitativos (Pérdida en ventas, incremento en gastos operativos).

Sistema de Gestión de Seguridad de la Información

1. Estrategias y principales políticas utilizadas para la gestión de la seguridad de información y de la ciberseguridad

- **Estrategias**

- Incorporar tecnologías de gestión y control de identidades con privilegios altos.
- Mejorar la detección y monitoreo en la red.
- Robustecer la gestión de parches e inventariado de equipos.
- Evaluar y alinear las iniciativas del negocio bajo los lineamientos de seguridad y el proceso de desarrollo seguro.
- Mejorar el proceso de gestión de vulnerabilidades dirigidas al negocio.

- **Política**

- Política de Seguridad de la Información

2. Principales requisitos logrados del SGSI (Sistema de Gestión de Seguridad de la Información)

- Gestión y control de identidades con privilegios altos:
 - Implementación de Gestión de Acceso Privilegiado (PAM)
 - Se gestiona el rol privilegiado (administrador) desde la consola de PAM.
 - El alcance inicial abarca todos los servidores Windows.
 - Permite tener logs de las sesiones realizadas por usuario y por equipo.

- **Detección y monitoreo de red:**
 - Implementación de herramienta para la detección y respuesta en la red (NDR).
 - Etiquetado de equipos y segmentos de red.
 - Activación de módulos de detección y respuesta automática sobre comportamientos anómalos en la red.

- **Gestión de parches e inventariado de equipos:**
 - Mejora del proceso de parchado equipos y aplicaciones.
 - Mejora en tiempos de respuesta para la aplicación de parches críticos reportados.

- **Alineamiento de las iniciativas del negocio bajo lineamientos de seguridad y desarrollo seguro:**
 - Definición de los controles de seguridad desde la concepción de la iniciativa.
 - Diseño de diagramas de arquitectura y de flujos de las iniciativas presentadas.
 - Flujo de desarrollo seguro para iniciativas transaccionales o con cambios funcionales.

- **Gestión de Vulnerabilidades:**
 - Priorización de vulnerabilidades y seguimiento a través del comité de vulnerabilidades.
 - Acción temprana de parchado y remediación de vulnerabilidades reportadas por los fabricantes (boletines de seguridad).
 - Pruebas de re-test para vulnerabilidades reportadas en el Ethical Hacking

3. Programa de seguridad de la información

El Programa de Seguridad de la Información contiene los siguientes puntos:

- Cronograma mensual con campañas de concientización a colaboradores sobre temas de Ciberseguridad
- Cronograma trimestral de pruebas de phishing
- Pruebas de penetración y Ethical Hacking (anuales y a demanda)
- Creación de lineamientos de seguridad
- Evaluación mensual de Métricas siguientes:
 - Parchados de equipos
 - Equipos Protegidos Antivirus (Crowdstrike)
 - Capacitaciones de Ciberseguridad
 - Seguimiento de Cierre de Vulnerabilidades
 - Pruebas de Pishing
 - Evaluación de iniciativas del negocio