INFORME GESTIÓN DE RIESGOS 2023

INTRODUCCIÓN

La gestión efectiva de riesgos emerge como un componente crucial para asegurar la estabilidad financiera de las organizaciones, la integridad operativa y la sostenibilidad a largo plazo; dicha efectividad propone analizar y examinar a fondo las estrategias y prácticas implementadas en el ámbito de gestión de riesgos. De acuerdo con la naturaleza de nuestra actividad en la intermediación de seguros en las diferentes regiones del país, se miden aspectos clave como la identificación, evaluación de riesgos, la implementación de políticas y procedimientos, apetito de riesgo, así como la integración de tecnologías emergentes en la gestión de riesgos y ejecución de planes de acción frente a materialización de eventos.

En **ARESS CORREDORES DE SEGUROS S.A.,** se vela por el mejoramiento continuo en evaluación y gestión de riesgos, tanto estratégicos, financieros, reputacionales, de cumplimiento y operativos. Así mismo fortalecer nuestra cultura de riesgo y garantizar el cumplimiento de las responsabilidades desde los Accionistas, Junta Directiva y la Gerencia hasta cada uno de los niveles de la organización.

ANÁLISIS DEL CONTEXTO

Con el fin de obtener una comprensión más completa de los riesgos y oportunidades que la compañía enfrenta, así como para adaptarse proactivamente a un entorno empresarial en constante cambio, se realiza un análisis exhaustivo del contexto interno y externo. Este análisis se considera esencial para una gestión de riesgos efectiva y una toma de decisiones estratégica.

Contexto Externo

El mercado de seguros está marcado por una serie de desafíos y oportunidades que requiere una gestión diligente de los riesgos asociados. Las empresas del sector asegurador se enfrentan al desafío de equilibrar la necesidad de innovación y crecimiento, con la gestión eficaz de los riesgos.

La capacidad de las compañías para brindar herramientas efectivas para la gestión, análisis y mitigación de riesgos organizacionales se vuelve crucial en este contexto. Esto incluye la adopción de tecnologías avanzadas, la implementación de prácticas de gestión de

riesgos sólidas y el fortalecimiento de la cultura de riesgo dentro de la organización.

Además, es esencial evaluar el entorno macroeconómico y político del país. La incertidumbre y los posibles cambios gubernamentales o normativos pueden impactar significativamente en el sector asegurador y en la forma en que las compañías operan y se adaptan a nuevas condiciones.

En Aress Corredores de Seguros nos esforzamos por estar preparados para afrontar un entorno externo dinámico y desafiante, donde consideramos que la gestión efectiva de riesgos y nuestra capacidad de adaptación son pilares fundamentales para garantizar el éxito sostenible de nuestra compañía a largo plazo.

Contexto Interno

Se destaca la evaluación integral del contexto interno de la compañía. Esto implica analizar la estructura organizacional, los objetivos estratégicos, los procesos y actividades empresariales, así como los factores organizacionales como el diseño de la organización, las tecnologías de la información y la cultura empresarial. Además, se enfatiza en mantener relaciones sólidas con las partes interesadas internas. La cultura y los valores de la empresa también son aspectos cruciales que influyen en la gestión de riesgos, destacándose el compromiso con la responsabilidad, la transparencia y la ética en todas las operaciones.

METODOLOGÍA E IDENTIFICACIÓN DE RIESGOS

El proceso de gestión de riesgos de la compañía está basado en principios y directrices establecidos en el estándar Australiano AS/ NZS 4360, el cual es de reconocida aceptación y aplicación a nivel mundial, y las Normas Técnicas Colombianas emitidas por el ICONTEC: NTC 5254 e ISO 31000:2018.

Nuestro Enfoque:

- **Sistemático:** Se aplica a todas las actividades de la organización.
- **Proactivo:** Anticipa y previene riesgos.
- **Basado en información:** Se basa en datos y análisis para tomar decisiones.
- **Inclusivo:** Involucra a todos los niveles de la organización.
- **Personalizado:** Se adapta a las necesidades específicas de la organización.

Etapas:

1. **Comunicación y consulta:** Definir roles, responsabilidades y cómo se comunicarán los riesgos.

2. **Establecimiento del contexto:** Identificar factores internos y externos que pueden afectar a la organización.
3. **Evaluación del riesgo:** Identificar, analizar y evaluar los riesgos.
4. **Tratamiento del riesgo:** Seleccionar e implementar estrategias para abordar los riesgos.
5. **Seguimiento y revisión:** Monitorear y revisar la eficacia del sistema de gestión de riesgos.
6. **Mejora continua:** Buscar oportunidades para mejorar el sistema de gestión de riesgos.

SISTEMA DE GESTIÓN DE RIESGOS

la gestión de riesgos está en nuestra estrategia y en nuestro Gobierno Corporativo. Contamos con una Política definida por la Junta Directiva, los Comités y la Gerencia. El Sistema de Gestión de Riesgos permite identificar, medir, monitorear y gestionar los riesgos de la compañía y sus exposiciones y se diseñan e implementan según el tamaño, complejidad del negocio y procesos.

Los riesgos que analizamos los agrupamos en las siguientes categorías: estratégicos, financieros, de mercado, legales y/o regulatorios y operativos. A continuación, describimos cada uno de ellos y las subcategorías más relevantes, así como los procedimientos para evaluarlos y medir el grado de exposición que tenemos, y los mecanismos implementados por la Gerencia para su gestión, monitoreo y mitigación.

RIESGOS ESTRATÉGICOS

se refiere a la posibilidad de que la compañía no logre alcanzar sus objetivos estratégicos debido a la incertidumbre en el entorno empresarial, decisiones incorrectas de la alta dirección o cambios en las condiciones del mercado.

Para gestionar el riesgo estratégico en la compañía se han tomado medidas para identificar, evaluar y mitigar las amenazas potenciales que podrían obstaculizar el logro de los objetivos estratégicos.

RIESGOS FINANCIEROS

El desempeño de los mercados financieros y de las economías de la región, tienen efectos en la operación de los negocios y, por lo tanto, en sus resultados financieros. Esto conlleva a que cuenten con sistemas de gestión que les permitan monitorear su exposición al riesgo de crédito, mercado y liquidez, desde el manejo de las unidades de negocio contable y cartera. Este riesgo tiene 3 subcategorías:

RIESGO DE MERCADO:

Se refiere a la posibilidad de pérdidas debido a cambios en los precios de los activos financieros, tasas de interés, tipos de cambio u otros factores de mercado. Para gestionar este riesgo, la compañía diversifica su cartera de inversiones, monitorear de cerca los mercados y ajusta sus estrategias de inversión según sea necesario, informando periódicamente a la Junta Directiva.

RIESGO DE CRÉDITO:

Es la posibilidad de que una contraparte incumpla sus obligaciones financieras como las compañías de seguros y clientes, lo que podría resultar en pérdidas para la empresa. Para gestionar este riesgo, la compañía realiza evaluaciones de crédito sólidas antes de realizar transacciones con clientes o contrapartes, establece límites de exposición al riesgo de crédito, diversifica su cartera, se crean estrategias de cobranza para reducir el riesgo crediticio asociado a las mismas.

RIESGO DE LIQUIDEZ:

Se refiere a la incapacidad de la compañía para cumplir con sus obligaciones financieras debido a la falta de efectivo o activos líquidos disponibles. Para gestionar este riesgo, la compañía mantiene reservas de efectivo adecuadas, monitorear de cerca sus flujos de efectivo y mantiene líneas de crédito disponibles como medida de precaución.

RIESGOS OPERACIONALES:

Los riesgos operacionales son los posibles contratiempos o problemas que pueden surgir en el día a día de una empresa como la nuestra, que se dedica a la intermediación de seguros. Estos riesgos pueden afectar nuestra capacidad para llevar a cabo nuestras actividades de manera eficiente y efectiva como posibles errores en la administración de pólizas, problemas con nuestros sistemas informáticos, interrupciones en nuestros servicios, contar con talento humano capacitado y competente para materializar la estrategia y lograr el objetivo del proceso del cual hace parte, tener el ambiente propicio que movilice la cultura y potencie la contribución de las personas, el diseño e implementación de procesos y la tecnología que requieren para hacer realidad la propuesta de valor o incluso situaciones como fraudes y corrupción.

Es importante comprender que la compañía cuenta con un sistema de gestión de riesgo orientado a prevenir y mitigar estos riesgos, sin embargo, siempre existe la posibilidad de que ocurran.

Contamos con procesos y procedimientos establecidos para identificar, evaluar y gestionar estos riesgos de manera efectiva,

con el objetivo de proteger los intereses de nuestros clientes, proveedores, empleados y demás partes interesadas, garantizando que podamos brindarles el mejor servicio posible. Además, estamos comprometidos con la transparencia y la comunicación abierta.

FALLAS EN LOS PROCESOS:

Para evaluar el grado de exposición de este riesgo, se tiene una mirada integral desde lo estratégico y lo operativo, que se puede aplicar para procesos o áreas específicas. Su valoración parte de una medición cualitativa y otra cuantitativa. En la primera, se identifica a partir de talleres, conversaciones, entrevistas y grupos focales, la percepción del estado de cada uno de los riesgos en la Compañía y se realiza un entendimiento de cifras, gestión, operación y estrategias. La información recopilada nos permite entender la exposición al riesgo y los posibles impactos que podemos tener. Gracias a esto podemos proponer opciones de gestión para definir e implementar indicadores de riesgo/gestión para cada uno de los factores que permitan monitorear cambios en su estado, así como también los eventos de riesgo materializados.

FRAUDE, SOBORNO Y CORRUPCIÓN:

La evaluación de exposición del riesgo de fraude, soborno y corrupción se hace principalmente desde la identificación y priorización de los procesos expuestos al fraude financiero, operativo y contable, la información sensible de la compañía, los cargos críticos, los conflictos de interés, las variables del entorno que pueden incrementar el riesgo y generamos valoración de escenarios de riesgo creíbles, posibles y prospectivos que permitan cuantificar su impacto.

Para gestionar este riesgo, desde el Gobierno Corporativo, la Compañía declara “cero tolerancia” al fraude, el soborno y corrupción, y define unos marcos de actuación alineados con sus principios corporativos para guiar la toma de decisiones, como lo son la Política Antifraude y Anticorrupción, el Código de Ética y Conducta y el Reglamento Interno de Trabajo. Así mismo, se establece al Comité de Ética como el máximo responsable del Programa Antifraude y Anticorrupción y está alineado y complementado con los Programas de Ciberseguridad, Gestión de ética y cumplimiento y Control Financiero.

Adicionalmente, cada una de las áreas expuestas a estos riesgos como comercial, técnica, cartera, proveedores, indemnizaciones, etc.; implementan mecanismos de control y monitoreo para mitigar este riesgo.

De manera transversal para la Compañía, se define la Línea Ética como el principal medio

de denuncia frente a situaciones de desviación de la conducta por parte de sus grupos de interés. Este medio también presta servicios de consulta frente a dudas o inquietudes asociadas a los marcos de actuación.

RIESGO CYBER:

El riesgo cibernético se refiere a las amenazas y vulnerabilidades asociadas con el uso de tecnologías de la información y la comunicación (TIC), así como con la interconexión de sistemas digitales. Este riesgo abarca una amplia gama de posibles incidentes, incluyendo ataques de hackers, malware, phishing, robo de datos, fallas en la seguridad de la información y otros eventos que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos y sistemas de una organización. El riesgo cibernético puede tener consecuencias significativas, como pérdidas financieras, daños a la reputación, interrupciones en las operaciones comerciales y posibles sanciones legales.

Dentro de las medidas de seguridad cibernética implementadas por la Compañía para estar preparados para responder efectivamente a estas amenazas se destacan Instalar firewalls y sistemas IDS para monitorear y controlar el tráfico de red entrante y saliente, identificando y bloqueando cualquier actividad sospechosa o maliciosa, utilización de software antivirus y antimalware en todos los dispositivos y sistemas para detectar y eliminar amenazas de software malicioso, Mantener todos los sistemas operativos, aplicaciones y software actualizados con los últimos parches de seguridad para protegerse contra vulnerabilidades conocidas, mecanismos de autenticación más robustos en los sistemas y aplicaciones críticas para agregar una capa adicional de seguridad; planes de respuesta a incidentes para abordar y mitigar los impactos de posibles brechas de seguridad, así como planes de continuidad del negocio para garantizar la operatividad continua en caso de interrupciones graves, entre otros.

RIESGOS DE LA/FT:

Aunque una compañía esta exceptuada del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) estamos conscientes que de igual manera enfrenta riesgos relacionados con el lavado de activos y la financiación del terrorismo. Por lo anterior y como buena práctica decidió Implementar el sistema LAFT, el cual nos permite identificar, evaluar y gestionar estos riesgos de manera proactiva, lo que ayuda a proteger los intereses de la empresa y a prevenir posibles consecuencias negativas.

RIESGO NORMATIVO Y LEGAL:

El riesgo operacional de incumplimiento normativo y legal se refiere a la posibilidad de que la compañía no cumpla con las leyes, regulaciones, normativas y estándares aplicables en su industria. Esto puede incluir leyes relacionadas con la intermediación de seguros, protección al consumidor, lavado de activos, financiación del terrorismo, privacidad de datos, entre otros aspectos legales y regulatorios.

Para gestionar adecuadamente este riesgo se han implementado medidas y controles efectivos tales como: Integrar el riesgo de incumplimiento normativo y legal en el proceso general de gestión de riesgos de la compañía, identificando y evaluando los riesgos asociados y desarrollando estrategias para mitigarlos de manera efectiva, mantenerse actualizado sobre todas las leyes, regulaciones y normativas aplicables y asegurarse de comprender cómo se aplican a las operaciones de la compañía, desarrollar y documentar políticas y procedimientos claros que establezcan los estándares de cumplimiento para todos los empleados y partes interesadas relevantes. Estos abordan áreas críticas como la ética comercial, la privacidad de los datos, la prevención del lavado de activos y la protección al consumidor, entre otros, Se brinda capacitación regular a los empleados sobre las leyes y regulaciones aplicables, así como sobre los riesgos asociados con el incumplimiento normativo y legal y los cambios en los procesos implementados por la compañía para garantizar su cumplimiento, entre otros.

EVENTOS DE RIESGO OPERATIVO RELEVANTES DURANTE EL PERIODO

Durante el período no hubo eventos de riesgo operativo relevantes materializados. Sin embargo, la compañía continúa trabajando por el mejoramiento continuo del sistema en pro de la mitigación de riesgos, buscando optimizar los procesos, implementación de mejoras a través de herramientas tecnológicas y eliminación de procesos manuales en la operación.

INTERVENCIÓN DE RIESGOS:

La organización ha establecido un proceso para la intervención de riesgos priorizados de acuerdo con la medición del riesgo residual, basado en la ejecución de planes de acción para la eliminación o mitigación de los eventos operativos.

ESTRATEGIAS DE MITIGACIÓN

Implementación de controles internos mejorados:

Se reforzaron los controles internos en áreas clave de la operación, como la emisión de

pólizas, la gestión de reclamos y el registro oportuno en el software de riesgos de la compañía para reforzar la reducción de riesgos y control en la medición de riesgos de manera objetiva y oportuna.

Software de Riesgos:

La compañía cuenta con un software de riesgos propio para facilitar la medición, análisis e intervención de los riesgos. Durante el año se lograron mejoras significativas para la medición efectiva e integral de los riesgos. Adicionalmente se establecieron controles que previenen cambios subjetivos en la medición y resultado final.

Actualización de Políticas y Procedimientos:

Se revisaron y actualizaron las políticas y procedimientos internos para garantizar que estén alineados con las mejores prácticas, las regulaciones más recientes y la eficiencia operativa.

Cultura de Riesgo:

La organización logró un mayor fortalecimiento frente a la cultura de riesgo que promueve la identificación, evaluación y control de los riesgos.

Formación y Capacitación

Durante el año, se brindó capacitación continua al personal en áreas críticas como el cumplimiento normativo, la gestión de riesgos, la seguridad cibernética y la atención al cliente para mejorar la conciencia y la competencia en la gestión de riesgos.

Revisión del Plan de Continuidad del Negocio:

Se actualizó y se viene probando regularmente los planes de continuidad del negocio y los procedimientos de recuperación ante desastres para garantizar la capacidad de la empresa para mantener la operación en caso de interrupciones graves.

Mejoras en tecnología y seguridad cibernética:

Durante el 2023 se Invirtió en tecnología y sistemas de seguridad cibernética avanzada para proteger los datos de los clientes, prevenir el acceso no autorizado a la información confidencial y mitigar los riesgos de ciberataques.