CAPÍTULO 22 POLÍTICA DE GESTÃO DO RISCO OPERACIONAL

22.1 PROPRIETÁRIO DA POLÍTICA

APROVAÇÃO CA: 31/10/2023
VIGÊNCIA: 10/2023 a 31/2024

A Diretoria Corporativa de Riscos.

22.2 ABRANGÊNCIA

A presente Política será aplicável a todas as entidades do Grupo.

22.3 OBJETIVOS

Os principais objetivos da presente Política de Gestão do Risco Operacional são:

- Estabelecer as pautas gerais, os princípios básicos e o âmbito geral de atuação em matéria de gestão de risco operacional que garantam uma aplicação coerente no Grupo.
- Estabelecer os processos necessários para identificar, medir, vigiar, elaborar e notificar os riscos operacionais, sua avaliação e a forma de mitigá-los.
- Promover uma sólida cultura de risco e um sistema eficaz de gestão do risco operacional.

22.4 IDENTIFICAÇÃO, MEDIÇÃO, VIGILÂNCIA E NOTIFICAÇÃO DO RISCO OPERACIONAL

A MAPFRE dispõe de um Sistema de Gestão de Riscos baseado na gestão integrada de todos os processos de negócio e na adequação do nível de risco aos objetivos estratégicos estabelecidos.

O risco operacional é um dos riscos compreendidos no Sistema de Gestão de Riscos, cuja gestão tem como objetivo atenuar as perdas reais e potenciais derivadas da inadequação ou das falhas dos processos, do pessoal e dos sistemas internos, ou da ocorrência de acontecimentos externos.

22.4.1 IDENTIFICAÇÃO

Com o objetivo de conhecer mais detalhadamente e de forma estruturada as diferentes casuísticas que podem ocasionar a materialização desta tipologia de riscos, adota-se a categorização de riscos e eventos operacionais amplamente difundidos nas normas internacionais.

O risco operacional é inerente ao desenvolvimento de qualquer atividade, e sua ocorrência pode gerar uma perda e/ou uma consequência negativa sobre os resultados empresariais.

Entre os exemplos de falhas ou inadequações com causa ou origem nas quatro fontes do risco operacional, vale destacar:

- *Processos*: erro no desenho ou execução dos processos, tanto seguradores como de suporte.
- *Pessoal*: erros humanos, fraude, dependência excessiva de pessoal-chave, supervisão da gestão inadequada, desequilíbrios entre habilidades e requisitos do cargo.
- *Sistemas*: proteção de dados ou segurança inadequadas, controles de acesso fracos, falta de evidências suficientes antes do aumento da produção, sistemas ou ferramentas deficientes, instáveis ou muito complexos.
- *Evento externo*: mudanças no contexto regulatório, desastres naturais (enchentes, terremotos, incêndios etc.) e desastres causados pelo homem (terrorismo, instabilidade política e social)que possam afetar a continuidade das operações.

22.4.2 MEDIÇÃO

A avaliação do risco operacional é feita por meio dos seguintes procedimentos:

- A análise qualitativa dinâmica por processos para que os gestores de cada área ou departamento identifiquem e avaliem os riscos em potencial que afetam tanto os processos de negócio quanto de suporte. Essa análise considera a autoavaliação de riscos, a documentação de manuais de controles internos nos quais são identificados os controles associados a riscos, a avaliação da eficácia dos controles e a gestão de medidas corretivas estabelecidas para mitigar ou reduzir os riscos e/ou melhorar o ambiente de controle.

- A análise de cenários, considerando o risco de eventos extremos, mas plausíveis. Eles são definidos com a participação dos Diretores e permitem conhecer os fatores que intervêm em cada cenário e suas consequências para o Grupo. Cada cenário será avaliado em termos de impacto e probabilidade, considerando a avaliação do custo que o evento de risco teria nas operações (impacto) e da frequência com que o evento pode ocorrer, baseado na experiência da gestão e no histórico (probabilidade). A Diretoria Corporativa de Riscos determinará os cenários que serão analisados globalmente no Grupo em termos de probabilidade e impacto. Tudo isso, sem prejuízo às competências já atribuídas em outras políticas a outras Áreas ou Diretorias do Grupo.

- De forma complementar, a quantificação do risco operacional nas entidades seguradoras e resseguradoras do Grupo do Espaço Econômico Europeu será feita de acordo com a fórmula padrão estabelecida nas normas de Solvência II.

22.4.3 LIMITES ESPECÍFICOS E ACOMPANHAMENTO

Como indicado acima, a medição do risco operacional toma como base uma análise dinâmica por processos, de forma que os responsáveis por cada área identificam e avaliam periodicamente os indicadores de riscos potenciais e de controles implantados nas operações. Os resultados são analisados através de:

- *Criticidade de riscos*: indicador que examina a importância e a probabilidade de ocorrência dos riscos avaliados. Este varia entre 100 (pior resultado) e 0 (ausência de risco), considerando aceitável ou assumível uma criticidade igual ou inferior a 68,3.
- *Suficiência dos controles*: indicador que analisa a suficiência dos controles vinculados a um tipo de risco ou processo, assim como a efetividade desses controles para mitigar, detectar ou prevenir os riscos avaliados nesse tipo de risco ou processo.

  Este indicador se complementa com o indicador secundário *GEC avaliados* (GEC: grau de efetividade dos controles), que mede o grau de efetividade dos controles identificados nos manuais de controle interno da entidade. Ambos os indicadores variam entre 100 (controles eficazes e seguros) e 0 (controle fraco ou mal desenhado).

Estabeleceu-se o nível de tolerância em 75 e 31,7, respectivamente, para a criticidade de riscos e a suficiência dos controles.

22.4.4 VIGILÂNCIA

A primeira linha de defesa (que assume os riscos e gerencia os controles) de cada entidade do Grupo será responsável por evitar que os riscos operacionais assumidos ultrapassem os limites de risco estabelecidos para esses efeitos.

Por sua natureza, o risco operacional é inerente a todas as atividades desenvolvidas em uma organização ou entidade e pode ser causado por qualquer funcionário, independentemente do nível profissional que ele ocupe na organização.

Portanto, é importante que todos os funcionários conheçam as fontes de risco operacional dentro do seu ambiente de trabalho, já que atuam cotidianamente como gestores de riscos operacionais e ajudam na gestão ativa deles.

A primeira linha de defesa informará à Diretoria de Riscos sobre os eventos ou incidentes de risco operacional. Com essa finalidade, a Diretoria de Riscos manterá um registro ou banco de dados de eventos de risco operacional para categorização e gestão.

Corresponderá à Diretoria de Riscos verificar que os riscos assumidos não superem os limites de risco estabelecidos, aplicando as metodologias determinadas e empregando as ferramentas informáticas implementadas a esse fim.

22.4.5 NOTIFICAÇÃO

A Diretoria de Riscos, dentro de sua competência, deverá elaborar e enviar aos órgãos de governança correspondentes, como o Comitê de Riscos, os relatórios periódicos de acompanhamento dos riscos operacionais (por exemplo, o relatório anual de controle de riscos e os relatórios periódicos de acompanhamento de eventos e incidentes). A Diretoria de Riscos das entidades, por sua vez, deverá enviar esses relatórios à Diretoria Corporativa de Riscos. Essas informações serão enviadas pelo menos trimestralmente, exceto se o envio anual for suficiente devido à natureza dos riscos em questão. Em todos os casos, os órgãos de governança devem ser informados imediatamente a respeito de qualquer risco que:

- Devido à sua evolução, ultrapasse os limites de risco estabelecidos;
- Possa resultar em perdas iguais ou superiores aos limites de risco estabelecidos; ou
- Possa ameaçar o cumprimento das exigências de solvência ou a continuidade de funcionamento da Entidade.