MANUAL DE GERENCIAMENTO DE RISCO OPERACIONAL

SUMÁRIO

1 – INTRODUÇÃO 3
2 – OBJETIVO 3
3 – DEFINIÇÃO 3
4 – ESTRUTURA SIMPLIFICADA GERENCIAMENTO RISCO OPERACIONAL 4
5 – EVENTOS DE RISCO OPERACIONAL 4
6 – GESTÃO DE RISCOS 6
7 – GERENCIAMENTO DE RISCO OPERACIONAL 7
7.1 – Identificação 7
7.2 – Avaliação e Mensuração 8
7.3 – Controle 8
7.4 – Mitigação 8
7.5 – Monitoração e Reporte 9
8 – AVALIAÇÃO DOS PROCESSOS 9
9 – PROCEDIMENTOS DE CONFORMIDADE 9
10 – PLANO DE AÇÃO 9
11 – POLÍTICAS DE CONTINUIDADE/GESTÃO DE SERVIÇOS/TI 10
12 – DIVULGAÇÃO E REVISÃO 10
13 – CONSIDERAÇÕES FINAIS 11

1 – INTRODUÇÃO

O manual contempla atender os requisitos para a implementação da estrutura simplificada de gerenciamento contínuo de risco operacional, em atendimento as normas vigentes quanto à existência de diretrizes e procedimentos.

Visa orientar a Diretoria, funcionários e colaboradores externos relevantes da Cooperativa nos procedimentos internos destinados a minimizar a ocorrência de riscos, estabelecendo métodos de controle conforme ressaltados nas Resoluções nº 4.557/17 e nº 4.606/17, ambas do Conselho Monetário Nacional.

A **Cooperativa de Economia e Crédito Mútuo dos Empregados da Merck Sharp & Dohme Farmacêutica - COOPERMSD** deverá implementar a sua estrutura simplificada de gerenciamento contínuo de risco operacional onde contempla a identificação, mensuração, avaliação, monitoração, reporte, controle e mitigação dos riscos que a Instituição está exposta.

Deverá prever políticas, estratégias, rotinas e procedimentos para o gerenciamento de riscos, periodicamente avaliados nas reuniões da Diretoria e registradas em ata.

Destacamos que, os processos relativos ao gerenciamento de riscos deverão ser avaliados periodicamente pela auditoria interna contratada pela Cooperativa.

2 – OBJETIVO

Desenvolver funções internas que permitam à Cooperativa o monitoramento dos riscos aos quais está sujeita, adequadas ao seu perfil e modelo de negócio.

3 – DEFINIÇÃO

Risco operacional é a possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas.

O risco operacional inclui também o risco legal associado à inadequação ou deficiência em contratos firmados pela COOPERMSD, bem como sanções em razão de descumprimento de dispositivos legais e às indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Instituição.

A avaliação do risco legal é realizada de forma contínua pela Diretoria da Cooperativa.

Define-se perda operacional como o valor quantificável associado aos eventos de risco operacional.

4 – ESTRUTURA SIMPLIFICADA GERENCIAMENTO RISCO OPERACIONAL

A estrutura simplificada de gerenciamento contínuo de risco operacional estabelecida tem como objetivo a identificação, avaliação, mensuração, monitoramento, reporte, controle, mitigação do risco operacional e deve estar compatível com o modelo de negócio, com a natureza das operações, com a complexidade dos produtos, dos serviços, das atividades e dos processos.

A estrutura deve conter mecanismos que permitam a implementação das políticas, dos processos, de infraestrutura condizentes com a natureza e complexidade da Cooperativa.

Assegurar a aderência, o comprometimento de funcionários e colaboradores para a adequada gestão do risco operacional, da continuidade de negócios e dos objetivos da Instituição.

Na estrutura devem estar definidos:

a) os papéis e principais responsabilidades dos envolvidos na gestão de risco operacional;

b) identificadas as linhas de reporte que asseguram a comunicação apropriada;

c) especificadas as atividades de controle para o adequado gerenciamento de risco operacional.

5 – EVENTOS DE RISCO OPERACIONAL

Eventos de risco operacional são aqueles decorrentes de falhas ou inadequações de processos, pessoas, sistemas, eventos externos e podem provocar impactos indesejáveis no resultado da Cooperativa, seja por meio de despesas incorridas ou pela diminuição de receita.

➢ O fator Processos está ligado a falhas, deficiências ou inadequações nos processos internos. Adequação à legislação, pontos de controle, comunicação interna e segurança física são aspectos que devem ser observados na modelagem de processos para evitar risco operacional.

Alguns eventos causados por este fator de risco são: falta de diligência, reconciliação inadequada, riscos de aquisição, falha em novos produtos ou linhas de negócios, procedimentos de segurança física inadequada, processo de controle de qualidade inadequado, benefícios indevidos a empregados, empregadores, diretores, entre outros.

➢ O fator Pessoas está ligado a falhas, deficiências ou inadequações no desempenho das atribuições pelos funcionários, colaboradores e contratados, envolvendo os aspectos referentes à conduta (postura ética, honestidade, negligência), competências (habilidades, conhecimentos e experiência) e ambiente de trabalho (cultura organizacional e motivação).

➢ O fator Sistemas está ligado a falhas, deficiências ou inadequações nos sistemas utilizados pela Cooperativa envolvendo aspectos de hardware, software, rede de comunicação, segurança lógica, análise e programação.

Alguns eventos causados por este fator de risco são: perda de dados, falhas sistêmicas diversas, interrupções no fornecimento de informação eletrônica (interna e externa), tecnologia insuficiente ou obsoleta ao negócio, erro operacional - relacionado com a tecnologia, uso não autorizado ou mau uso da tecnologia, falhas nos equipamentos, hardware inadequado, invasões por hackers, falhas na proteção da rede, vírus de computadores, falhas de programação entre outros.

➢ O fator Eventos Externos considera situações de força maior, ambiente externo e agente externo. Envolvem desastres naturais e catástrofes, criação/alteração de legislação, ações criminosas, fornecedores, terceirizados e clientes.

➢ São classificados como eventos de perda efetiva aqueles cuja manifestação causou perda financeira ou contábil para a Cooperativa, refletindo diretamente no resultado.

➢ Os documentos associados a perdas efetivas devem ser arquivados por um período mínimo de 5 (cinco) anos, respeitados aqueles com prazo de expurgo específico.

➢ Os eventos de quase-perda são eventos de risco operacional que não causaram perda efetiva por conta da intervenção de agente interno ou externo. Neste caso, a intervenção mencionada é essencial para impedir uma perda efetiva. Devem ser identificados e monitorados por indicarem fragilidades que devem ser corrigidas.

A Cooperativa, conforme a sua estrutura simplificada de gerenciamento, deverá utilizar ferramenta para o monitoramento da severidade dos eventos de risco operacional adequada ao seu porte e complexidade dos negócios.

6 – GESTÃO DE RISCOS

A gestão de risco operacional está submetida à Política de Estrutura Simplificada de Gerenciamento Contínuo de Risco Operacional, que deverá ser elaborada e aprovada pela Diretoria da Cooperativa.

O modelo de gestão do risco operacional adotado tem por objetivo identificar, mensurar, avaliar, monitorar, reportar, controlar e mitigar as exposições ao risco de produtos, processos e serviços, em conformidade com norma vigente.

Entende-se que a boa governança de riscos envolve, entre outros, os seguintes elementos:

➢ Envolvimento da alta direção;
➢ Responsabilidades claramente definidas;
➢ Segregação de funções conforme a realidade da Cooperativa;
➢ Rotinas adequadas de auditoria e supervisão.

A política de gerenciamento contínuo de risco da Cooperativa deve estabelecer como premissas as melhores práticas na gestão do risco operacional visando, dentre outros:

- Estruturar a área de risco operacional com ferramentas adequadas conforme o perfil da Instituição;
- Assegurar a efetividade do gerenciamento do risco operacional.

As falhas, de preferência, devem ser registradas em base de dados única para identificação e análise das principais causas de perdas operacionais, permitindo uma atuação objetiva na eliminação dos problemas.
Para o efetivo gerenciamento das perdas, este registro de informações é feito, considerando:

- Descrição do evento;
- Identificação do tipo de risco;
- Valor da perda;
- Órgão afetados e responsáveis;
- Plano de ação.

7 – GERENCIAMENTO DE RISCO OPERACIONAL

As fases do gerenciamento do risco operacional são: Identificação, avaliação, mensuração, controle, mitigação, monitoração e reporte.

7.1 – Identificação

Consiste em identificar e classificar os eventos de risco operacional a que a Cooperativa está exposta, indicando áreas de incidência, causas, potenciais impactos financeiros associados aos processos, produtos e serviços da Instituição.

A modelagem de processos tem por objetivos:

- Identificar os riscos operacionais;
- Documentar o processo, a fim de possibilitar visão ampla das atividades da Cooperativa;
- Subsidiar análise da situação atual, visando melhoria continua, e;
- Possibilitar o gerenciamento dos processos sob diversas óticas (controle, riscos, etc.).

7.2 – Avaliação e Mensuração

É a quantificação ou dimensionamento da exposição ao risco operacional identificado, com o objetivo de avaliar o impacto nas operações da Cooperativa.

Pode, também, envolver avaliação qualitativa dos riscos identificados, estimando sua probabilidade de ocorrência e impacto de forma a determinar o nível de tolerância ao risco.

7.3 – Controle

Consiste em registrar o comportamento dos riscos operacionais, limites, indicadores e eventos de perda operacional, bem como implementar mecanismos de forma a garantir que os limites e indicadores de risco operacional permaneçam dentro dos níveis desejados.

O controle está associado à diminuição da incerteza em relação a eventos futuros, ou seja, se o grau de dúvida em relação aos procedimentos existentes e suas consequências sobre as atividades estão dentro de um limite tolerável, consideramos que está sob controle.

A Cooperativa tem como objetivo manter um controle eficiente e adequado a sua realidade, para evitar ou diminuir as incertezas em relação a eventos futuros.

Os controles necessários ao gerenciamento adequado dos riscos operacionais são considerados eficientes e eficazes se:

- Os objetivos das operações da Cooperativa estão sendo alcançados;
- As demonstrações financeiras publicadas são preparadas de maneira confiável;
- As leis e regulamentos aplicáveis estão sendo cumpridos.

7.4 – Mitigação

Consiste em criar e implementar mecanismos para modificar o risco buscando reduzir as perdas operacionais por meio da remoção da causa, alteração da probabilidade de ocorrência ou alteração das consequências do evento.

Após a conclusão do mapeamento, e identificados os riscos operacionais, a administração da Cooperativa sugere ações com o intuito de mitigá-los.

Essas ações, que tem por característica estar no âmbito de responsabilidade e decisão da Diretoria, podem ser acompanhadas periodicamente para verificação quanto à implantação ou não.

7.5 – Monitoramento e Reporte

Monitoramento é a ação que tem por objetivo identificar as deficiências do processo de gestão do risco operacional de forma que as fragilidades detectadas sejam levadas ao conhecimento da Diretoria.

É a fase de retroalimentação do processo de gerenciamento de risco operacional, onde é possível detectar fragilidades nas fases anteriores.

8 – AVALIAÇÃO DOS PROCESSOS

A identificação dos riscos é avaliada com base em análises de:

- Detalhamento do risco;
- Fatores de contribuição para a ocorrência do risco;
- Probabilidade/Impacto;
- Controles mitigadores;
- Eficiência/eficácia dos controles;
- Avaliação do diretor responsável;
- Plano de ação, e;
- Prazo pela implementação.

9 – PROCEDIMENTOS DE CONFORMIDADE

Os Procedimentos de Conformidade têm o objetivo de avaliar a aderência às normas internas e externas. Consistem em questionários – lista de verificação, elaborados a partir dos manuais, políticas, regulamentos internos da Cooperativa e as normas vigentes do órgão fiscalizador.

10 – PLANO DE AÇÃO

Ação definida pela Diretoria, mencionando prazo para implementação, visando melhorar processos, minimizar riscos ou solucionar problemas identificados nos relatórios de auto avaliação e também, os apresentados pelas Auditorias contratadas.

11 – POLÍTICAS DE CONTINUIDADE / GESTÃO DE SERVIÇOS / TI

A política de continuidade de negócios e o plano de contingência da COOPERMSD devem ser elaboradas e aprovadas pela Diretoria.

O plano de contingência constitui documento no qual é apresentada a estrutura organizada, para combater determinada emergência, ocasionada pela ocorrência de risco operacional.

No plano de contingência devem estar definidas as responsabilidades, as ações para o controle da emergência e a mitigação dos efeitos decorrentes, uma vez que, nesse setor econômico, interrupções nos negócios representam risco de perdas financeiras, de degradação da imagem no mercado e de insatisfação dos associados.

O objetivo do plano de contingência é permitir a continuidade dos processos de negócios da Cooperativa afetada pela emergência, quando os componentes que os suportam falharem em função de algum evento, ameaça ou desastre tecnológico, humano, natural e/ou físico.

A contratação de prestadores de serviços deve estar em conformidade com a Política de Gestão de Serviços Terceirizados.

A Cooperativa deverá manter o gerenciamento do risco operacional decorrente de serviços terceirizados.

Para os contratos de TI deverá constar a permissão de acesso ao Banco Central do Brasil aos termos firmados, documentação e informação referente aos serviços prestados e dependências do contrato.

12 – DIVULGAÇÃO E REVISÃO

O manual aprovado pela Diretoria, está sendo comunicada para os funcionários e colaboradores relevantes para o necessário cumprimento, de forma a promover a disseminação da cultura na Cooperativa.

A publicação está na internet, no site da Cooperativa e o documento físico encontra-se nas dependências da Cooperativa.

Este manual deverá ser revisado com frequência mínima de 2 (dois) anos, ou se houver mudanças significativas, sendo aprovado pela Diretoria e registrada em ata de reunião.

13 – CONSIDERAÇÕES FINAIS

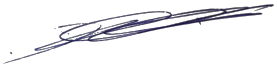
O manual deverá ser arquivado e mantido à disposição do Banco Central do Brasil por 5 (cinco) anos.

Todas as observações e ocorrências, assim como ações a serem aprimoradas para atualização deste manual serão inseridas nas atas da Diretoria.

São Paulo/SP, 13 de novembro de 2020.

Electronically signed by: Carlos Kanji Cesar Kamijo
Reason: Approved
Date: Jun 3, 2021 10:25 ADT

Carlos Kanji César Kamijo
Diretor Presidente



Electronically signed by: Jose Angelo Francolin
Reason: Approved
Date: Jun 7, 2021 11:33 ADT

José Angelo Françolin
Diretor Administrativo

Electronically signed by: Rubio Vinicius de Marcantonio
Reason: Approved
Date: Jun 7, 2021 10:17 ADT

Rúbio Vinicius de Marcantonio
Diretor Operacional

MANUAL DE RISCO OPERACIONAL v13112020

Final Audit Report 2021-06-07

Created:	2021-06-03
By:	Janete Aparecida Rogante (janete_rogante@merck.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA9FdsBlmnj5UdwuJUeCd4dDeqfWvmfeFX

"MANUAL DE RISCO OPERACIONAL v13112020" History

Document created by Janete Aparecida Rogante (janete_rogante@merck.com)
2021-06-03 - 1:00:12 PM GMT- IP address: 155.91.45.238

Document emailed to Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com) for signature
2021-06-03 - 1:01:41 PM GMT

Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com) verified identity with Adobe Sign authentication
2021-06-03 - 1:25:52 PM GMT

Document e-signed by Carlos Kanji Cesar Kamijo (carlos_kanji@merck.com)
Signature Date: 2021-06-03 - 1:25:52 PM GMT - Time Source: server- IP address: 155.91.45.236

Document emailed to Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com) for signature
2021-06-03 - 1:25:54 PM GMT

Email viewed by Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com)
2021-06-07 - 12:22:59 PM GMT- IP address: 201.27.176.24

Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com) verified identity with Adobe Sign authentication
2021-06-07 - 1:17:54 PM GMT

Document e-signed by Rubio Vinicius de Marcantonio (rubio_marcantonio@merck.com)
Signature Date: 2021-06-07 - 1:17:54 PM GMT - Time Source: server- IP address: 155.91.45.235

Document emailed to Jose Angelo Francolin (joseangelo_francolin@merck.com) for signature
2021-06-07 - 1:17:56 PM GMT

Email viewed by Jose Angelo Francolin (joseangelo_francolin@merck.com)
2021-06-07 - 2:23:16 PM GMT- IP address: 155.91.45.234

Jose Angelo Francolin (joseangelo_francolin@merck.com) verified identity with Adobe Sign authentication
2021-06-07 - 2:33:31 PM GMT

Document e-signed by Jose Angelo Francolin (joseangelo_francolin@merck.com)
Signature Date: 2021-06-07 - 2:33:31 PM GMT - Time Source: server- IP address: 155.91.45.234

Agreement completed.
2021-06-07 - 2:33:31 PM GMT