BANCO MERCANTIL

Política Gerenciamento do Risco Operacional

Vigência a partir de

21/12/2023

Validade

21/12/2024

Versão

01

Divulgação EXTERNA

Sumário

1. APRESENTAÇÃO

A presente Política é aplicável a todos que estão indicados no item "Abrangência" deste documento.

A Política Institucional de Gerenciamento do Risco Operacional do Conglomerado Mercantil foi construída baseando-se nas diretrizes do Conselho Monetário Nacional que, por meio da Resolução nº. 4.557/17, alterada pelas Resoluções nºs. 4.745/19, 4.926/21, 4.943/21 e 5.076/23, dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

Em conformidade ao artigo 32º da Resolução CMN nº. 4.557/17, define-se o **risco operacional** como a possibilidade de ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas. Tal definição inclui o risco legal associado à inadequação ou deficiência em contratos firmados pelo Banco Mercantil, bem como sanções em razão de descumprimento de dispositivos legais e a indenização por danos a terceiros decorrentes das atividades desenvolvidas pela Instituição.

2. BASE LEGAL

Tipo	Número/Ano	Objetivo
Resolução CMN	4.557/2017	Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.
Resolução CMN	4.926/2021	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações
Resolução CMN	4.943/2021	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.
Resolução CMN	5.076/23	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, e a Resolução nº 4.606, de 19 de outubro de 2017.

3. ABRANGÊNCIA

Esta Política se aplica ao Banco Mercantil e às empresas do Grupo Mercantil. A ciência e o cumprimento das diretrizes e regras aqui estabelecidas são obrigatórios a todos os seus colaboradores e terceiros.

4. GLOSSÁRIO DE TERMOS E SIGLAS

- **CRO** – Diretor de Risco (*Chief Risk Officer)*
- **RAS** – Declaração de Apetite a Riscos (*Risk Appetite Statement*)
- **RCSA** – Questionário de auto avaliação de riscos e controles (*Risk and Control Self-Assessment)*
- **ICR** – Indicador Chave de Risco
- **OKR** – Objetivos e Resultados-Chave (*Objectives and Key Results*)
- **COSO** – – Comitê das Organizações Patrocinadoras da Comissão Treadway (Committee of Sponsoring Organizations of the Treadway Commission)
- **LGPD** – Lei Geral de Proteção de Dados

5. ESTRUTURA DE GERENCIAMENTO DO RISCO OPERACIONAL

A Estrutura de Gerenciamento do Risco Operacional do Grupo Mercantil está constituída em uma unidade única, centralizada na Gerência de Risco Operacional e Controles Internos, subordinada à Diretoria de Riscos e Compliance (CRO – Chief Risk Officer) e abrange todas as instituições do Conglomerado Prudencial.

O Gerenciamento do Risco Operacional no Mercantil integra-se às estratégias e aos negócios de cada Instituição participante do grupo, com o intuito de alinhar todos os processos existentes e praticados com as políticas vigentes.

A Estrutura de Gerenciamento do Risco Operacional favorece uma ação compartilhada e multidisciplinar, na qual os funcionários de cada área são os especialistas do processo e desempenham importante papel em uma gestão integrada de riscos.

5.1. Apetite ao Risco Operacional

O apetite a riscos refere-se aos tipos e níveis de riscos que, de forma ampla, a Instituição se dispõe a admitir na realização dos seus negócios e objetivos.

O apetite a riscos da Instituição é definido pela Alta Administração e está alinhado à estratégia da Organização, estando estabelecido por meio da Declaração de Apetite por Riscos (RAS – Risk Appetite Statement) documento aprovado pelo Conselho de Administração. É um processo contínuo, que se inicia com o Planejamento Estratégico e Mercadológico, passando pela identificação dos riscos estratégicos e respectivos apetites e limites operacionais.

Diante do elevado volume de atividades, operações e transações realizadas, é natural que sejam incorridas perdas operacionais resultantes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, além da própria exposição a eventos externos.

A estratégia da Instituição para o Gerenciamento do Risco Operacional prevê o monitoramento da exposição aos riscos por meio das ferramentas de gestão que visam a identificação (causas-raízes) e mitigação das perdas operacionais. São acompanhados indicadores que auxiliam na gestão do risco, em atendimento às diretrizes estratégicas definidas, assegurando que as perdas estejam dentro do apetite definido na RAS.

Considera-se indicadores que relacionam o valor das perdas operacionais internas que mensuram, de forma segregada entre as principais origens (cíveis, trabalhistas, fraudes, entre outros), tanto em termos nominais quanto relativizados em função de parâmetros como a receita operacional ou as despesas com pessoal da Instituição. Ainda neste contexto, a RAS contempla indicadores de tecnologia abrangendo a disponibilidade de serviços críticos, tempo médio para reparo (MTTR) e a segurança cibernética. De forma complementar, foram estabelecidas tolerâncias ao risco operacional, níveis máximos de risco que o Mercantil pode assumir ao realizar suas atividades. Quando ultrapassadas, os motivos são avaliados e planos de ação são definidos e acompanhados para que o nível de risco volte aos limites ou ao apetite estabelecido.

5.2. Escopo de Atuação do Gerenciamento do Risco Operacional

A estrutura de Gerenciamento do Risco Operacional irá identificar, mensurar, avaliar, monitorar, reportar, controlar e mitigar os riscos associados ao Conglomerado Prudencial do grupo Mercantil. Alinhado a este conceito, que é apresentado na documentação COSO ERM, as principais ações desenvolvidas são:

- **Identificação de Eventos** – Os eventos internos e externos que influenciam o risco operacional são identificados e classificados entre riscos e oportunidades. Essas oportunidades são canalizadas para os processos de estabelecimento de estratégias da administração ou de seus objetivos. A identificação de possíveis exposições a riscos se dá através de mapeamentos de processos, ferramentas de gestão dentre outros;

- **Avaliação de Riscos** – Os riscos identificados são analisados considerando a probabilidade e a consequência e priorizados com base no grau de severidade, no contexto do apetite ao risco, para determinar o modo pelo qual deverão ser administrados;

- **Avaliação de Controles (incluindo execução de testes)** - As atividades de controles existentes nos processos são mapeadas e avaliadas, tendo em vista que um efetivo sistema de controles internos reduz a probabilidade de erros humanos e irregularidades em processos e sistemas, que resultam na diminuição das perdas operacionais;

- **Resposta a Risco e Mitigação** – Diante da exposição ao risco residual, a Instituição estabelece a resposta ao mesmo, que inclui evitar, reduzir, compartilhar ou aceitar os riscos de acordo com a estratégia e a avaliação do efeito, custos e benefícios. São desenvolvidas ações para manter o alinhamento com os apetites e tolerâncias definidos na RAS;

- **Monitoramento e Comunicação** – O monitoramento é realizado através de atividades gerenciais contínuas e/ou de avaliações independentes. Todo o resultado desta gestão é reportado aos gestores e à Alta Administração através de relatórios que sinalizam os aspectos qualitativos e quantitativos da exposição a risco operacional da Instituição.

6. METODOLOGIA APLICADA

Baseado nos direcionamentos e orientações do COSO, a metodologia consiste no estabelecimento e na disseminação de políticas claras, métodos e técnicas padronizados e aplicáveis ao Grupo Mercantil, tendo como objetivo identificar, mensurar, avaliar, monitorar, reportar, controlar e mitigar as exposições a riscos. É constituída pelas etapas qualitativa e quantitativa.

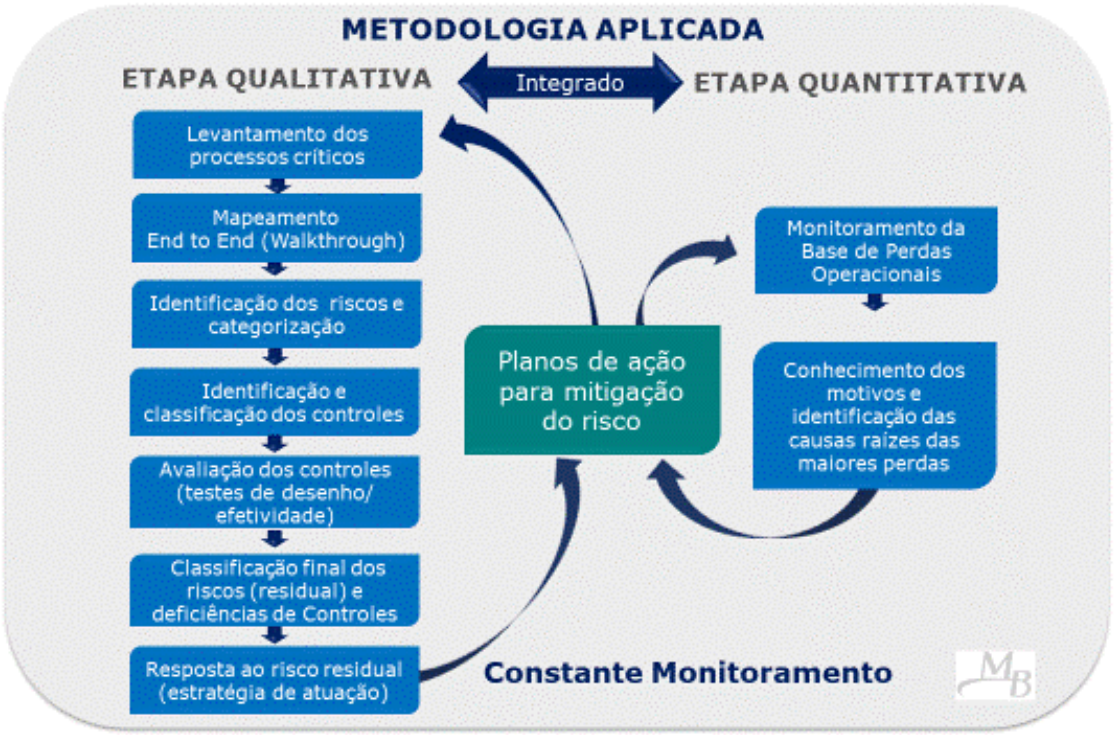

Diagrama 2 - Metodologia Aplicada

6.1. Etapa Qualitativa

A etapa qualitativa compreende as seguintes etapas:

- **Levantamento dos Processos Críticos:** são priorizados os mapeamentos dos processos considerados críticos do Conglomerado. Estabeleceu-se como critérios para classificação de criticidade e priorização das atividades os seguintes itens como: a materialidade financeira relacionada ao processo, histórico de perdas operacionais, exigência regulamentar, processos contingenciados que possuem maior criticidade em casos de interrupção e aspectos relevantes na visão da Alta Administração.

- **Mapeamento – "*End to End*" (*Walkthrough*):** compreende o entendimento de ponta a ponta de um processo. Os processos, em sua maioria, permeiam mais de uma área administrativa gestora e/ou Ponto de Atendimento. Através do mapeamento é possível identificar os riscos e controles.

- **Identificação dos Riscos e Categorização:** a próxima fase consiste na identificação das exposições a eventos de risco operacional. Os eventos de risco operacional são categorizados de acordo com a resolução vigente, conforme a seguir:

  - Fraude Interna;
  - Fraude Externa;
  - Demandas Trabalhistas e Segurança deficiente do local de trabalho;
  - Práticas Inadequadas relativas a usuários finais, clientes, produtos e serviços;
  - Danos a Ativos Físicos próprios ou em uso pela Instituição;
  - Situações que acarretem a interrupção das atividades da Instituição ou a descontinuidade dos serviços prestados, incluindo o de pagamentos;
  - Falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI);
  - Falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da Instituição, incluindo aquelas relacionadas aos arranjos de pagamento.

A avaliação de riscos é realizada junto ao gestor, maior conhecedor e responsável pelo processo, com relação à probabilidade de ocorrência do risco e seu impacto no caso de se concretizar. São considerados cinco níveis de risco: "muito baixo", "baixo", "médio", "alto" e "muito alto". Para avaliação são observados alguns balizadores que definem o grau de impacto, que são: financeiro, reputacional, regulatório, estrutural/ processual, privacidade/ LGPD e ambiente tecnológico. Para probabilidade são considerados a materialidade dos riscos e o grau de confiança no ambiente de controles.

- **Identificação e Classificação dos Controles:** um efetivo sistema de controles internos reduz a probabilidade de erros humanos e irregularidades em processos e sistemas, resultando na diminuição das perdas operacionais. Os controles podem ser classificados pela sua tipologia (detectivo, preventivo, corretivo, nível de entidade (ELC) ou diretivos), natureza (manual, automatizado ou híbrido – manual dependente de TI ou semiautomáticos) e frequência/periodicidade de execução do controle.

- **Avaliação dos Controles: Teste Desenho / Efetividade:** para avaliação dos controles utiliza-se os testes de desenho e de efetividade, os quais visam validar se a atividade de controle em avaliação fornece segurança razoável para mitigação do risco associado, e ainda se está em efetivo funcionamento. De acordo com a mitigação de riscos, o controle pode ser classificado como "chave" ou "não chave", sendo que os controles "chaves" serão testados.

O **teste de desenho** tem como objetivo validar se a estrutura da atividade de controle é suficientemente precisa para detectar o evento de risco antes de sua materialização, ou então detectar a não conformidade para ser solucionada. O escopo do teste de desenho é mais restrito e limitado, e avalia se o controle está projetado e operando de maneira adequada. Já o **teste de efetividade** visa validar se o controle está evitando ou detectando o evento de risco no período avaliado dentro do esperado na sua modelagem. O escopo do teste de efetividade tem amplitude maior, e avalia se o controle está mitigando o fator de risco.

Em caso de deficiências identificadas durante a realização dos testes de desenho ou de efetividade, são elaboradas recomendações de melhoria ou planos de ação relativas a aquela atividade de controle ou a implementação de um novo controle.

Nesta fase também é avaliada a **qualidade dos controles**, de acordo com o resultado dos testes, além de suas características e o seu contexto no processo, podendo estes serem classificados como "inefetivos", "parcialmente efetivos" ou "efetivos". Para se concluir sobre o nível de efetividade do controle e consequente contribuição para a mitigação do risco a ele vinculado, são considerados alguns balizadores ou atributos durante a avaliação do desenho do controle, tais como: evidência da execução do controle, histórico de falhas do controle, incidência sobre o risco, competência e autoridade do operador do controle, grau de intervenção humana e existência de um padrão de execução formalizado. A avaliação adequada da qualidade do controle é fundamental para que os riscos residuais, a que a Instituição está exposta, sejam conhecidos e reproduzam a realidade.

- **Avaliação dos Riscos Residuais - Matriz de Riscos:** a avaliação de riscos é realizada junto ao gestor, maior conhecedor e responsável pelo processo, com relação à probabilidade de ocorrência do risco e seu impacto no caso de se concretizar. São considerados cinco níveis de risco: "muito baixo", "baixo", "médio", "alto" e "muito alto", observando-se os impactos relativos a: financeiro, reputacional, regulatório, estrutural/ processual, privacidade/ LGPD e ambiente tecnológico. Esta exposição ao risco operacional é definida ainda através da relação de causa e efeito no contexto do processo em avaliação.

A classificação dos controles conjugada com o nível de risco gera o risco residual.

O gerenciamento do risco operacional utiliza regras de parametrização para cada classificação de risco e controle, o que permite que o risco residual gerado seja baseado em critérios objetivos, não dependendo assim, do julgamento de quem o avalia. A matriz de riscos gerada é essencial para uma gestão eficiente. Ela sintetiza o resultado das informações levantadas no mapeamento dos processos e na identificação e avaliação dos riscos e controles, tornando-se base para a definição de planos de ação para mitigação dos riscos.

Complementarmente, a avaliação do risco legal é realizada de forma contínua na Instituição, sendo que a área Jurídica é envolvida em diversos momentos, seja durante o processo de estudo e desenvolvimento de novos produtos / serviços, seja na formatação dos contratos e nas avaliações do risco legal envolvido.

- **Resposta ao Risco Residual:** Para todo risco residual é indicada a definição de um Plano de Ação para mitiga-lo, o qual pode ser classificado como:

  - ***Ação de Monitoramento***: ações que visam acompanhar o risco e sua evolução, utilizada para exposição a riscos residuais classificados como "muito baixo" e "baixo";

  - ***Ação de Gestor***: ações tomadas com o objetivo de manter o risco sob controle, utilizada para exposição a riscos residuais "médios";

  - ***Ação de Prioridade***: ações tomadas com maior brevidade e/ou de imediato evitando que o risco se concretize ou aumente, podendo expor a Instituição. Utilizada para exposição a riscos residuais "altos" e "muito altos".

As estratégias adotadas para implementar uma ação devem estar de acordo com a relação entre o nível de risco identificado e o aceitável e poderão ser de evitar, reduzir, transferir ou aceitar o risco.

- **Planos de Ação para Mitigação do Risco:** como estratégia da Instituição, decidiu-se pela não aceitação dos riscos residuais "altos" e "muito altos". Para estas exposições, que extrapolam o apetite definido pelo Mercantil, planos de ação são adotados visando reduzi-las a um nível aceitável. Os responsáveis pelos processos devem definir prazos para implementação dos planos de ação, os quais são monitorados pela equipe de Gerenciamento do Risco Operacional, sendo posteriormente averiguada sua efetividade na mitigação do risco que a originou. As ações relativas a deficiências de controles também são monitoradas para que possam ser avaliadas e sua implementação seja refletida no risco residual.

As ações com o referido grau de risco também são classificadas de acordo com o nível de impacto / relevância para a Instituição e podem ser acompanhadas pelo CCCI – Comitê de *Compliance* e Controles Internos. Casos de exceção podem ocorrer se o custo do controle sobrepor seu benefício, sendo essa avaliação foco de discussão entre os gestores responsáveis e equipe de riscos, podendo requerer a aprovação da Diretoria responsável em conjunto com o CRO.

6.2. Etapa Quantitativa

- **Monitoramento da Base de Perdas Operacionais:** a Base de Perdas Operacionais tem como objetivo registrar as informações relativas aos eventos decorrentes da exposição ao risco operacional, provendo o Grupo Mercantil de informações consistentes, padronizadas e atualizadas. No Sistema ROP – Base de Perdas Operacionais Internas são registrados os eventos de perdas operacionais que impactaram a Instituição, constituído por duas bases: gerencial e contábil.

  - **Base gerencial**: contempla os eventos de perdas operacionais identificados pelas áreas ou incluídos em sistemas operacionais do Mercantil. Possui detalhamento sobre a causa raiz da perda e uma série de informações adicionais, que permitem avaliações mais qualificadas para o adequado gerenciamento do risco operacional.

  - **Base contábil**: contempla as principais contas contábeis com os dados de perdas operacionais e provisões relacionadas. Possui a movimentação analítica das contas contábeis de despesa sem, porém, possuir detalhamento das causas.

A utilização de ambas as bases possibilita a melhor gestão das perdas operacionais, bem como a comparação de dados e avaliações complementares a fim de garantir a integridade, critérios de abrangência, consistência e confiabilidade das informações prestadas. Vale ressaltar que a Instituição não adotou ponto de corte, permitindo maior granularidade da base gerencial.

- **Identificação das Causas Raízes das Perdas Operacionais:** a partir da análise da Base de Perdas Operacionais é possível identificar os motivos das perdas mais representativas e suas causas raízes. Isso permite que ações sejam implantadas para o controle da exposição ao risco operacional.

A análise da evolução das perdas e/ou de indicadores relativos ao ambiente de negócios e aos controles internos, possibilita uma visão crítica das etapas qualitativas e quantitativas conduzindo a uma retroalimentação de todo o ciclo de gestão.

Ressalta-se que a base gerencial é viva e mutável: as áreas relatantes de perdas operacionais internas podem efetuar a correção de informações inseridas no ROP, sendo observados os critérios e os procedimentos definidos quanto a alteração de dados dentro e fora da competência em aberto no sistema. Para competência fechada, deve-se justificar e documentar o pedido de alteração via demanda ou SAMB. Como consequência, análises de períodos anteriores podem sofrer modificações para melhor registro.

- **Planos de Ação para Mitigação do Risco:** para perdas operacionais mais relevantes ou que tenham ultrapassado níveis de tolerância definidos via indicadores, é realizado um trabalho compartilhado com os gestores responsáveis pelos processos a fim de definir planos de ação para atuação nas causas raízes e redução do nível de perdas. Estes planos de ação são acompanhados e as perdas monitoradas com o objetivo de garantir a mitigação das exposições a riscos operacionais. Aqueles classificados com alto grau de impacto / relevância também são acompanhados pela Alta Administração.

6.3. Gestão de Terceiros Relevantes

Para fins da aplicação da Resolução CMN nº. 4.557/17, CMN nº 4.893/21 e Lei 13.709/2018 - LGPD, entende-se por "terceiro relevante" aquele prestador de serviço cuja atividade profissional, dada a sua relevância e imprescindibilidade, constitui elemento essencial para a organização e que, se malconduzida e/ou não fiscalizada de forma adequada, pode trazer riscos sistêmicos de alto custo para a organização.

O Banco Mercantil possui procedimentos definidos para Gestão de Terceiros Relevantes, divulgados internamente e sendo objeto de monitoramento. Desta forma, na avaliação da relevância de um terceiro, o processo de Gestão de Terceiros Relevantes considera os seguintes aspectos:

- Interrupção, falhas, erros significativos ou lapso de controles com impacto operacional e financeiro, podendo expor a entidade a riscos graves, afetar o atendimento aos clientes e comprometer fortemente a estratégia e o resultado da Instituição;

- Dependência do terceiro para o cumprimento das obrigações regulatórias e execução de processos com impacto no atendimento aos clientes;

- Os serviços não podem ser transferidos para outro terceiro sem um esforço demorado e/ou oneroso;

- O terceiro necessita ter acesso a dados restritos e informações confidenciais do Mercantil ou realizar o tratamento de dados pessoais de clientes e/ou funcionários do Mercantil;

- O terceiro fará uso de infraestrutura tecnológica de nuvem para armazenamento ou processamento de dados.

Em resumo, o terceiro é classificado como relevante com base em risco envolvido e a avaliação dos aspectos mencionados acima se dá através das respostas obtidas de questionário de segmentação aplicado durante o processo de cadastro. De acordo com o peso resultante, o terceiro é classificado ou não como relevante. São considerados terceiros relevantes as empresas classificadas nos tiers 1 e 2 (Muito Alto e Alto).

Tier	Descrição
Muito Alto	- Afeta catastroficamente os serviços prestados pelo Mercantil, caracterizando-se por eventos relevantes que comprometem fortemente a estratégia e o resultado da Instituição. - Processos do terceiro/fornecedor e da Instituição são altamente integrados. - Instituição altamente dependente do terceiro/fornecedor para o cumprimento das obrigações regulatórias e execução de processos, com elevado impacto no atendimento aos clientes. - Interrupção, falha, erros significativos ou lapso de controles teriam um impacto operacional e financeiro significativo e pode expor a entidade a riscos graves. - Os serviços não podem ser transferidos para outro fornecedor sem um esforço extremamente demorado e / ou oneroso - O terceiro necessita ter acesso a dados restritos e informações confidenciais do Mercantil ou realizar o tratamento de dados pessoais de clientes e/ou funcionários do Mercantil. - O terceiro fará uso de infraestrutura tecnológica de nuvem para armazenamento ou processamento de dados.

Alto	- Afeta significativamente os serviços prestados pelo Mercantil, caracterizando-se por eventos relevantes que comprometem moderadamente a estratégia e o resultado da Instituição. - Processos do terceiro/fornecedor e da Instituição são pouco integrados. -Instituição com moderada dependência do terceiro/fornecedor para o cumprimento das obrigações regulatórias e execução de processos, com moderado impacto no atendimento aos clientes. -Interrupção, falha, erros significativos ou lapso nos controles teriam um impacto operacional e financeiro moderado e aumento na exposição ao risco. - Os serviços não podem ser transferidos para outro fornecedor sem esforço demorado e / ou oneroso. - O terceiro necessita ter acesso a dados restritos e informações confidenciais do Mercantil ou realizar o tratamento de dados pessoais de clientes e/ou funcionários do Mercantil. - O terceiro fará uso de infraestrutura tecnológica de nuvem para armazenamento ou processamento de dados.
Médio	- Afeta moderadamente os serviços prestados pelo Mercantil e compromete pouco a estratégia e o resultado da Instituição. - Processos do terceiro/fornecedor e da Instituição podem ser integrados. - Instituição com pouca dependência do terceiro/fornecedor para o cumprimento das obrigações regulatórias e execução de processos, com pouco impacto no atendimento aos clientes. - Falhas nos controles dos terceiros/fornecedores resulta em limitado impacto operacional, financeiro e exposição ao risco. - Os serviços podem ser transferidos para outro fornecedor com um esforço mínimo a moderado.
Baixo	- Afeta pouco os serviços prestados pelo Mercantil e pode impactar a estratégia e o resultado da Instituição. - Processos do terceiro/fornecedor e da Instituição não estão integrados. - O relacionamento é completamente baseado no custo e desempenho do fornecedor. - Falhas nos controles dos terceiros/fornecedores resulta em pequeno impacto operacional, financeiro e exposição ao risco. - Os serviços podem ser transferidos para outro fornecedor com esforço mínimo.
Muito Baixo	- Não causam danos e prejuízos aos clientes e nem afetam a estratégia e o resultado da Instituição. - Processos do terceiro/fornecedor e da Instituição não estão integrados. - O relacionamento é completamente baseado no custo e desempenho do fornecedor. - Falhas nos controles não teriam consequência operacionais, financeiras ou de risco. - Os serviços podem ser facilmente transferidos para outro fornecedor.

O processo de gestão de terceiros é direcionado pelo risco envolvido na atividade. Para os terceiros considerados críticos ou relevantes, foram definidos processos padronizados que contemplam:

- Segmentação por meio da classificação dos terceiros com base em risco;
- Contratação avaliando critérios de decisão e riscos envolvidos;
- Monitoramento e gerenciamento dos terceiros relevantes;
- Desligamento.

A descrição da metodologia encontra-se detalhada no Procedimento de Gestão de Terceiros Relevantes, disponível como documento vinculado a essa política.

6.4. Risco Operacional: Apoio na decisão de Investimentos

Anualmente é realizado o orçamento dos investimentos de TI e de Infraestrutura a fim de definir quais recursos serão investidos visando o atendimento dos objetivos estratégicos da Instituição. A Gerência de Risco Operacional e Controles Internos participa deste processo entendendo a natureza e objetivo de cada projeto / investimento, realizando a identificação de riscos e levantando o nível de criticidade. Após entendimento, é emitido um parecer associado a necessidade e priorização do investimento com base no risco apresentado. Este reporte é apresentado ao CEO e CFO do Banco Mercantil para tomada de decisão.

Mensalmente, é realizado o monitoramento da execução dos investimentos juntamente com a Gerência de FP&A e demais áreas envolvidas para entendimento do que foi realizado e também se certificar sobre a implementação de ações que visem melhorias no ambiente de controle.

7. REPORTES

O monitoramento do risco operacional é suportado por relatórios gerenciais com o objetivo de suprir os gestores e a Alta Administração com informações que sinalizem os aspectos qualitativos e quantitativos da exposição ao risco operacional da Instituição e as ações para a sua mitigação:

- ***Relatório de Gerenciamento do Risco Operacional e da Continuidade de Negócios***: possui periodicidade trimestral e contempla todo o ciclo de gestão do Risco Operacional, demonstrando a avaliação das exposições a riscos e das perdas operacionais, o impacto resultante, a análise de variação sobre as principais flutuações de saldo em cada categoria de perda, bem como a análise das causas raízes das perdas operacionais e as ações em andamento ou concluídas para a sua mitigação. Apresenta ainda a visão dos indicadores constantes na RAS e os ICR's demonstrando o desempenho dos indicadores ao longo do ano, bem como ações para tolerâncias ultrapassadas. Contempla também a gestão de Terceiros Relevantes e reportes sobre incidentes internos e externos. Neste relatório também são reportadas informações consideradas relevantes, durante o período de referência, que podem causar algum impacto na gestão do Risco Operacional para a Instituição.

- ***Painel de ICR's***: possui periodicidade mensal e apresenta uma visão do resultado dos ICR's monitorados, análises específicas de cada indicador e o acompanhamento das ações definidas quando as tolerâncias dos índices são ultrapassadas.

- ***Resumo Executivo de Riscos Operacionais:*** ao final das atividades de mapeamento de processos críticos e identificação e avaliação de riscos, a Gerência de Risco Operacional e Controles Internos reporta o resultado do trabalho realizado junto aos gestores e diretor responsáveis pelo processo, apresentando o mapa dos riscos e controles identificados, a avaliação, o risco residual, deficiências de controles diagnosticadas bem como sugestões de melhorias que irão auxiliar na construção de Planos de Ação para mitigação dos riscos classificados como Altos ou Muito Altos. Importante ressaltar a vinculação do mapa de riscos à decisão de investimentos da Instituição, embasando de forma objetiva sua real necessidade.

Além do envio dos reportes periódicos à Alta Administração e gestores relacionados com o tema, BI's foram desenvolvidos para suprir a necessidade de informação em um formato de fácil acesso e que facilita o fluxo de tomada de decisão.

8. APURAÇÃO DO REQUERIMENTO DE CAPITAL PARA RISCO OPERACIONAL

Os requisitos mínimos de Nível I e de Capital Principal a serem mantidos pelas instituições consideram a relação entre o capital disponível em cada nível e a exposição dos ativos ponderados ao risco (RWA), os quais consistem da soma de três parcelas, cada uma delas relativa a uma natureza de risco – sendo uma delas, a exposição ao risco operacional (RWAOPAD):

$$RWA = \underset{\textit{Risco de Crédito (RC)}}{RWACPAD} + \underset{\textit{Risco de Mercado (RM)}}{RWAMPAD} + \underset{\textit{Risco Operacional (RO)}}{RWAOPAD}.$$

No Grupo Mercantil, o cálculo da parcela do RWAOPAD adota a metodologia de Abordagem Padronizada Alternativa Simplificada.

9. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades atinentes a esta Política estão distribuídos entre as alçadas abaixo indicadas:

- Conselho de Administração
- Comitê de Auditoria
- CEO, Vice-Presidências e Diretorias
- Comitê de Riscos
- Diretoria de Riscos e Compliance – CRO (Chief Risk Officer)
- Gerência de Risco Operacional e Controles Internos
- Áreas de Suporte
- Áreas de Validação
- Terceiros Relevantes
    - Cumprir as diretrizes e cláusulas contratuais acordadas entre as partes;
    - Gerenciar seus próprios riscos no que diz respeito a questões operacionais, fiscais, trabalhistas, socioambientais, dentre outros;
    - Assegurar, nos casos de greve, paralisação ou indisponibilidade, a continuidade da prestação dos serviços;
    - Comunicar a área responsável pelo terceiro qualquer tipo de incidente que possa ocasionar problemas na prestação de serviços;
    - Assegurar a adequada capacitação dos prestadores de serviços sobre os riscos operacionais das entregas e/ou dos processos executados de forma complementar ao Mercantil.

10. CONSIDERAÇÕES FINAIS

Esta Política deve ser objeto de avaliação periódica com o intuito de que seja continuamente aprimorada e de esteja sempre atualizada.

Este documento entra em vigor a partir de sua publicação, ficando à disposição dos órgãos de fiscalização e supervisão.

BANCO MERCANTIL