GRUPO MERCANTIL

Política de Gerenciamento do Risco Operacional

Vigência a partir de: 23/01/2026
Validade: 1 ano
Versão: 03

Sumário

Divulgação Externa

1. APRESENTAÇÃO

A Política Institucional de Gerenciamento do Risco Operacional do Grupo Mercantil foi elaborada com base nas diretrizes do Conselho Monetário Nacional que, por intermédio da Resolução nº. 4.557/17, alterada pelas Resoluções nºs. 4.745/19, 4.926/21, 4.943/21, 5.076/23 e a Resolução nº. 356/23, dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

De acordo com o 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 Grupo Mercantil, bem como sanções em razão do descumprimento de dispositivos legais e a indenização por danos a terceiros decorrentes das atividades desenvolvidas pela Instituição.

2. 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 empresas do Grupo Mercantil.

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.

Neste contexto, destaca-se que o gerenciamento prevê procedimentos e critérios de decisão quanto à gestão de terceiros relevantes, bem como alocação de recursos para este fim, além de estrutura focada no gerenciamento de riscos de sistemas, processos e infraestrutura de TI.

2.1. Apetite ao Risco Operacional

O Apetite ao Risco Operacional estabelece os tipos e níveis de risco que a Instituição se dispõe a admitir na realização dos seus negócios e na busca por alcançar seus objetivos estratégicos. Tal apetite é definido pela Alta Administração e formalizado na Declaração de Apetite por Riscos (RAS – Risk Appetite Statement), documento aprovado pelo Conselho de Administração que está alinhado à estratégia da organização.

Diante do elevado volume de atividades, operações e transações realizadas, é natural que sejam incorridas perdas operacionais. A estratégia de Gerenciamento do Risco Operacional prevê o monitoramento contínuo da exposição aos riscos, assegurando que as perdas decorrentes de falhas, deficiências ou inadequação de processos internos, pessoas e sistemas, bem como de eventos externos, permaneçam dentro dos limites definidos na RAS. Para tal, são utilizados os seguintes mecanismos:

Monitoramento de Perdas: O acompanhamento abrange o valor das perdas operacionais internas (cíveis, trabalhistas, fraudes, entre outras), constantes de uma Base de Perdas Operacional, mensuradas tanto em termos nominais quanto relativizados em relação a parâmetros de negócio, como quantidade de clientes, receitas e despesas da Instituição, considerando aspectos qualitativos sobre sua originação e causas-raízes.

Monitoramento de Tecnologia e Segurança: A gestão contempla indicadores que mensuram a disponibilidade de serviços críticos, o tempo médio para recuperação e aspectos sobre segurança cibernética, em alinhamento com a RAS.

2.2. 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 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 de desenho e efetividade) - 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;

Divulgação Externa

- **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 dos processos e à Alta Administração através de relatórios que sinalizam os aspectos qualitativos e quantitativos da exposição a risco operacional da Instituição.

Diagrama 1 – Ações de Gestão

3. METODOLOGIA APLICADA

Baseado nos direcionamentos e orientações do COSO ERM, 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.

Divulgação Externa

Diagrama 2 - Metodologia Aplicada

3.1. Gestão das Perdas Operacionais

3.1.1. Etapa Qualitativa

A etapa qualitativa compreende as seguintes atividades:

a) **Levantamento dos Processos Críticos**: os mapeamentos dos processos considerados críticos do Grupo Mercantil são priorizados. Para a classificação de criticidade e priorização das atividades, foram estabelecidos os seguintes critérios: materialidade financeira relacionada ao processo, histórico de perdas operacionais, exigência regulamentar e aspectos relevantes na visão da Alta Administração, esta última capturada por meio de entrevistas com seus principais executivos. A avaliação destes critérios, bem como dos processos considerados críticos, é realizada anualmente e aprovada pela CRO - *Chief Risk Officer*, a fim de assegurar que novos processos ou alterações sejam contempladas.

b) **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.

c) **Identificação dos Riscos e Categorização**: a fase subsequente compreende a identificação das exposições a eventos de risco operacional. Os eventos de risco operacional são categorizados em conformidade com a resolução vigente, conforme detalhado a seguir:

- Fraudes internas;

Divulgação Externa

- Fraudes externas;
- 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 conduzida em conjunto com o gestor, que detém conhecimento aprofundado e a responsabilidade pelo processo, considerando a probabilidade de ocorrência do risco e seu impacto caso se materialize. São considerados cinco níveis de risco: "muito baixo", "baixo", "médio", "alto" e "muito alto" conforme parâmetros estabelecidos na metodologia.

Para avaliação, são observados os seguintes balizadores:

Probabilidade	Impacto
• Frequência de execução do processo (volume de transações); • Materialidade dos riscos; • Capital intelectual/recursos humanos (treinamento, expertise, qualificação); • Normas e procedimentos (existência, aderência).	• Financeiro; • Reputacional; • Regulatório; • Estrutural/processual; • Privacidade/ LGPD; • Ambiente Tecnológico.

Ressalta-se que, para riscos relativos a processos de tecnologia, são ainda considerados na avaliação do grau de probabilidade os seguintes parâmetros:

- Quantidade de incidentes de segurança da informação e;
- Disponibilidade do ambiente.

E para o impacto:

- Disponibilidade do ambiente.

d) **Identificação e Classificação dos Controles**: um efetivo sistema de controles internos reduz a probabilidade de erros humanos e irregularidades em processos e sistemas,

Divulgação Externa

resultando na diminuição das perdas operacionais. Os controles podem ser classificados por 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.

e) **Avaliação dos Controles:** para avaliação dos controles, utilizam-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 se está em efetivo funcionamento. De acordo com sua eficácia na 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, alternativamente, detectar a não conformidade para que seja solucionada. O escopo do teste de desenho é mais restrito e limitado, avaliando 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, conforme esperado em sua modelagem. O escopo do teste de efetividade tem amplitude maior, avaliando se o controle está mitigando o fator de risco.

Nesta fase, também é avaliada a qualidade dos controles, de acordo com o resultado dos testes, além de suas características e do seu contexto no processo, podendo estes serem classificados como "inefetivos" ou "efetivos". Para se concluir sobre o nível de efetividade do controle e a 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, aos quais a Instituição está exposta, sejam conhecidos e reproduzam a realidade.

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

f) **Avaliação dos Riscos Residuais - Matriz de Riscos:** a avaliação de riscos é realizada em conjunto com o gestor, em relação à probabilidade de ocorrência do risco (de muito baixo a muito alto, conforme descrito acima) e seu impacto em relação às dimensões das categorias de risco, caso se materialize. A 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 inerente, 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 do avaliador. 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.

Divulgação Externa

g) **Planos de Ação para Mitigação do Risco e Resposta ao Risco Residual**: Para todo risco residual é indicada a definição de um Plano de Ação para mitigá-lo, o qual pode ser classificado como:

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

- Ação de Gestão: tem como objetivo 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 a um risco acima do apetite definido. Utilizada para exposição a riscos residuais "altos" e "muito altos".

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 estratégias adotadas para implementar uma ação devem estar de acordo com a relação entre o nível de risco identificado e o apetite, e poderão ser no sentido de evitar, reduzir, transferir ou aceitar o risco.

As ações relativas a deficiências de controles também são monitoradas para que possam ser avaliadas e sua implementação seja refletida no risco residual. Para este monitoramento são definidos prazos de acordo com o grau de criticidade do risco residual. Neste contexto, ressalta-se que é avaliado o custo x benefício da implementação do controle em relação ao risco apresentado.

As ações também são classificadas de acordo com o nível de impacto / relevância para a Instituição e podem ser acompanhadas pelo Comitê de Compliance, Controles Internos e Gestão de Perdas. A assunção de risco pode ocorrer caso o custo do controle sobreponha seu benefício, ou caso se tratar de um posicionamento estratégico da Instituição, sendo essa avaliação foco de discussão colegiada entre os membros do referido Comitê e os gestores responsáveis, devendo a decisão ser tomada juntamente à Diretoria responsável e o CRO.

h) **Monitoramento do perfil de risco e exposições**: há um acompanhamento contínuo dos trabalhos realizados pela Auditoria Externa, Auditoria Interna, Prevenção a Fraudes, Compliance e pelas demais áreas de 2ª linha, responsáveis pela gestão corporativa dos riscos da Instituição, com o objetivo de verificar as conclusões e acompanhar eventuais deficiências de controles, os respectivos planos de ação e a exposição aos riscos correspondentes.

3.1.2. Etapa Quantitativa

A etapa quantitativa consiste na mensuração e análise das perdas operacionais, com o objetivo de prover informações consistentes para a gestão de riscos e subsidiar a implementação de ações de mitigação.

a) **Monitoramento da Base de Perdas Operacionais:** A consolidação dos eventos de perda operacional ocorre mensalmente no sistema centralizador ROP (Base de Perdas

Divulgação Externa

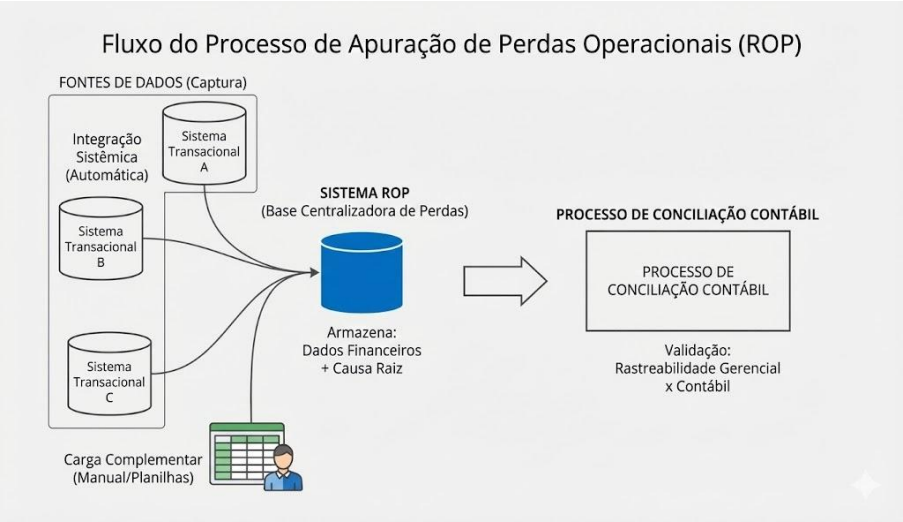
Operacionais Internas). O processo de alimentação desta base é estruturado de forma a garantir a captura abrangente dos eventos via:

- **Integração Sistêmica (Fluxo Principal):** A maior parte dos registros é capturada automaticamente via integração com os sistemas transacionais legados (ex: Sistemas SIC, Benner, Oracle) que processam movimentações financeiras e despesas caracterizadas como perdas operacionais.

- **Carga Complementar (Fluxo Manual):** Eventos não capturados pelos sistemas principais são registrados diretamente pelas áreas internas responsáveis, por meio de interfaces manuais ou importação padronizada (ex: planilhas).

É importante ressaltar que, independentemente de sua origem (sistêmica ou manual), todos os registros inseridos no ROP devem possuir rastreabilidade contábil.

O ROP armazena tanto as características financeiras quanto a causa raiz do evento. A rastreabilidade permite que os dados gerenciais do ROP sejam submetidos periodicamente ao processo de conciliação contábil, garantindo a integridade, consistência e confiabilidade das informações que subsidiarão as análises de causa e a definição de planos de ação preventivos.



Em casos de necessidade de ajustes da base faz-se necessário realizar a solicitação para que a equipe de Tecnologia realize a adequação.

b) Identificação das Causas Raízes das Perdas Operacionais: A análise da Base de Perdas Operacionais permite a identificação dos motivos e das causas raízes dos eventos mais representativos. Tal identificação é fundamental para o direcionamento de ações que visem 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 proporciona uma visão crítica das etapas qualitativas e quantitativas, resultando em uma retroalimentação de todo o ciclo de gestão.

c) Planos de Ação para Mitigação do Risco: Para eventos de perdas que sejam considerados relevantes ou que ultrapassem os níveis de tolerância definidos, são elaborados

Divulgação Externa

planos de ação em conjunto com os gestores dos processos. Tais planos são monitorados com o objetivo de garantir a efetiva mitigação da exposição aos riscos operacionais.

d) Elaboração de Projeções de Perdas: Realização de análise de cenários para identificar eventos que possam gerar impactos futuros relevantes, indicando a necessidade de controles, medidas de mitigação ou de capital adicionais, suportando assim, o processo orçamentário e o gerenciamento do capital.

3.2. 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 mal conduzida e/ou não fiscalizada de forma adequada, pode trazer riscos sistêmicos de alto custo para a organização.

O Grupo 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 são considerados os seguintes aspectos:

- Sustentação do core business: terceiros que, dada a sua relevância, constituem elemento essencial para o negócio.

- Tratamento de dados: relacionado a risco de privacidade em razão do volume e tipo de tratamento.

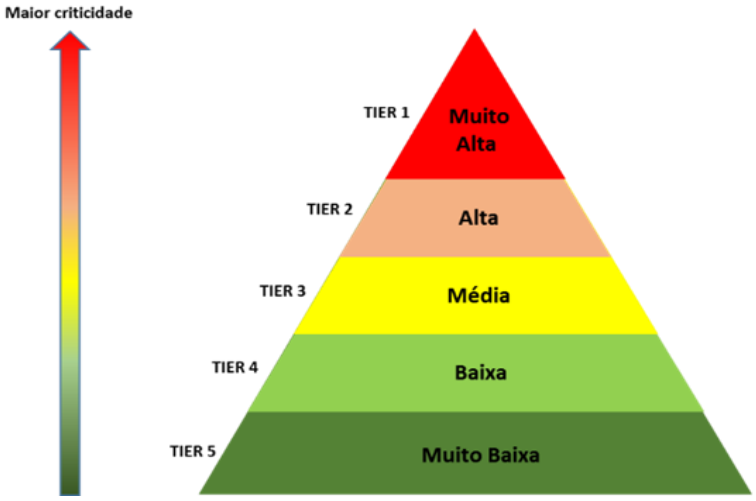
- Infraestrutura de TI: classificação do modelo de infraestrutura em que os dados e sistemas são mantidos (on premise ou nuvem)

- Tipo de acesso: estabelecimento do risco relacionado à conexão para garantir o acesso remoto seguro.

Em resumo, o terceiro é classificado como relevante com base no risco envolvido, e a avaliação dos aspectos mencionados é realizada por meio das respostas obtidas no 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 níveis 1 e 2 (Muito Alto e Alto).

Divulgação Externa

Parâmetros de Criticidade
Terceiros Relevantes



Descrição dos parâmetros de avaliação:

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 resultam 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 resultam 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:

1. Segmentação por meio da classificação dos terceiros com base em risco;

Divulgação Externa

2. Contratação avaliando critérios de decisão e riscos envolvidos;

3. Monitoramento e gerenciamento dos terceiros relevantes;

4. Desligamento.

A descrição da metodologia encontra-se detalhada no **Manual de Procedimento de Gestão de Terceiros Relevantes**, disponível como documento vinculado a essa política, destacando-se a diligência mais robusta e rigorosa para os terceiros de alto risco.

3.3. Risco Operacional: Avaliação na decisão de Investimentos

Anualmente, durante o processo de revisão orçamentária do Grupo Mercantil, é realizada a avaliação dos investimentos de Tecnologia e de Infraestrutura para o próximo ciclo visando tanto o atendimento dos objetivos estratégicos da Instituição sob a ótica de negócios, quanto à contribuição dos projetos para mitigação de riscos.
A Gerência de Risco Operacional e Controles Internos atua ativamente nesse processo indicando os riscos mais críticos - presente na matriz de riscos - e demais preocupações para que sejam definidos os investimentos necessários para sua mitigação. O parecer das equipes indica a priorização do investimento com base no risco apresentado, sendo sua inclusão na peça orçamentária e posterior execução da alçada do Comitê de Projetos.
Mensalmente, é realizado o monitoramento do nível de execução dos investimentos juntamente com a Gerência de FP&A, Gerência de Processamento e Monitoramento e demais áreas envolvidas, garantindo a implementação de ações que visem melhorias no ambiente de controles da organização.

3.4. Risco Operacional: Aspectos relacionados à Prevenção e Monitoramento de Fraudes

O Mercantil possui uma estrutura específica dedicada à gestão, monitoramento e suspeitas de fraude. A **Gerência de Prevenção a Fraudes** adota uma atuação abrangente e preventiva para a proteção integral da Instituição.

Estratégia de Prevenção: foca na criação de processos e estratégias de prevenção a fraudes dimensionadas de acordo com o risco de cada canal, produto e modelo de venda. Para isso, são utilizadas ferramentas robustas, tais como: Listas Internas e Externas (Uso da Base de Interoperabilidade da Resolução Conjunta n.º 6 do BACEN); Captura com Liveness (Coleta de selfies com prova de vida, reduzindo e mitigando o risco de DeepFake); Score de Biometria Facial e Facematch; Documentoscopia; Direcionamento para Mesa de validação quando o risco exigir intervenção humana; e por fim ferramentas de prevenção a fraude integradas ao nosso aplicativo. Essas ferramentas são cruciais para a avaliação de risco transacional e para a identificação proativa de possíveis tentativas de fraudes e golpes.

Também fazem parte da estratégia de prevenção da Instituição o mapeamento e análise dos eventos para a identificação de causas raízes de fraudes a fim de minimizar as perdas; o monitoramento ativo e contínuo dos processos internos de maior risco, com avaliação e implementação contínua de ações para antecipar e mitigar potenciais ameaças e; monitoramento ativo das contas dos nossos clientes correntistas com o objetivo de evitar a consumação de possíveis golpes antes que criminosos tenham êxito.

Prevenção e Investigação de Fraudes Internas: O Mercantil mantém uma estrutura dedicada focada em fraudes internas. Seu objetivo primário é proteger os ativos da

Divulgação Externa

organização e sua reputação, garantir um ambiente de trabalho ético e seguro, além de proporcionar uma resposta proativa e eficaz contra riscos financeiros e operacionais.

Inovação e Processos de Gestão: O processo de monitoramento é essencial para identificar e mapear riscos de forma proativa, compreender o comportamento de cada produto, bem como detectar variações que exijam ajustes imediatos nas regras, produtos, serviços ou fornecedores que atuam na prevenção a fraudes. Para isso, são realizados investimentos em ferramentas automatizadas, como as esteiras antifraude, que são cruciais na prevenção de perdas, incluindo os canais digitais (App Mercantil, Meu Mercantil, WhatsApp).

Reporte e Governança: As perdas decorrentes de fraudes, sejam elas externas ou internas, são contabilizadas na base de perdas operacionais do Grupo Mercantil. Estes dados são reportados à Alta Administração por meio de análises e indicadores. Adicionalmente, a Gerência de Prevenção a Fraudes utiliza dashboards de monitoramento para garantir uma atuação rápida e tempestiva nas ocorrências.

3.5. Risco Operacional: Gestão da Segurança da Informação

A gestão da segurança da informação, essencial para a mitigação do risco operacional, é realizada através da implementação e monitoração de um conjunto abrangente de diretrizes e controles. O Mercantil busca preservar a integridade, a confidencialidade e a disponibilidade de suas informações e dados. Todos os ativos de informação, classificados por importância e nível de proteção, são protegidos contra acesso, modificação, destruição ou divulgação não autorizados. As diretrizes incluem a adoção de controles para prevenir e detectar softwares maliciosos, o uso de criptografia, a garantia de que a segurança seja parte integrante do desenvolvimento de sistemas de informação, e a prevenção de acessos não autorizados. A proteção física das instalações e mídias de informação e o gerenciamento seguro das operações e comunicações também são premissas.

Além disso, o Mercantil possui uma **Política de Segurança da Informação** robusta que, além de nortear e contribuir com diretrizes, aborda a **Contingência e Continuidade de Negócios**. Isso envolve manter recursos e instalações de processamento de informações críticas em áreas seguras e protegidas contra interrupções, falhas ou desastres. Para assegurar a restauração do ambiente em tempo hábil, procedimentos de execução, retenção e salvaguarda de recursos são estabelecidos e periodicamente testados por meio de planos de simulação.

A Instituição garante, ainda, a conformidade com todos os requisitos legais e regulamentações pertinentes. A **Gerência de Segurança Cibernética e Informação** é a área responsável por elaborar, atualizar e gerenciar a política e seus manuais de procedimentos, assegurando a eficácia de todas as atividades de segurança.

4. 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

Divulgação Externa

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, além de uma visão resumida dos apontamentos/recomendações geradas. 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 que a vinculação do mapa de riscos à decisão de investimentos da Instituição, embasa de forma objetiva à 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.

5. APURAÇÃO DO REQUERIMENTO DE CAPITAL PARA RISCO OPERACIONAL

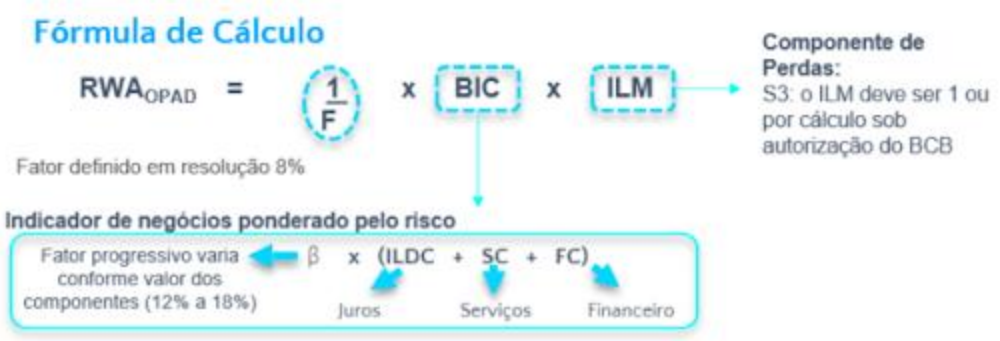
Os requisitos mínimos de Nível I e de Capital Principal a serem mantidos pelas instituições consideram a relação entre o capital disponível em cada nível e a exposição dos ativos ponderados ao risco (RWA), os quais consistem da soma de três parcelas, cada uma delas relativa a uma natureza de risco –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

$$RWA = RWACPAD + RWAMPAD + RWAOPAD.$$

Risco de Crédito (RC) Risco de Mercado (RM) Risco Operacional (RO)

Conforme prevê a Resolução BCB nº.356/2023, que estabelece os procedimentos para o cálculo da parcela dos ativos ponderados pelo risco (RWA) relativa ao cálculo do capital requerido para o risco operacional mediante abordagem padronizada (RWAOPAD), eliminou o uso de abordagens anteriores (BIA, ASA ou AMA) e tornou o novo modelo obrigatório para todas as Instituições Financeiras, sendo sua aplicação gradual de 2025 a 2028, conforme o calendário da norma.

Divulgação Externa



Em que:

I - F = fator estabelecido: hoje em 8%;

II - BIC = Indicador de Negócios Ponderado, conforme definido no art. 4º; e

É calculado levando-se em consideração a atividade operacional das Instituições, sendo sua fórmula:

BIC = BI (Business Indicator) x alíquota sobre o volume de negócios da Instituição

O Business Indicator, por sua vez, é composto por três blocos contábeis distintos: ILDC, SC e FC, que refletem com maior precisão o perfil de geração de valor e exposição operacional da instituição.

- O componente **ILDC** (*Interest, Leasing and Dividend Component*) abrange a margem financeira bruta, incluindo receitas e despesas com juros, receitas com arrendamento mercantil e dividendos.

- O componente **SC** (*Services Component*) captura a dimensão de serviços, refletindo comissões, tarifas, receitas com serviços prestados e despesas correlatas.

- O componente **FC** (*Financial Component*) considera os ganhos e perdas com ativos financeiros, incluindo operações de carteira bancária e carteira de negociação.

A nova abordagem introduz, também, o conceito de escalonamento de alíquotas aplicadas ao Business Indicator, criando faixas progressivas de capital requerido conforme o volume de negócios da instituição.

A estrutura de alíquotas funciona da seguinte forma: para instituições com BI de até R$ 5 bilhões, se aplica uma alíquota de 12%, para as instituições com BI entre R$ 5 bilhões e R$ 150 bilhões, se aplica uma alíquota de 15%, e ainda para instituições com BI superior a R$ 150 bilhões, se aplica uma alíquota de 18%.

No caso do Mercantil, a alíquota aplicável é de 12%.

III - ILM = Multiplicador de Perdas Internas, conforme definido no art. 10.
O ILM é um fator multiplicador aplicado ao componente principal de capital (BIC) e é calculado com base no total de perdas operacionais líquidas incorridas pela instituição nos últimos dez

Divulgação Externa

anos, ponderadas segundo uma fórmula logarítmica calibrada para evitar distorções extremas.

O funcionamento do ILM estabelece que, quando as perdas históricas são iguais ao BIC, o ILM será igual a 1 (capital neutro), e que quando as perdas históricas forem maiores que o BIC, o ILM será superior a 1, aumentando o capital exigido, e ainda quando as perdas forem menores que o BIC, o ILM será inferior a 1, reduzindo o capital exigido.

Importante ressaltar, que para Instituições enquadradas no segmento S3 ou S4 o ILM é igual a 1 (neutro), ou poderá ser calculado na forma do disposto nos arts. 10 e 11 da Resolução BCB nº356, condicionado à prévia autorização do Banco Central do Brasil. Entretanto, a partir do exercício da opção pelo cálculo do ILM, após autorizado pelo Banco Central do Brasil, a mudança será irrevogável.

Implantação da nova resolução:

A nova abordagem estabelece um cronograma de faseamento da implementação, visando mitigar impactos abruptos sobre o capital regulatório e permitir uma transição gradual e controlada. A Resolução BCB nº 356 prevê que de 2025 a 2028, a diferença entre o capital calculado pela nova metodologia e o capital exigido segundo a metodologia anterior (BIA/ASA) será aplicada de forma escalonada: em 2025, se aplica 25% da diferença, em 2026, se aplica-se 50% da diferença, em 2027 se aplica 75% da diferença, e finalmente em 2028, se aplica 100% da diferença, com adoção integral da nova metodologia.

A realização do cálculo do RWAOpad é semestral e é de responsabilidade da Gerência de Risco Operacional e Controles Internos.

6. PAPÉIS E RESPONSABILIDADES

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

- Conselho de Administração ou Diretoria
- 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

A estrutura de Gerenciamento do Risco Operacional prevê uma atuação compartilhada do gestor responsável pelo Terceiro Relevante e da equipe de Risco Operacional. De acordo o procedimento adotado pelo Mercantil é de responsabilidade do terceiro relevante:

Divulgação Externa

- 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.

7. CONSIDERAÇÕES FINAIS

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

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

8. REFERÊNCIAS NORMATIVAS

Tipo	Número/Ano	Objetivo
Resolução CMN	4.557/2017 (alterada pelas resoluções 4.745/2019, 4.926/2021, 4.943/2021, 5.076/2023, 5.077/2023, 5.089/2023, 5.187/2024)	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.

Divulgação Externa

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	5.076/2023	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, e a Resolução nº 4.606, de 19 de outubro de 2017.
Resolução CMN	356/2023 (alterada pela resolução 447/2024)	Estabelece os procedimentos para o cálculo da parcela dos ativos ponderados pelo risco (RWA) relativa ao cálculo do capital requerido para o risco operacional mediante abordagem padronizada (RWAOPAD), de que tratam a Resolução CMN nº 4.958, de 21 de outubro de 2021, e a Resolução BCB nº 200, de 11 de março de 2022.

9. GLOSSÁRIO

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

Divulgação Externa

–ABRANGÊNCIA–

Esta Política abrange a(s) seguinte(s) empresa(s) do Grupo Mercantil[1]:

Banco Mercantil de Investimentos S.A.; Banco Mercantil do Brasil S.A.; Bem Aqui - Administradora e Correta de Seguros, Previdência Privada e Correspondente Bancário S.A.; Domo - Digital Tecnologia S.A.; MBMKTP - Mercantil do Brasil Marketplace e Empreendimentos Imobiliários S.A.; Mercantil do Brasil Corretora S.A. - Câmbio, Títulos e Valores Mobiliários; Mercantil do Brasil Distribuidora S.A. - Títulos e Valores Mobiliários; Mercantil Financeira S.A. - Sociedade de Crédito, Financiamento e Investimento

A ciência e o cumprimento das diretrizes e regras deste normativo são obrigatórios a:

Terceiros (fornecedores, prestadores de serviços, parceiros de negócio, agentes intermediários e associados, donatários, patrocinados, acionistas e demais terceiros) das empresas do Mercantil acima citadas; Todos os colaboradores das empresas do Mercantil acima citadas (administradores, empregados e estagiários, independentemente de cargo ou função exercidos)

-

[1] Empresas que compõem o Grupo Mercantil:
Empresas operacionais: MB+, BMI, MC, MD, MF, Domo, Bem Aqui, MBMKTP
Empresas não operacionais: Sansa, Macs, Cosefi, e Fundos MB BI e MB FII.