



Política de Resiliência Operacional

Vigência a partir de: 02/07/2026
Validade: 1 ano
Versão: 03

Sumário

1. APRESENTAÇÃO.....	2
2. DIRETRIZES E PRINCÍPIOS DE RESILIÊNCIA	3
2.1. Arcabouço de Resiliência	3
2.2. Gestão da Continuidade dos Negócios.....	4
2.2.1. Cenários de Interrupção.....	5
2.2.2. Metodologia aplicada à Gestão de Continuidade dos Negócios.....	6
2.3. Continuidade nos Pontos de Atendimento.....	8
2.4. Continuidade dos Serviços de Tecnologia e Cyber.....	8
2.5. Gerenciamento de Incidentes e Crises	9
2.6. Comunicação com Órgãos Reguladores e Fiscalizadores	9
3. PAPÉIS E RESPONSABILIDADES.....	10
4. CONSIDERAÇÕES FINAIS	11
5. REFERÊNCIAS NORMATIVAS.....	11
6. GLOSSÁRIO	12

1. APRESENTAÇÃO

A resiliência operacional é a capacidade de uma organização de antecipar, absorver, adaptar-se e recuperar-se rapidamente de interrupções inesperadas. Ela garante a continuidade dos serviços essenciais, protegendo pessoas, processos, tecnologia e resultados financeiros contra crises ou imprevistos.

Para além de continuidade do negócio, o conceito de resiliência foca em quatro pilares principais:

- Antecipação: identificar vulnerabilidades e riscos potenciais antes que eles causem danos reais;
- Absorção: resistir a choques e interrupções, minimizando o impacto imediato nas operações;
- Adaptação: ajustar rapidamente processos e estratégias para manter o funcionamento da empresa em cenários adversos; e
- Recuperação: restabelecer a normalidade e aprender com o incidente para fortalecer o negócio no futuro

A presente Política de Resiliência Operacional do Grupo Mercantil foi elaborada em conformidade com as diretrizes de gerenciamento de riscos, capital e divulgação de informações estabelecidas pelos órgãos reguladores vigentes, sendo aplicável conforme definido no item "Abrangência" deste documento.

Esta Política tem como alicerce, sem se limitar a eles, os seguintes normativos, sendo sua aplicação extensiva conforme definido no item "Abrangência":

- Conselho Monetário Nacional (CMN) e Banco Central do Brasil (Bacen):
- Resolução CMN nº 4.557/2017 (e suas alterações pelas Resoluções nº 4.745/19, 4.926/21 e 4.943/21): Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital;
- Resolução CMN nº 4.968/2021: Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil;
- Resolução CMN nº 4.893/2021 (e suas alterações pela Resolução Bacen nº 5.274/2025): Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.
- Comissão de Valores Mobiliários (CVM) e B3:

- Resoluções CVM nº 21, 32, 33 e 35 (2021): Normatiza a intermediação, monitoramento e o fluxo de reporte tempestivo de incidentes relevantes em mercados de valores mobiliários;
- B3: Programa de Qualificação Operacional (PQO) – Roteiro Operacional (Item 131).

Ressalta-se que a aplicação desta Política deve observar a vigência e as eventuais atualizações dos normativos supracitados, garantindo o alinhamento contínuo às exigências regulatórias.

2. DIRETRIZES E PRINCÍPIOS DE RESILIÊNCIA

Em conformidade com a regulamentação vigente, a estratégia de Resiliência Operacional do Grupo Mercantil fundamenta-se na manutenção de um ciclo contínuo de identificação de processos críticos e avaliação de impactos operacionais. Esta abordagem assegura a elaboração e a manutenção de planos de contingência robustos, cuja eficácia é validada periodicamente por meio de um programa de testes, garantindo a resiliência da instituição frente a eventuais interrupções.

Para suportar essas diretrizes, o Grupo adota uma estrutura de governança ágil e integrada, desenhada para favorecer a tomada de decisão rápida e minimizar impactos de incidentes. A responsabilidade pela execução e supervisão deste tema é compartilhada de maneira estratégica entre áreas chaves, garantindo sinergia e cobertura de todos os riscos.

Neste modelo de governança, a Diretoria Executiva de Riscos e Compliance atua na gestão macro da continuidade dos Negócios, sob a ótica das diretrizes corporativas. De forma complementar, a Diretoria de Operações e Eficiência em Processos, lidera a estratégia voltada para a continuidade dos Pontos de Atendimento, enquanto a Vice-Presidência de Produtos, Tecnologia e Serviços assegura a continuidade dos Serviços de Tecnologia.

Dada a complexidade e a interconexão dos temas, as áreas mencionadas neste documento atuam como co-responsáveis pela governança macro da Resiliência e Continuidade das Operações. Compete a cada uma delas garantir o monitoramento contínuo de seus respectivos processos, formalizando os procedimentos contemplados no escopo de gestão da continuidade dos negócios por intermédio dos Planos de Contingência e demais normativos, os quais devem ser aprovados pelos gestores internos, seguindo os critérios técnicos definidos por meio de Manuais de Procedimentos específicos e em consonância com as diretrizes desta Política.

2.1. Arcabouço de Resiliência

O arcabouço de Resiliência Operacional do Grupo Mercantil é fundamentado em quatro frentes estratégicas que integram as esferas de Negócios, Atendimento, Tecnologia e Cyber sob a governança centralizada do time de Gestão da Continuidade dos Negócios, visando garantir a antecipação de ameaças, a proteção do perímetro corporativo físico e lógico, resistir e absorver choques operacionais, e recuperar de forma tempestiva suas operações críticas perante cenários críticos.

Essa estrutura organiza-se por meio de cenários transversais e pilares de atuação setorial. No âmbito transversal, o ecossistema engloba as diretrizes macro da organização através do Plano de Gestão de Crise, do Plano para Questões de Saúde Pública e do Procedimento de Classificação de Incidentes.



Os pilares de atuação setorial (continuidade dos negócios) dividem-se em três: Continuidade dos Negócios, a Continuidade nos Pontos de Atendimento (PAs) e a Continuidade de Tecnologia e Cyber. Como pilar de sustentação e instância deliberativa estratégica, o Comitê de Crise atua de forma centralizada e extraordinária para agilizar a tomada de decisões e integrar o fluxo de informações entre todas as frentes, mitigando com eficácia os impactos institucionais.

2.2. Gestão da Continuidade dos Negócios

O objetivo da Gestão de Continuidade dos Negócios é garantir o funcionamento da Instituição em níveis aceitáveis na ocorrência de crises ou eventos que possam interromper suas atividades operacionais e estratégicas. Tais medidas buscam garantir a continuidade dos negócios e a prestação ininterrupta de serviços aos clientes. Para este fim, os processos considerados críticos terão suas contingências planejadas e testadas, com o intuito de mitigar o impacto de eventuais incidentes.

Para suportar esta estratégia, o Grupo Mercantil estabeleceu uma estrutura hierárquica de documentação que se desdobra a partir dos Planos de Contingência e do Plano de Gestão de Crise, direcionando as ações nas três esferas de atuação, apoiadas pelos seguintes documentos e normativos internos, sem se limitar exclusivamente, aos itens mencionados:

- **Continuidade dos Negócios (Processos Corporativos):** Sustentada pela Análise de Impacto (BIA), Planos de Contingência Operacional (PCO) e Procedimentos de Gestão de Terceiros Relevantes;
- **Continuidade nos Pontos de Atendimento (Rede de Atendimento):** Suportada pelos Manuais de Procedimentos Internos dos Pontos de Atendimento (PA's);
- **Continuidade dos Serviços de Tecnologia e Cyber (Infraestrutura Sistêmica):** Sustentada pelo Plano de Continuidade dos Serviços de TI, Plano de Resposta a Incidentes Cibernéticos e pelas Políticas Corporativas de Segurança da Informação e de Segurança Cibernética.

Este arcabouço é complementado por planos específicos, como o Plano de Contingência para Questões de Saúde Pública (visando a continuidade operacional e a saúde de colaboradores e clientes) e o Plano de Gestão de Crise para eventos associados ao Risco de Imagem e Reputação. Este último concentra-se no fluxo de atividades para a tomada de decisão pela Administração sobre o gerenciamento do risco, o estabelecimento de diretrizes para a comunicação de impactos e a restauração dos processos internos.

Para assegurar a efetividade contínua da estrutura de Gestão de Continuidade de Negócios, os Planos e os Testes de Contingência Operacional devem ser atualizados, no mínimo, a cada 2 (dois) anos, ou em periodicidade inferior caso exigido por legislação aplicável.

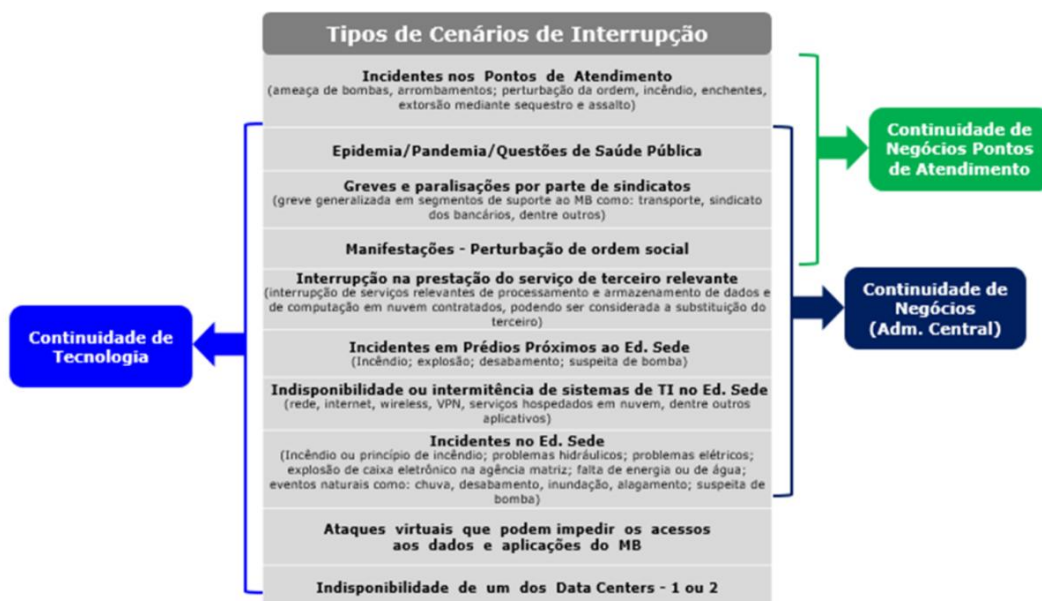
2.2.1. Cenários de Interrupção

O Grupo Mercantil também contempla cenários que possam resultar na indisponibilidade, total ou parcial, de seus canais, produtos e serviços, abrangendo indisponibilidades sistêmicas. Para cada tipologia de cenário, deverá ser implementada uma estratégia de solução detalhada nos planos de resposta.

Os principais cenários de indisponibilidade mapeados, sem limitação aos citados, classificam-se em:

- **Incidentes em Pontos de Atendimento:** Assaltos, arrombamentos, ameaças de bombas ou contra a integridade do patrimônio, perturbação da ordem, incêndios, enchentes e extorsão mediante sequestro;
- **Eventos de Pessoas e Externos:** Epidemias, pandemias, questões de saúde pública, manifestações e greves/paralisações;
- **Cenários Tecnológicos e de Terceiros:** Interrupção de serviço de terceiro relevante (processamento, nuvem, descontinuidade de serviços), ataques virtuais, indisponibilidade de Data Centers, de acesso à rede e aplicações (VPN) e falhas em sistemas;

- **Incidentes em Infraestrutura (Edifício Sede e entorno):** Incêndio, problemas estruturais, falta de energia / água, eventos naturais ou incidentes em prédios vizinhos.

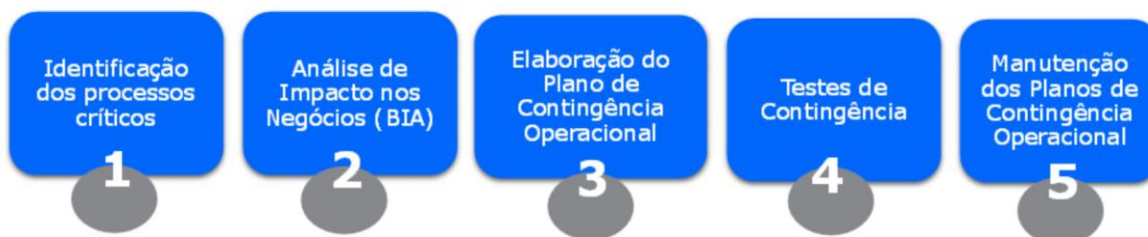


Ressalta-se que, em contexto de contingência, a execução dos processos não garante patamar de produtividade e eficácia equivalente à situação de normalidade. As soluções de Continuidade de Negócios adotadas estão alinhadas às diretrizes estabelecidas na Política de Segurança da Informação e na Política de Segurança Cibernética do Grupo Mercantil.

2.2.2. Metodologia aplicada à Gestão de Continuidade dos Negócios

A metodologia adotada pelo Grupo Mercantil fundamenta-se nas melhores práticas globais, especialmente nas normas técnicas ABNT NBR ISO 22.301 e ABNT NBR ISO 22.313. Esta diretriz estabelece um ciclo único e integrado, aplicável a todos os processos definidos como críticos, com o propósito de mensurar o impacto de uma interrupção e assegurar a resiliência organizacional.

O ciclo de gestão é composto pelas seguintes etapas, projetadas para garantir que as estratégias de continuidade sejam robustas, testadas e atualizadas:



1. **Identificação dos processos críticos:** Realização de levantamento preliminar via Questionário Pré BIA junto aos gestores para avaliar as características dos macroprocessos e os impactos em caso de interrupção das atividades em diversos aspectos (financeiro, clientes, legal, etc). A priorização da contingência é definida com base nos seguintes critérios: Exigência Regulamentar; Tempo de Indisponibilidade Tolerável; Atuação de Terceiros Relevantes e Criticidade do Processo para Controles Internos (conforme a avaliação da Alta Administração).

Ainda neste contexto, a identificação e/ou revisão dos processos que devem ser contingenciados pode se dar também por meio dos mapeamentos de processos críticos realizados pela equipe de Risco Operacional e Controles Internos, através de benchmarking no mercado, demandas de órgãos reguladores e fiscalizadores, solicitações de auditorias internas e externas e, ainda, durante a ocorrência de interrupções.

2. **Análise de Impacto nos Negócios (BIA):** Registro detalhado das informações que permitem a análise pormenorizada do impacto da interrupção em cada um dos processos críticos. Os resultados desses questionários apontam os recursos e infraestrutura mínimos necessários para o contingenciamento, incluindo a avaliação das contingências específicas dos terceiros relevantes envolvidos nos processos.
3. **Plano de Contingência Operacional - PCO:** Elaboração de planos baseados nos questionários de Análise de Impacto nos Negócios (BIA), tendo como objetivo detalhar as providências a serem adotadas em caso de interrupção dos processos críticos da área, os prazos estimados para restabelecimento das atividades, os fluxos de comunicação, e a contingência de terceiros relevantes, se houver. Nos planos também são apresentadas as estratégias de continuidade para as áreas, sendo classificadas de acordo com o nível de criticidade do processo.
4. **Testes de Contingência:** Realizados com a finalidade de verificar possíveis deficiências, comprovar a eficácia dos planos, bem como aculturar, treinar e aumentar a confiança dos usuários nos documentos elaborados. São utilizados métodos de testes definidos de acordo com o grau de maturidade do processo e exigências regulamentares. São disponibilizadas duas categorias de testes: Discussão e Simulação. O Relatório do Teste, contendo as especificações operacionais utilizadas para a execução, a definição e justificativa do método de teste utilizado e as observações e deficiências identificadas durante sua execução. Esse Relatório é formalmente enviado ao gestor da área contingenciada e à equipe de continuidade de TI.
5. **Manutenção dos Planos de Contingência Operacional:** Os planos podem sofrer manutenções por alterações nos processos e estruturas das áreas da Instituição, após algum teste ou outra situação em que se identifique tal necessidade, seja por correção, seja por evolução dos planos. Neste caso, realizam-se as modificações ou iniciam-se novamente as fases anteriores.

Para garantir a efetividade e tempestividade na gestão e elaboração dos Planos de Contingência Operacional, são estabelecidos prazos específicos para o posicionamento dos gestores à Gerência de Risco Operacional e Controles Internos.

Adicionalmente, em conformidade com a gestão de terceiros, é requerida a formalização de cláusulas contratuais que assegurem a continuidade e a existência de planos de contingência próprios para prestadores de serviços relevantes. A diligência aplicada a estes parceiros deve ser rigorosa e proporcional ao risco que representam para a Instituição.

As áreas internas devem buscar reduzir a dependência exclusiva de fornecedores, avaliando a adoção de estratégias de mitigação como a contratação de redundância (mais de um prestador por região) e o estabelecimento de Acordos de Nível de Serviço (SLA) robustos para minimizar impactos em caso de interrupção.

2.3. Continuidade nos Pontos de Atendimento

A gestão da Continuidade nos Pontos de Atendimento tem como premissa assegurar a disponibilidade dos serviços e o suporte aos clientes frente a interrupções de natureza tecnológica, operacional, logística ou de segurança. A atuação nessas unidades é regida pelos protocolos de resposta definidos nos Manuais de Funcionamento e normativos internos, visando a mitigação imediata de impactos operacionais.

Esta diretriz orienta o tratamento de incidentes críticos, conforme categorizados na Seção 2.2.1., que causem a interrupção no atendimento. Na ocorrência de tais eventos, é gerado um Relatório de Crise descrevendo os detalhes da ocorrência, as ações tomadas e as medidas complementares para resolução, com o suporte centralizado da Administração Central.

Como estratégia de contingência logística para a interrupção dos Pontos de Atendimento, a Instituição mantém um Posto de Atendimento Móvel. Esta unidade consiste em um container equipado para substituir temporariamente um ponto físico, garantindo a continuidade dos serviços essenciais e minimizando o impacto na prestação de serviços aos clientes em decorrência de desastres, falhas de equipamentos ou ações intencionais.

2.4. Continuidade dos Serviços de Tecnologia e Cyber

A continuidade dos serviços de tecnologia do Grupo Mercantil é regida pelo Plano de Continuidade de Serviços de TI (PCTI), que estabelece os procedimentos técnicos para o restabelecimento de operações em cenários de interrupção crítica, incluindo a indisponibilidade total de Data Centers.

A eficácia deste plano é validada periodicamente por meio de testes de contingência de ativos isolados e, principalmente, pela execução de Testes de Recuperação de Desastres (DR - Disaster Recovery). O Teste de DR tem como objetivo comprovar a capacidade de processamento e manutenção dos serviços críticos no ambiente alternativo, sendo o processo executado pelos times técnicos, acompanhado pela Gerência de Risco Operacional e Controles Internos, e validado pelas auditorias interna e externa.

Para assegurar a detecção tempestiva de falhas e a resiliência sistêmica, o Grupo mantém o monitoramento da disponibilidade tecnológica em regime integral (24 horas por dia, 7 dias por semana) através do Network Operation Center (NOC). Esta estrutura centraliza a identificação de eventos que possam impactar a continuidade e realiza o acionamento escalonado das equipes técnicas para solução, garantindo suporte físico e remoto a qualquer momento.

Esta estratégia de continuidade está intrinsecamente alinhada à Política de Segurança Cibernética, que define as diretrizes para minimizar impactos e recuperar ativos de informação em casos de incidentes de segurança, englobando também serviços de processamento, armazenamento de dados e computação em nuvem. A governança destes temas é reforçada por reportes periódicos ao Comitê de TI, à Vice-Presidência de Produtos, Tecnologia e Serviços e ao Conselho de Administração, garantindo o cumprimento das exigências regulatórias vigentes, em especial as dispostas na Resolução CMN nº 4.893/2021 e na Resolução BCB nº 5.274/2025.

2.5. Gerenciamento de Incidentes e Crises

O Gerenciamento de Incidentes e Crises do Grupo Mercantil é estruturado para garantir a resposta em dois níveis de severidade:

1. **Nível Operacional (Acionamento do PCO):** A decisão de ativar o Plano de Contingência Operacional (PCO) é delegada a cada Diretoria responsável pelos processos afetados, devendo ser comunicada à Diretoria Executiva de Riscos e Compliance. Os PCOs detalham as instruções técnicas a serem seguidas para o restabelecimento dos processos afetados.
2. **Nível Estratégico (Acionamento do Comitê de Crise):** Diante de eventos de maior severidade que demandam atuação integrada da Instituição, é acionado o Comitê de Crise. Esta instância de governança, de caráter extraordinário e flexível, centraliza a gestão da situação em crises classificadas como de criticidade Muito Alta (R5). Sua função primordial é apoiar a tomada de decisão estratégica, controlar o fluxo de comunicação institucional e supervisionar as ações de mitigação até a restauração completa das operações. A classificação atribuída ao incidente orienta a urgência e a priorização das ações de mitigação. A confirmação de relevância do evento, no entanto, é formalmente estabelecida com base nos parâmetros das áreas de atuação e consolidada após a normalização dos processos, assegurando que o enquadramento reflita o real impacto operacional e de negócio.

2.6. Comunicação com Órgãos Reguladores e Fiscalizadores

O Grupo Mercantil assegura a comunicação tempestiva do acionamento de seus Planos de Contingência Operacional (PCO) aos órgãos supervisores, sempre que houver previsão legal ou mediante requisição específica, seguindo rigorosamente os formatos exigidos. Adicionalmente, a Instituição mantém seus PCOs e respectivos relatórios de testes permanentemente à disposição das autoridades de fiscalização e controle.

A notificação formal de incidentes que impactem a segurança, operações, integridade de dados ou conformidade legal é precedida de uma avaliação imediata. Considerando que o reporte não é mandatório para todos os eventos, a comunicação formal será deliberada por uma análise integrada entre as áreas de Jurídico, Riscos e Compliance e o Comitê de Crise.

Esta avaliação considera:

- A natureza e gravidade do impacto.
- O volume de dados ou clientes atingidos.

- Os limites internos de risco.
- A estrita observância dos prazos legais estabelecidos por cada regulador.

As obrigações de reporte abrangem, mas não se limitam, às comunicações aos seguintes órgãos:

- **Banco Central do Brasil (BCB ou Bacen):**

Para incidentes sujeitos à comunicação obrigatória, especialmente aqueles relacionados a risco operacional, continuidade de negócios e segurança cibernética, conforme Resolução CMN nº 4.893/2021 e a Circular BCB nº 3.979/2020).

- **Comissão de Valores Mobiliários (CVM):**

Para eventos enquadrados como "Fato Relevante", que possam influir na decisão de investimento do mercado.

- **Autoridade Nacional de Proteção de Dados (ANPD):**

Para incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais (em cumprimento à Lei Geral de Proteção de Dados - LGPD).

- **Conselho de Controle de Atividades Financeiras (COAF):**

Para os incidentes associados a conduta, ética e conformidade, especificamente envolvendo suspeitas de Lavagem de Dinheiro e Financiamento ao Terrorismo.

- **Secretaria Nacional do Consumidor (Senacon) e Procons:**

Para interrupções graves de serviços ou eventos que afetem massivamente os clientes, demandando coordenação de resposta ao público. |

3. PAPÉIS E RESPONSABILIDADES

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

- Conselho de Administração
- Comitê de Auditoria
- Comitê de Riscos
- Comitê de Crise (Ad hoc)
- CEO, Vice-Presidências e Diretorias
- Vice-Presidência de Produtos, Tecnologia e Serviços
- Diretoria Executiva de Riscos e Compliance

- Gerência de Processamento e Monitoramento
- Gerência de Segurança Cyber
- Gerência de Suporte Administrativo e Infraestrutura
- Superintendência de Comunicação e Marketing
- Demais Áreas
- Terceiros Relevantes
 - Garantir a continuidade da prestação de serviços ao Grupo Mercantil em cenários de greve, paralisação ou qualquer modalidade de indisponibilidade operacional;
 - Apresentar e assegurar a resolutividade de seu Plano de Continuidade de Negócios no que tange aos produtos e serviços fornecidos ao Grupo Mercantil;
 - Submeter formalmente os resultados obtidos nos Testes de Contingência realizados;
 - Engajar-se de forma efetiva em testes e simulações nos processos de negócio que envolvam seus respectivos produtos e serviços;

4. 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.

5. REFERÊNCIAS NORMATIVAS

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	4.745/2019	Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.
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	4.968/21	Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
Resolução CVM	35/2021	Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.
Resolução CVM	32/2021	Dispõe sobre a prestação de serviços de custódia de valores mobiliários e revoga a Instrução CVM nº 542 , de 20 de dezembro de 2013.
Resolução CVM	33/2021	Dispõe sobre a prestação de serviços de escrituração de valores mobiliários e de emissão de certificados de valores mobiliários e revoga a Instrução CVM nº 543, de 20 de dezembro de 2013.
Resolução CVM	21/2021	Dispõe sobre o exercício profissional de administração de carteiras de valores mobiliários e revoga a Instrução CVM nº 426, de 28 de dezembro de 2005, a Instrução CVM nº 557, de 27 de janeiro de 2015, a Instrução CVM nº 558, de 26 de março de 2015, a Instrução CVM nº 597, de 26 de abril de 2018, a Deliberação CVM nº 51, de 25 de junho de 1987, a Deliberação CVM nº 740, de 11 de novembro de 2015 e a Deliberação CVM nº 764, de 4 de abril de 2017.

6. GLOSSÁRIO

- ANPD – Autoridade Nacional de Proteção de Dados
- Bacen – Banco Central do Brasil
- BIA – *Business Impact Analysis* (Análise de Impacto nos Negócios)
- CID – Confidencialidade, Integridade e Disponibilidade (Tríade de Segurança)
- CMN – Conselho Monetário Nacional
- COAF – Conselho de Controle de Atividades Financeiras
- CVM – Comissão de Valores Mobiliários
- DR – *Disaster Recovery* (Recuperação de Desastres)

- GCN – Gestão de Continuidade de Negócios
- IAM – Gestão de Identidade e Acessos
- LGPD – Lei Geral de Proteção de Dados
- NOC – *Network Operation Center*
- PAs – Pontos de Atendimento
- PCO – Plano de Contingência Operacional
- PCTI – Plano de Continuidade de Serviços de TI
- PLD – Prevenção à Lavagem de Dinheiro e ao Financiamento ao Terrorismo
- PQO – Programa de Qualificação Operacional
- RAS – *Risk Appetite Statement* (Declaração por Appetite ao Risco)
- RCA – Relatório de Análise da Causa Raiz
- Senacon – Secretaria Nacional do Consumidor
- SLA – Acordos de Nível de Serviço
- TI – Tecnologia da Informação |

–ABRANGÊNCIA–

Esta Política abrange a(s) seguinte(s) empresa(s) do Grupo Mercantil¹:

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.