

1. ÁREA RESPONSÁVEL

- 1.1. Gerência de Riscos, Controles Internos, *Compliance* e Integridade – Gerco.

2. REGULAMENTAÇÃO

- 2.1. Lei nº 13.260/2016;
- 2.2. Lei nº 12.846/2013;
- 2.3. Lei nº 13.303/2016;
- 2.4. Circular nº 3.979/2020;
- 2.5. Decreto nº 8.945/2016;
- 2.6. Instrução Normativa BCB nº 33/2020;
- 2.7. Resolução CMN nº 4.945/202;
- 2.8. Resolução CMN nº 4.557/2017;
- 2.9. Resolução BCB nº 85/2021;
- 2.10. Norma ABNT NBR ISO 31000:2018 - Gestão de Riscos - Diretrizes;
- 2.11. Norma ABNT NBR ISO 22301:2020 - Gestão de Continuidade de Negócios; e
- 2.12. Norma ABNT NBR ISO 27005:2022 - Segurança da Informação.

3. PERIODICIDADE DE REVISÃO

- 3.1. No mínimo anualmente, ou extraordinariamente, a qualquer tempo.

4. 4. INTRODUÇÃO E CONCEITOS

4.1. Estabelecer as diretrizes relacionadas ao gerenciamento integrado de riscos e divulgação das informações de gestão de riscos, nos termos da legislação, das regulamentações aplicáveis e com base em melhores práticas de governança, resguardadas aquelas de natureza confidencial e proprietária.

4.2. **Risco de Estratégia:** possibilidade de resultados observados serem diferentes dos inicialmente esperados, em virtude de mudanças no ambiente de negócios, da utilização de premissas inadequadas na tomada de decisão ou de falhas na execução de iniciativas e ações estratégicas. A partir da sua definição, tem-se sua subdivisão em três categorias específicas, a saber:

4.2.1. **Risco de Mudanças no Ambiente de Negócios:** avalia o risco de mudanças no ambiente de negócios comprometer a Estratégia da Companhia, como: mudanças competitivas, mudanças regulatórias, mudanças tecnológicas, mudanças políticas, mudanças econômicas, mudanças sociais, culturais e ambientais e risco sistêmico;

4.2.2. **Risco de Tomada de Decisões Estratégicas Inadequadas:** falhas na definição e priorização da estratégia; e

4.2.3. **Risco de Execução:** avalia o risco de falhas na execução de iniciativas e ações que possam comprometer o cumprimento da Estratégia da Companhia, como: risco de tradução da estratégia, falta de recursos, risco de descontinuidade, risco de parcerias estratégicas e risco de materialidade.

4.3. **Risco de Liquidez:** possibilidade de a Companhia não ter a capacidade de honrar seus compromissos financeiros no vencimento, incorrendo em pouca ou nenhuma perda.

4.4. **Risco de Mercado:** possibilidade de ocorrência de perdas resultantes da flutuação nos valores de mercado de instrumentos detidos pela Companhia.

4.5. **Risco de Reputação:** Possibilidade da formação de percepção negativa a respeito da Companhia, em qualquer aspecto, por parte do público com quem transaciona ou se relaciona (clientes, contrapartes, colaboradores, acionistas, investidores e supervisores) e das entidades ou setores capazes de influenciar aqueles com quem transaciona (mídia, sindicatos e sociedade em geral), levando a perdas que possam afetar adversamente a sustentabilidade do negócio.

4.5.1. **Percepção Negativa de Mercado:** perdas resultantes da possibilidade de percepção desfavorável por parte do mercado a respeito da Companhia e seus parceiros.

4.5.2. **Percepção Negativa dos Órgãos Supervisores ou Fiscalizadores:** perdas resultantes da percepção desfavorável em relação à Companhia por parte de órgãos supervisores ou fiscalizadores.

4.5.3. **Percepção Negativa de Funcionários:** perdas resultantes da percepção desfavorável de funcionários em relação à Companhia.

4.6. **Risco de Modelo:** possibilidade de perdas decorrentes do desenvolvimento ou uso inadequados de modelos, em função da imprecisão ou insuficiência dos dados ou à formulação incorreta na sua construção.

4.7. **Risco Operacional:** possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou eventos externos. Esta definição incluem a possibilidade de perdas decorrentes de:

4.7.1. **Risco de Conduta:** a possibilidade de perdas decorrentes de má conduta da Instituição ou de atos inadequados na condução das suas atividades pela Alta Administração, funcionários, colaboradores e por aqueles que atuam em nome ou prestam serviços para a Companhia. A partir da sua definição, tem-se sua subdivisão em duas dimensões, a saber:

4.7.1.1. Conduta nas Relações de Trabalho e com as demais partes interessadas; e

4.7.1.2. Conduta no Relacionamento com Clientes e Usuários.

4.7.2. **Risco Cibernético:** possibilidade de perdas decorrentes de ataques cibernéticos contra a infraestrutura de TI ou sistemas corporativos, afetando a integridade, confidencialidade e disponibilidade.

4.7.3. **Risco de Conformidade:** possibilidade de perdas decorrentes do descumprimento de normas externas.

4.7.4. **Risco de Terceiros:** possibilidade de perdas decorrentes do relacionamento da Companhia com terceiros.

4.7.5. **Risco Legal:** possibilidade de perdas decorrentes de inadequação ou deficiência em contratos firmados pela Companhia; de sanções em razão do descumprimento de dispositivos legais; de indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Companhia e de alterações no ambiente normativo e no entendimento jurisprudencial.

4.7.6. **Risco de Segurança:** possibilidade de perdas decorrentes de falhas nos processos de segurança de patrimônio e de pessoas, dos negócios e das informações corporativas, inclusive dados pessoais. Essa definição inclui a possibilidade de perdas decorrentes de:

4.7.6.1. **Prevenção e Combate à Lavagem de Dinheiro, ao Financiamento do Terrorismo, ao Financiamento da Proliferação de Armas de Destruição em Massa e à Corrupção - PLD/FTP-C:** possibilidade de sanção pela inobservância de normas que mitiguem a utilização da Companhia para a prática de crimes de lavagem de dinheiro, de Financiamento do Terrorismo e de Corrupção; ou de sanção pela prática de ato lesivo qualificável como corrupção contra a administração pública nacional ou estrangeira.

4.7.7. **Risco de Tecnologia da Informação - TI:** possibilidade de perdas decorrentes de inadequações ou falhas na entrega e suporte de soluções e serviços de tecnologia, envolvendo infraestrutura, construção, operação.

4.8. **Risco Social, Ambiental e Climático (RSAC):** possibilidade de perdas decorrentes da exposição a danos sociais, ambientais e climáticos gerados pelas atividades da Companhia. A partir da sua definição, tem-se sua subdivisão em três categorias de risco:

4.8.1. **Social:** possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos ocasionados por eventos associados à violação de direitos e garantias fundamentais ou a atos lesivos a interesse comum.

4.8.2. **Ambiental:** possibilidade de ocorrências de perdas para a instituição ocasionadas por eventos associados à degradação do meio ambiente, incluindo o uso excessivo de recursos naturais.

4.8.3. **Climático:** em suas vertentes de risco de transição e de risco físico, como:

4.8.3.1. **Risco Climático de Transição:** possibilidade de ocorrências de perdas para a instituição ocasionadas por eventos associados ao processo de transição para uma economia de baixo carbono, em que a emissão de gases do efeito estufa é reduzida ou compensada e os mecanismos naturais de captura desses gases são preservados; e

4.8.3.2. **Risco Climático Físico:** possibilidade de ocorrências de perdas para a instituição ocasionadas por eventos associados a intempéries frequentes e severas ou a alterações ambientais de longo prazo, que possam ser relacionadas a mudanças em padrões climáticos.

5. ENUNCIADOS

5.1. A Alta Administração está comprometida com o processo de gestão de riscos e é responsável pela validação dos modelos adotados.

- 5.2. A Companhia não está sujeita ao Risco de Crédito, devido ao modelo de negócio, não existindo as figuras de tomador e devedor, inexistindo inadimplência, no sentido de risco, e sim, possível quebra de acordo, evento comum ao negócio e implícito no modelo de precificação das compras das carteiras.
- 5.3. Estabelecemos modelo de gestão de riscos, envolvendo estrutura de Comitês e Conselhos: Comitê Executivo de Gestão de Riscos e de Crises - Ceris, Comitê de Gestão de Riscos e de Capital - Coris/BB, Comitê de Auditoria - Coaud/BB, Conselho de Administração e Conselho Fiscal.
- 5.4. Dispomos de estrutura própria de gestão de riscos compatível com o porte da Companhia, natureza e complexidade do nosso negócio.
- 5.5. Somos conservadores na gestão de riscos.
- 5.6. Assumimos postura preventiva e estabelecemos limites de aceitação e tolerância na gestão de riscos dispostos na Declaração de Apetite e Tolerância à Riscos.
- 5.7. Primamos pela ética, legalidade, transparência e qualidade nas informações.
- 5.8. Incorporamos a gestão de riscos à tomada de decisões, em conformidade com as melhores práticas de mercado, em alinhamento com as políticas do Controlador e em observância às legislações, normas e diretrizes sobre o tema.
- 5.9. Adotamos a gestão integrada de riscos corporativos, com foco na interrelação entre processos, pessoas, sistemas, controles, riscos e resultados.
- 5.10. Realizamos o gerenciamento dos riscos através de atividades e instrumentos contemplados nos processos de identificação, mensuração, avaliação, controle, monitoramento, mitigação e reporte dos riscos.
- 5.11. Adotamos estrutura de gerenciamento de riscos, controles internos e conformidade com responsabilidades distribuídas em 3 linhas de defesa, compatível com o porte, a complexidade, a estrutura, o perfil de risco e o modelo de negócio da Companhia, de forma a assegurar sua robustez:
- 5.11.1. **1ª linha - Gerências Proprietárias dos Riscos:** atuam na identificação, avaliação, mensuração e mitigação dos riscos, garantindo que as atividades sob sua responsabilidade estejam de acordo com as metas e objetivos;
- 5.11.2. **2ª linha - Acompanhamento da Conformidade:** atuação da Gerco, que visa o monitoramento dos controles da 1ª linha de defesa, garantindo que ela funcione, bem como a supervisão dos riscos relevantes e visão sistematizada dos riscos da Companhia; e
- 5.11.3. **3ª linha - Avaliação de todo Processo:** avalia a 1ª e 2ª linha de defesa, bem como a Governança, Gestão de Riscos e Controles Internos e Demonstrações Financeiras. A Companhia possui convênio com o Banco do Brasil - BB para compartilhamento da Auditoria Interna e Externa/Independente. Contamos também, com o acompanhamento, supervisão e avaliação por áreas especializadas do BB. Além disso, temos as avaliações e orientações expedidas pelos órgãos fiscalizadores.
- 5.12. Executamos a atividade de gerenciamento de riscos de forma dinâmica e segregada das atividades de negócios, conformidade e de auditoria interna, envolvendo o fluxo contínuo de informações a saber:

5.12.1. **Preparação:** é a fase de coleta de dados, análise das informações, elaboração dos relatórios e preparação das recomendações para apreciação dos Comitês responsáveis;

5.12.2. **Decisão:** as decisões são tomadas pelos Comitês, Diretoria Executiva e Conselhos responsáveis;

5.12.3. **Execução:** as áreas intervenientes, incluindo a Gerco implementam as decisões tomadas; e

5.12.4. **Acompanhamento:** a Gerco acompanha o cumprimento das deliberações e seus impactos e as comunica aos Comitês competentes.

5.13. O gerenciamento eficaz dos riscos traz benefícios à Companhia tais como:

5.13.1. Eficiente alocação de capital;

5.13.2. Melhoria do processo decisório;

5.13.3. Redução dos custos;

5.13.4. Melhor relação com o risco e retorno;

5.13.5. Maior solidez, estabilidade e competitividade; e

5.13.6. Geração de valor para os acionistas.

5.14. As informações de gerenciamento dos riscos são contínuas, transparentes, claras, confiáveis e tempestivas. A divulgação dessas informações considera a conveniência estratégica e o sigilo da Companhia.

5.15. Identificamos, avaliamos e mitigamos os eventos de riscos relevantes associados às atividades da Companhia, indicando áreas de incidência, causas e potenciais impactos, observando as boas práticas de governança corporativa e de gestão de riscos.

5.16. Monitoramos, reportamos e controlamos a exposição aos riscos, considerando limites estabelecidos, buscando manter os riscos em conformidade com o apetite e tolerância aprovados pelo Conselho de Administração.

5.17. Utilizamos um conjunto de atividades, planos, métodos, indicadores, procedimentos integrados e documentados para assegurar a conformidade e a mitigação de riscos.

5.18. Avaliamos, monitoramos e revisamos periodicamente os modelos desenvolvidos para o gerenciamento de riscos com base nas legislações vigentes e nas melhores práticas de mercado.

5.19. Definimos e comunicamos formalmente responsabilidades, competências, normas e alçadas aos envolvidos nos diversos níveis e processos da Companhia., mantendo a apropriada segregação de funções e mitigando riscos de conflito de interesses.

5.20. Divulgamos, publicamente e periodicamente, informações inerentes aos riscos envolvidos nas atividades da Companhia e sua subsidiária.

5.21. Reportamos tempestivamente à Alta Administração, entidades externas de fiscalização e controle e acionistas, informações relevantes relacionadas ao gerenciamento de riscos que impactem a liquidez, perdas operacionais e a continuidade dos negócios.

5.22. A cultura de gestão de riscos é disseminada em toda a Companhia, buscando o aprimoramento profissional e a conscientização de todos os empregados para a importância do gerenciamento dos riscos.

5.23. Divulgamos a Política de Gestão de Riscos no site institucional da Companhia. <https://ativosbb.com.br/quem-somos/>.

5.24. Acompanhamos os processos internos, no âmbito de cada unidade organizacional.

5.25. Instituímos ações educacionais de modo a assegurar que todos os administradores participem de treinamento periódico, no mínimo anual, sobre a Política de Gestão de Riscos.

5.26. O processo de gerenciamento dos riscos conta com recursos humanos com conhecimento e experiência necessários ao desempenho de suas funções e sistemas informatizados adequados à implantação das políticas e estratégias aprovadas e observa as determinações legais e as exigências da supervisão da Companhia.

5.27. O processo de gerenciamento dos riscos é validado pela Diretoria Executiva, auditado pelas Auditorias Interna (Audit/BB) e Auditoria Independente e acompanhado e fiscalizado pelos Órgãos de Regulação e Fiscalização.

5.28. Utilizamos os resultados dos testes de conformidade e monitoramentos realizados nos controles, para a mitigação dos riscos da Companhia bem como na avaliação da adequação e da robustez das premissas e das metodologias utilizadas nos modelos para gerenciamento de riscos.

5.29. Asseguramos que os limites e as alçadas corporativas, previamente definidos, são observados no processo de gerenciamento de riscos.

5.30. Utilizamos no gerenciamento dos riscos, rotinas, processos e procedimentos, que garantem a avaliação, o controle e o monitoramento e mitigação dos riscos.

5.31. Acompanhamos e mantemos o banco de dados das legislações aplicáveis aos negócios da Companhia, para implementação de ações e manutenção da conformidade.

5.32. Adotamos procedimentos de acompanhamento, monitoramento, comunicação e reenquadramento de eventual extrapolação de limites.

5.33. Estabelecemos o máximo de risco que a Instituição aceita incorrer em seus negócios, alinhado à capacidade para assunção de riscos e seus objetivos estratégicos por meio da Declaração de Appetite e Tolerância a Riscos.

5.34. Revisamos a Declaração de Appetite e Tolerância a Riscos anualmente, de forma ordinária, ou extraordinariamente, quando necessário.

5.35. A administração dos riscos procura resguardar a segurança e solidez da Companhia, a geração de resultado econômico positivo, a agregação de valor para os investidores.

5.36. Realizamos testes de estresse integrados, quando aplicáveis, considerando efeitos extremos nos riscos e nos negócios.

5.37. Estabelecemos estrutura de governança para gestão de risco de modelos, com definição de diretrizes, papéis, responsabilidades e alçadas, observando adequada segregação de funções.

5.38. Adotamos diretrizes para gestão do ciclo de vida dos modelos, assegurando documentação, rastreabilidade e observância dos processos de governança aplicáveis, bem como diretrizes para continuidade e resiliência dos modelos e dos processos a eles associados.

5.39. Asseguramos que os dados utilizados em modelos atendam a critérios de integridade, completude, acurácia, segurança, controle de acesso, responsabilidade (*ownership*), conformidade legal e rastreabilidade, observadas as diretrizes de governança e proteção de dados.

5.40. Adotamos práticas para identificação, mensuração, monitoramento e controle do risco de modelos, bem como estabelecemos diretrizes para sua validação independente, aprovação e supervisão, de forma proporcional à materialidade, criticidade e finalidade de uso.

5.41. Orientamos o uso de modelos, incluindo aqueles baseados em Inteligência Artificial, por princípios de ética, responsabilidade, transparência e explicabilidade, com mitigação de vieses e atenção a potenciais impactos adversos, considerando o nível de automação e o impacto das decisões suportadas, especialmente aquelas automatizadas ou semiautomatizadas.

5.42. Consideramos, de forma principiológica, os impactos sociais, ambientais e de governança no uso de modelos e soluções de Inteligência Artificial, promovendo sua utilização responsável e sustentável.

5.43. Promovemos a capacitação e a conscientização dos envolvidos na gestão e uso de modelos, de forma compatível com suas responsabilidades.

6. VIGÊNCIA E VERSIONAMENTO

6.1. Esta Política foi aprovada pelo Conselho de Administração em 28.04.2020 e revisada em 27.04.2021, 26.04.2022, 24.04.2023, 22.04.2024, 28.04.2025 e 27.04.2026.