Av. Presidente Vargas, 800 - Belém (PA) - Companhia Aberta - Carta Patente: 3.369/00001 - CNPJ: 04.902.979/0001-44

PR, com utilização de choque compatível com o 1º e o 99º percentis de uma distribuição histórica de variações nas taxas de juros, considerando o período de manutenção (holding period) de um ano e o período de observação de cinco anos.

❖ Abordagem 2: estima a quantidade de pontos-base de choques paralelos de taxas de juros necessários para acarretar reduções do valor de mercado das operações não classificadas na carteira de negociação correspondentes a 5%, 10% e 20% do PR.

e) Risco social, ambiental e climático (RSAC)

A gestão do risco socioambiental e climático no Banco está estruturada em observância aos preceitos estabelecidos na Resolução CMN nº 4.557/2017 e Resolução CMN nº 4.945/2021, a partir da utilização de ferramentas de análise e monitoramento de risco das operações selecionadas em conformidade com a matriz de relevância e proporcionalidade do Banco.

O Banco estabeleceu a Política de Responsabilidade Social, Ambiental e Climática – PRSAC, que contempla princípios e diretrizes que norteiam as ações de sustentabilidade e de risco social, ambiental e climático, consideradas as dimensões estratégicas, de governança e econômicas, na atuação do Banco, tanto no aspecto institucional como nas operações de financiamento da empresa.

A concessão de empréstimos e financiamentos são condicionados à apresentação das exigências legais, quando for o caso, tais como certidões de regularidade ambiental e Licenças Ambientais. Em especial os financiamentos concedidos por meio do crédito rural, devem estar aderentes às restrições legais impostas pelo Manual do Crédito Rural (MCR).

No Banco, toda a operação rural recebe tratamento de análise socioambiental, realizada em ferramenta contratada, com exceção das dispensadas pelo MCR. A ferramenta cruza diferentes bancos de dados oficiais e produz relatório de acordo com a legislação ambiental e normas do Banco.

Todas as operações do crédito rural no Banco recebem análise socioambiental previamente à concessão de forma individual. Os critérios de análise socioambiental estão estabelecidos em normas internas e tem como premissa a mitigação de riscos socioambientais e o atendimento das exigências dos órgãos reguladores. O Banco possui metodologia interna de avaliação de níveis de RSAC aplicada em sistema de avaliação desenvolvido internamente, apurando o RSAC das operações as quais abrange em três níveis: Alto, Médio e Baixo. O gerenciamento de RSAC está estruturado e documentado em Norma de Procedimento interna, a qual determina a validade e periodicidade das avaliações, bem como apresenta as rotinas e procedimentos de gestão do risco.

f) Risco cibernético

A Segurança da Informação e Comunicações (SIC) é um conjunto de ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, sejam elas físicas ou digitais, contra diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar eventuais danos, maximizar o retorno dos investimentos e de novas oportunidades de negócio.

A Segurança Cibernética está contida dentro do âmbito da SIC e se configura como um conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado, permitindo o uso e o compartilhamento da informação digital de forma controlada. Sendo assim, a SIC é de maior abrangência, protegendo tecnologias, pessoas, informações físicas, entre outros, enquanto a Segurança Cibernética visa proteger somente ativos relacionados ao universo digital.

Nessa perspectiva, risco cibernético é o risco que se refere aos potenciais resultados negativos associados aos ataques cibernéticos. Por sua vez, os ataques cibernéticos podem ser definidos como tentativas de comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas tecnológicos.

No Banco, a estrutura de gerenciamento de riscos cibernéticos atende ao previsto na Resolução CMN nº 4.893/2021 e se aplica a toda a Instituição, dispondo de:

❖ Política de segurança da informação e cibernética, que tem por objetivo estabelecer o Sistema de Gestão da Segurança da Informação (SGSI) do Banco da Amazônia, considerando uma visão holística e coordenada dos riscos de SIC do Banco para definir e comunicar os princípios, valores, conceitos, diretrizes, controles suficientes à preservação e proteção das informações do Banco da Amazônia e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade, em todo o seu ciclo de vida, contida em qualquer suporte ou formato.

❖ Normas de procedimentos de segurança da informação que apoiam a estratégia definida na Política.

❖ Planos de resposta a incidentes de cibersegurança.

❖ Comitê de Segurança Corporativa, da Informação e de Comunicações: de caráter consultivo e deliberativo, tem por finalidade participar do processo de gestão de Segurança Corporativa, inclusive de Informação e de Comunicações do Banco.

A governança no gerenciamento de riscos cibernético adota também a abordagem das três linhas. Onde:

❖ A primeira linha, representada pelas áreas de tecnologia, pessoas e contratos, responsáveis por identificar, avaliar, reportar e gerenciar os riscos cibernéticos em ativos de tecnologia, recursos humanos e cadeia de suprimento, respectivamente, e pela execução dos controles e mitigadores de riscos, e, ainda, pela definição e implementação de planos de ação para garantir a efetividade do ambiente de controle;

❖ Na segunda linha, a área responsável pelo gerenciamento de risco cibernético, a qual define a estratégia e as políticas de segurança, bem como realiza o monitoramento dos riscos, a gestão de incidentes e é responsável pelo aculturamento da empresa acerca da segurança da informação. Ainda como parte da segunda linha, a área responsável pela gestão de continuidade de negócio, tema afeto à segurança da informação, é a área de controles internos responsável por definir as diretrizes e procedimentos inerentes à gestão de continuidade de negócios, estabelecendo o processo para análise de impacto nos negócios, estratégias para assegurar a continuidade das atividades da instituição e limitar perdas decorrentes da interrupção dos processos críticos de negócio;

❖ A terceira linha é representada pela Auditoria Interna.

g) Risco operacional

O Banco segue as diretrizes da Resolução CMN nº 4.557/2017, integrando a gestão do risco operacional à sua estrutura e a todos os níveis hierárquicos. Utiliza normas de procedimento com detalhamento de papéis e responsabilidades da Instituição conforme modelo das três linhas.

Realiza monitoramento contínuo dos eventos relacionados ao risco operacional, mantendo uma base histórica quantitativa e qualitativa de informações, reportando regularmente à Alta Administração. Ressalta-se, ainda, a promoção da cultura voltada à gestão de riscos e controles, com o objetivo de alcançar metas estratégicas e fortalecer a governança corporativa.

h) Risco legal

Em conformidade com as exigências do Bacen e de outros órgãos reguladores, o Banco atua rigorosamente no cumprimento de leis, normas e regulamentos aplicáveis às instituições financeiras. A área de Controles Internos monitora com vista a assegurar o atendimento das demandas legais.

Para divulgar normativos externos e monitorar o cumprimento das demandas legais, o Banco utiliza um Sistema de *Compliance* que fornece informações atualizadas sobre normas relacionadas as atividades bancárias para todas as áreas internas relacionadas.

i) Risco de integridade

A empresa mantém programas e políticas voltados para a integridade, além de um Código de Conduta Ética que fortalece o ambiente de controle interno do Banco.

A Política de Gestão da Integridade tem por finalidade estabelecer e difundir princípios, objetivos, diretrizes, competências e responsabilidades para a gestão da integridade, essenciais aos processos de governança e à gestão das políticas, programas e normas internas relacionadas.

Além dos programas e políticas, o Plano de Ação e os indicadores de integridade buscam garantir a eficiência na gestão por meio do acompanhamento e monitoramento, fortalecendo os pilares e princípios do programa, assim como as boas práticas na cultura institucional.