BANCO CÉDULA S.A.
CNPJ/MF: 33.132.044/0001-24

POLÍTICA DE GERENCIAMENTO DO RISCO OPERACIONAL

Atualização – Dezembro/2023

POLÍTICA DE GERENCIAMENTO DO RISCO OPERACIONAL

I - INTRODUÇÃO

A Política de Risco Operacional do BANCO CÉDULA tem como objetivo definir diretrizes para a implantação e disseminação da cultura para a gestão do Rico Operacional (RO) em todos os níveis da instituição. Estabelecendo papeis e obrigações para cumprir os objetivos traçados pela alta administração.

2 - DEFINIÇÃO

Define-se Risco Operacional (RO) como “possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas”.[1]

Os principais instrumentos que integram o modelo de Controle e Gestão de RO do BANCO CÉDULA tomam por base, principalmente, o registro histórico de eventos que resultem em perdas advindas de RO. Além do registro histórico, modelo compatível com o segmento do BANCO CÉDULA[2], outros instrumentos são utilizados para o Controle e Gerenciamento do RO, dentre os quais:

a) Definição do apetite de RO;
b) registro e avaliação de eventos de perdas;
c) treinamento periódico de todos os colaboradores e acompanhamento do seu engajamento à cultura da instituição;
d) autoavaliação de RO.

Para os fins estabelecidos neste documento, o RO contempla também o risco legal associado à inadequação ou deficiência em contratos firmados pelo BANCO CÉDULA, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição[3].

São eventos de risco operacional, dentre outros:

[1] Art. 32 da Resolução CMN 4.557/2017.
[2] O Banco Cédula S.A. está classificado como integrante do Segmento S4 pelo Banco Central do Brasil.
[3] Art. 32, § 1º da Resolução CMN 4.557/2017.

- **Fraudes Internas:** Perdas decorrentes de atos deliberados com objetivo de obter vantagem indevida, financeira ou não, praticados por um ou mais colaboradores, ou por uma área interna do BANCO CÉDULA.
- **Fraudes Externas**: Perdas decorrentes de atos deliberados com objetivo de obter vantagem indevida, financeira ou não, decorrente de ação praticada por parte externa e alheia o BANCO CÉDULA.
- **Demandas Trabalhistas e Segurança deficiente do local de Trabalho:** Perdas decorrentes de inobservância de contratos ou leis trabalhistas, de saude ou segurança do trabalho, do pagamento por reclamações por lesões, práticas discriminatórias, assédio sexual ou moral.
- **Práticas inadequadas relativas a usuários finais, clientes, produtos e serviços:** Perdas decorrentes de falha não intencional ou negligente para cumprir uma obrigação profissional com clientes, incorreções da estrutura de produtos e serviços ou em função de práticas comerciais inadequadas.
- **Danos a ativos físicos próprios ou em uso pelo BANCO CÉDULA:** Perdas decorrentes de danos aos ativos físicos ocasionados por desastres naturais ou outros acontecimentos extraordinários.
- **Situações que acarretem a interrupção das atividades da instituição ou a descontinuidade dos serviços prestados, incluindo o de pagamentos:** Perdas decorrentes de ruptura e descontinuidade de negócios, atividades, produtos ou operações da instituição.
- **Falhas em sistemas, processos ou infraestrutura de tecnologia de Informação (TI):** Perdas decorrentes da interrupção ou da má performance dos negócios, causadas por falhas em sistemas.
- **Falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da instituição, incluindo aquelas relacionadas aos arranjos de pagamento do BANCO CÉDULA**: Perdas decorrentes de administração de processo ou gestão de processos, processamento de informações, processamento de transação com problemas, relações com contrapartes ou relacionados com a apresentação de informações.
- **Risco Cibernético:** possibilidade de ocorrência de perdas resultantes de incidentes cibernéticos entendidos como qualquer evento relacionado com o ambiente cibernético que: a) produz efeito adverso ou representa ameaça

aos sistemas de tecnologia da informação (TI) ou à informação que esses sistemas processam, armazenam ou transmitem; ou b) infringe políticas ou procedimentos de segurança referentes aos sistemas de TI.

Incluem-se, ainda, para eventuais falhas vinculadas a atividade de pagamento as seguintes situações: falhas na proteção e na segurança de dados sensíveis relacionados tanto às credenciais dos usuários finais quanto a outras informações trocadas com o objetivo de efetuar transações de pagamento; falhas na identificação e autenticação do usuário final em transação de pagamento; falhas na autorização das transações de pagamento e falhas na iniciação de transação de pagamento.

O BANCO CÉDULA possui estrutura de gerenciamento capacitada a identificar, avaliar, monitorar, controlar e mitigar seus riscos, inclusive aqueles decorrentes de serviços terceirizados.

A Diretoria do BANCO CÉDULA está plenamente engajada no processo, tendo definido e aprovado essa política de gerenciamento e disponibilizado adequados recursos humanos e materiais para o bom funcionamento dessa estrutura.

3 – DIRETRIZES

O BANCO CÉDULA tem como diretrizes em sua política de RO:

- A disseminação da cultura de mitigação de riscos demonstrando a todos os colaboradores a importância de seguir os procedimentos de controles internos através da divulgação na intranet ou no sítio do BANCO CÉDULA a presente política e demais manuais operacionais;
- O estrito cumprimento da legislação aplicável ao BANCO CÉDULA expedida pelos reguladores bem como aderência de todos os colaboradores às políticas e aos procedimentos internos;
- A definição de responsabilidades em conformidade com a estrutura organizacional da instituição;
- A segregação de atividades exercidas pelos colaboradores, de maneira a mitigar/eliminar a ocorrência de conflito de interesses que possam expor a instituição a escolhas viciadas por parte de seus colaboradores;

- A elaboração periódica de relatórios sobre a situação dos controles internos para apresentação à alta administração do BANCO CÉDULA;
- Manutenção da estrutura de gerenciamento de RO alinhada às necessidades do BANCO CÉDULA, periodicamente revisada para garantir o estrito cumprimento da presente política mitigando/eliminando quaisquer riscos porventura existentes ou que possam ser previstos nos testes;
- Elaboração de relatórios periódicos sobre a exposição do BANCO CÉDULA aos riscos operacionais para fins de registro de não conformidades e perdas operacionais registradas e monitoradas pelos sistemas de controle.

4 - GERENCIAMENTO

O gerenciamento de risco operacional deve prever:

a) Identificação, avaliação, monitoramento, controle e mitigação do risco operacional;

b) Documentação e armazenamento de informações referentes às perdas associadas ao risco operacional;

c) Elaboração, com periodicidade mínima anual, de relatórios que permitam a identificação e correção tempestiva das deficiências de controle e de gerenciamento do risco operacional;

d) Realização, com periodicidade mínima anual, de testes de avaliação dos sistemas de controle de riscos operacionais implementados;

e) Elaboração e disseminação da política de gerenciamento de risco operacional ao pessoal da instituição, em seus diversos níveis, estabelecendo papéis e responsabilidades, bem como as dos prestadores de serviços terceirizados;

f) Existência de plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional; Implementação, manutenção e divulgação de processo estruturado de comunicação e informação.

O gerenciamento do RO é um dos pontos fundamentais do BANCO CÉDULA que opera no seguimento de pequenas e médias empresas, instituição

apresenta risco operacional baixo em razão de que suas atividades que se concentram em:

4.1) TÍTULOS E VALORES MOBILIÁRIOS E INSTRUMENTOS FINANCEIROS DERIVATIVOS

a) Títulos de Renda Variável (Ações de Companhias Abertas)

4.2) OPERAÇÕES DE CRÉDITO

a) Financiamento, Empréstimo e Capital de Giro – Em regra são operações de mútuo lastreadas em garantias reais (Alienação Fiduciária de Imóveis) ou caução de recebíveis e garantias fidejussórias;

b) Conta Rotativa – Limite de Crédito disponibilizado ao cliente que entrega títulos para serem caucionados/ entregues em penhor, amortizando a dívida até restabelecer o limite;

c) Crédito Pessoal – mútuo com pessoa física;

4.3) CAPTAÇÃO DE CDB

a) Pessoa Física;

b) Pessoa Jurídica.

5 - ESTRUTURA DE GERENCIAMENTO DE RISCO

Nos termos definidos pelo CMN, um Diretor é indicado a representar o BANCO CÉDULA junto ao Banco Central, responsável por supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de riscos incluindo seu aperfeiçoamento e definir as políticas e objetivos gerais e respaldar a Alta Administração com informações relevantes sobre a implementação e gerenciamento dos riscos operacionais e pela correta identificação dos riscos inerentes aos processos por ele geridos, bem como pela categorização, avaliação, controle, monitoramento e tomada de ações de mitigação. Uma vez identificado, deverá acompanhar o status dos controles praticados sobre ele e reportar periodicamente a fim de permitir ao BANCO CÉDULA a atualização da ferramenta de gestão.

A estrutura de gerenciamento de RO do BANCO CÉDULA[4] é composta de três níveis: Nível Estratégico; Nível Gerencial e Nível Operacional.

I - NÍVEL ESTRATÉGICO:

O nível estratégico é formado pela Diretoria e pelo Departamento de Compliance.

São atribuições do nível estratégico:

- Decidir as diretrizes e objetivos que a gestão de RO deve alcançar, assim como aprovar, discutir e registrar todas as mudanças ocorridas na política de RO;
- Garantir que o departamento de Compliance possua a adequada estrutura de profissionais em quantidade e qualidade, recursos, infraestrutura e tecnologia, e que receba todas as informações necessárias para atingir a sua missão;
- Definir o nível de aceitação do risco da instituição (resposta ao risco; analisar as deficiências relevantes que forem apontadas pelo nível gerencial e que requeiram definições e ações estratégicas.

II - NIVEL GERENCIAL:

O Nível Gerencial é formado pelos responsáveis por cada departamento que têm como missão o cumprimento das diretrizes e objetivos traçados pelo nível estratégico.

São atribuições do nível gerencial:

- Observar a legislação aplicável a cada departamento elaborando e revisando periodicamente os seus manuais operacionais bem como a sua aderência por seus integrantes;
- Garantir que os riscos operacionais locais sejam correta e satisfatoriamente monitorados e controlados;
- Garantir a existência de um processo apropriado para avaliação de potenciais riscos operacionais envolvendo novos produtos;

[4] Dispensada a formação de Comitê de Risco, na forma do art. 60, XIX da Resolução CMN 4.557/2017.

- Emitir relatórios com informações que serão submetidas ao nível estratégico, e que devam conter ações a serem implementadas para correção tempestivas das deficiências apontadas e para manter o histórico e garantir a continuidade dos processos da área;
- Comunicar quaisquer ocorrências encontradas ao departamento de compliance tão logo tome ciência.

O Nível Gerencial pode propor, posteriormente, modificações nas responsabilidades acima descritas para ajustá-las as necessidades das exigências, práticas internas e dos órgãos reguladores. Estas modificações deverão ser submetidas e aprovadas pelo nível estratégico.

III - NÍVEL OPERACIONAL:

O nível operacional é composto pelo Departamento de Compliance que possui, dentre as suas atribuições:

- Descrever, monitorar, avaliar e sugerir modificações junto ao nível estratégico acerca dos riscos que cada departamento está sujeito, inclusive a verificação de conformidade com as políticas e normas dos órgãos reguladores por toda a instituição;
- Sugerir e implementar, após a aprovação do nível estratégico, plano para melhoria dos controles existentes, baseando-se no profundo conhecimento do dia-a-dia de sua área e em conjunto com os responsáveis pelo processo;
- Desenhar estratégias de teste dos controles identificados para mitigação do risco.

6 – DAS AUDITORIAS EXTERNA E INTERNA:

As auditorias externa e interna procederão a testes dos procedimentos estabelecidos para assegurar o cumprimento desta política e verificação periódica da efetividade operacional dos controles.

7 – DO DEPARTAMENTO DE COMPLIANCE

O Departamento de Compliance tem por missão o acompanhamento das rotinas operacionais e regulatórias por parte da instituição e de todos os seus colaboradores devendo, ainda:

- Acompanhar, e divulgar internamente, toda e qualquer legislação e demais normativos expedidos pelo Banco Central do Brasil, CMN e demais órgãos;
- Disseminar a Política de Controles Internos;
- Acompanhar a e Execução de testes de aderência normativa, com consequente supervisão da implementação de planos de ação e
- Elaborar, supervisionar e atualizar todas as regras internas, especialmente no que se refere a prevenção à lavagem de dinheiro e combate ao financiamento ao terrorismo.

8 - MONITORAMENTO E GESTÃO DE RISCO OPERACIONAL

O monitoramento e Gestão de RO foram desenvolvidos a partir do mapeamento dos processos da empresa e a identificação dos riscos inerentes a cada um deles. Cabe ressaltar que, assim como os processos são dinâmicos, os riscos também possuem seu dinamismo. Daí a importância de que seja algo vivo dentro da empresa com atualizações frequentes, não só do resultado dos testes e controles, como também da própria identificação dos riscos nos processos.

Essa estrutura, integrada com o processo do BANCO CÉDULA, registra eventuais perdas operacionais incorridas, realiza avaliações periódicas de suas atividades e processos, identificando os riscos inerentes e a efetividade dos controles praticados e quando necessário implementa planos de ação para mitigar os riscos e aprimorar os controles, mecanismo que resulta em menor exposição a riscos.

O BANCO CÉDULA gerencia seus riscos operacionais em total consonância com as disposições regulamentares e as melhores práticas do mercado.

Para o adequado controle do RO o BANCO CÉDULA possui estrutura de Tecnologia da Informação (TI) compatível com o nível de apetite de risco determinado pela Alta Administração e todos os sistemas utilizados nas rotinas do BANCO CÉDULA possuem limites operacionais em conformidade com as atividades desenvolvidas por cada colaborador, bem como são capazes de gerar todos os relatórios necessários para a aferição dos acessos e de qual *login* tratou dos dados no sistema, sendo que todas as senhas de acesso devem ser alteradas periodicamente, o que já se encontra parametrizado pelos sistemas.

Destaca-se que todos os sistemas, processos e infraestrutura de TI cumprem com as seguintes premissas:

a) asseguram a integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados;

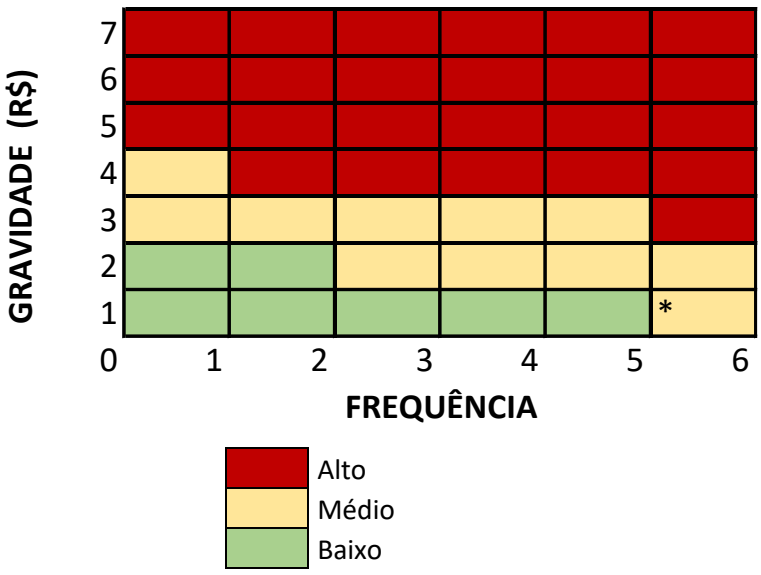
b) são robustos e adequados às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse;

c) incluem mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques digitais.

Para fins de monitoramento deve-se aplicar na análise principalmente os seguintes fatores: impacto do risco (gravidade); reiteração do evento (frequência) que dispostos matricialmente indicarão qual o grau de impacto do referido risco, conforme exemplificado abaixo, optando-se, sempre que possível, por uma mensuração financeira, todavia há situações onde não será possível mensurar o impacto (regulatório e/ou reputação, etc...), nesses casos deve-se mensurar por uma projeção aproximada do impacto para a instituição classificando como de maior ou menor gravidade, conforme o caso:

GRAVIDADE (R$)	
7	Acima de 500.000
6	Acima de 100.000 até 500.000
5	Acima de 50.000 até 100.000
4	Acima de 10.000 até 50.000
3	Acima de 5.000 até 10.000
2	Acima de 1.000 até 5.000
1	Até 1.000

FREQUÊNCIA (EVENTOS)	
6	ACIMA DE 5
5	5
4	4
3	3
2	2
1	1



* Para mais de 5 eventos deve ser verificado se os valores totais expostos não superam o montante de R$ 50.000,00, tido como valor de alto risco adotado pelo BANCO CÉDULA.

8.1. IDENTIFICAÇÃO DOS RISCOS

A identificação dos riscos visa garantir que os principais riscos sejam de ciência de todos os envolvidos e responsáveis. As fontes de identificação estão no mapeamento dos processos (políticas, manuais procedimentos, matrizes de riscos locais e globais), análise de produtos e serviços e levantamentos em geral.

8.2 - AVALIAÇÃO DOS RISCOS

Após a identificação os riscos devem ser avaliados e aprovados pelas alçadas competentes. Em complemento, para os riscos não aceitos pela instituição, um plano de ação será elaborado e acompanhado.

8.3 - MONITORAMENTO DE RISCO

O monitoramento dos riscos é realizado através da criação de indicadores de riscos em linha com os principais riscos identificados pela matriz. Em complemento, são realizados testes internos que avaliam os controles previamente entendidos como críticos para o BANCO CÉDULA.

Neste sentido é feito o cruzamento dos dados em conformidade com o determinado pelo CMN, com a realização de testes de estresse tomando por metodologia a análise de sensibilidade para aferir a probabilidade e constatar as eventuais perdas atreladas ao RO.

Estes testes devem ser realizados no mínimo a cada trimestre, com todos os seus resultados devidamente documentados e entregues para o Nível Estratégico tomar as medidas que entender cabíveis.

Anualmente, devem ser elaborados relatórios circunstanciais a serem apresentados para a alta administração e divulgados conforme determinação do CMN na própria página do BANCO CÉDULA na rede mundial de computadores.

8.4 - MITIGAÇÃO DE RISCO

A mitigação de riscos ocorre a partir do momento em que os riscos a que a Instituição incorre são reconhecidos e monitorados. A mitigação de riscos ocorre através da implementação de planos de ação a minimização ou extinção do impacto destes riscos no BANCO CÉDULA.

8.5 - REPORTE DE RISCOS

A etapa de reporte assegura que todos os processos de gestão de riscos e controles sejam divulgados à Administração. A divulgação ocorre em forma de comitês e reuniões tempestivas de acompanhamento.

8.6 - COMUNICAÇÃO

A comunicação de falhas e pontos de melhoria é realizada através de comitês e reuniões de acompanhamento.

Eventuais deficiências e solicitação de revisão, bem como divulgações e publicações de novos procedimentos, ficará a cargo da Diretoria de risco, que informará as áreas envolvidas.

8.7 - PLANO DE CONTINUIDADE DOS NEGÓCIOS

Para as principais ameaças de riscos já está em vigor o plano de continuidade dos negócios, que tem como objetivo assegurar a continuidade das operações dos processos de negócios, levando em consideração a inexistência de pessoas, dados, sistemas, equipamentos e instalações.

9 – DA CONTRATAÇÃO DE TERCEIRIZADOS

O BANCO CÉDULA, com a finalidade de otimizar os seus recursos humanos, adota como parte de sua política a contratação de colaboradores terceirizados que deverão passar por criteriosa avaliação de suas competências especialmente as qualificações necessários ao exercício da atividade para a qual tenha sido contratada, devendo conter, em todos os contratos, cláusulas de confidencialidade e respeito às legislações aplicáveis ao BANCO CÉDULA, especialmente sobre a proteção e tratamento de dados de clientes.

Essa terceirização poderá se dar através da contratação de empresas ou por meio de contratação direta de prestadores de serviços autônomos especializados para atividades pontuais, devendo constar do planejamento da alta administração recursos suficientes para a avaliação, gerenciamento e monitoramento do RO decorrente de serviços terceirizados relevantes para o funcionamento regular da instituição.

Para as atividades de *facilities* poderão contratadas empresas especializadas para tais atribuições, de forma a garantir a manutenção das atividades de limpeza, segurança, etc.

Todo e qualquer colaborador terceirizado, ou de empresa terceirizada, deve assinar um compromisso de cumprir com as políticas internas do BANCO CÉDULA, bem como as normas contidas no seu Código de Ética.

Devem constar dos contratos referentes à prestação de serviços terceirizados de TI a permissão **de acesso do Banco Central do Brasil a**: a) termos firmados; b) documentação e informações referentes aos serviços prestados e c) dependências do contratado.

10 – EXCEÇÕES À POLÍTICA

Toda e qualquer exceção à política deverá ser encaminhadas ao conhecimento da Diretoria de RO que ficará encarregado de avaliar e, se achar necessário, levar para o Nível Estratégico, que estudará o fato e indicará os procedimentos a serem adotados.

11 – ALTERAÇÃO E REVISÃO DA POLÍTICA

Quaisquer alterações das políticas estabelecidas deverão ser encaminhadas ao conhecimento da Diretoria de RO que ficará encarregada de avaliar e, se achar necessário, levar para o Nível Estratégico, que estudará o fato e indicará os procedimentos a serem adotados**.**

Anualmente será revisada a Política de RO.

Área responsável pela Confecção	Diretoria de Riscos e Compliance
Área responsável pela Aprovação	Conselho de Administração
Vigência	A contar de 20/12/2023