Sumário:

01. OBJETIVO

Esta política faz parte da estrutura de gerenciamento contínuo e integrado de riscos do Conglomerado Financeiro BOCOM BBM ("BOCOM BBM") e tem como objetivo apresentar um conjunto de princípios e diretrizes que devem nortear a estratégia de controle e gerenciamento do **Risco Operacional** do BOCOM BBM.

02. CONCEITUAÇÃO/DEFINIÇÃO

02.01. **Risco operacional**

Conforme estabelecido no art. 32 da Resolução nº 4.557, de 2017, Risco Operacional é a possibilidade de perda direta ou indireta, resultante de eventos externos ou de deficiência, inadequação ou falhas de processos internos, pessoas ou sistemas. Soma-se à definição de risco operacional, o risco legal que está associado à inadequação ou associado à inadequação ou deficiência em contratos firmados pela instituição, às sanções em razão de descumprimento de dispositivos legais e às indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

02.02. **Categorias de Risco Operacional**

Nos últimos anos, o Risco Operacional se tornou mais complexo, à medida que seu número e diversidade de tipos aumentaram. As principais categorias gerenciadas pelo BOCOM BBM são:

02.02.01. Fraudes Internas

Perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar regulamentos, leis ou as políticas da empresa, que envolvam pelo menos uma parte interna, excluindo diversidade/acontecimentos discriminatórios.

02.02.02. Fraudes Externas

Perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar leis, praticados por um terceiro; podem incluir lavagem de dinheiro, roubo de identidade e deturpação de ativos ou receitas.

02.02.03. Demandas Trabalhistas e segurança deficiente do local de Trabalho

Perdas devido a recrutamento inadequado/ineficaz de pessoal, ausência de gestão de talentos, treinamento e ou alto *turnover*. Também considera perdas decorrentes de atos inconsistentes com contratos ou leis trabalhistas, saúde, segurança, pagamento de reclamações por lesões corporais, ou de diversidade/eventos discriminatórios.

02.02.04. Práticas inadequadas relativas a usuários finais, clientes, produtos e serviços

Perdas decorrentes de uma falha não-intencional ou negligente para cumprir uma obrigação profissional com clientes específicos (incluindo exigências fiduciárias e de adequação ao perfil do cliente), ou da

natureza ou desenho de um produto ou serviço. Podem incluir perdas de prazos ou orçamentos de projetos perdidos, bem como entregas perdidas / incompletas e / ou de baixa qualidade.

02.02.05. Danos a ativos físicos próprios ou em uso pela Instituição

Prejuízos decorrentes de perdas ou danos aos ativos físicos (instalações) ocasionados por desastres naturais ou outros acontecimentos (ação humana por exemplo);

02.02.06. Situações que acarretem a interrupção das atividades (Indisponibilidade) da instituição ou a descontinuidade dos serviços prestados

Perdas decorrentes de ruptura nos negócios, ocasionadas pela ausência ou não fornecimento de serviços essenciais, seja de agentes internos ou externos à empresa.

02.02.07. Falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI)

Perdas decorrentes de falhas em sistemas, processos ou na infraestrutura de Tecnologia da Informação decorrentes de fatores internos (falha em backup, indisponibilidade dos sistemas, entre outros) ou externos (má desempenho do prestador de serviço contratado, efeitos da natureza, entre outros).

02.02.08. Falhas na execução, cumprimento de prazos e gerenciamento das atividades (falhas de processos)

Perdas decorrentes na administração, condução, execução e gerenciamento das atividades vinculadas aos processos de negócios da instituição.

02.02.09. Dano à Segurança da Informação

Perda em função de roubo, acesso indevido ou vazamento de dados pessoais ou sensíveis. Inclui perdas associadas ao acesso não autorizado a sistemas seja por ausência de segregações, por meio de *hacking*, ou danos aos sistemas, entre outros motivos.

02.03. **Fatores de risco**

- Pessoas: Relacionam-se à competência, conduta ética e desempenho das suas atribuições;
- Processos: Fluxos e etapas do desenvolvimento de produtos e serviços e condução de atividades da organização, definição dos normativos internos e aderência à legislação;
- Tecnológicos: Sistemas, Infraestrutura e arquitetura de TI, disponibilidade de armazenamento, processamento e rede;
- Externos: Relacionados com as ocorrências do meio ambiente, do ambiente regulatório do país e do ambiente social (partes relacionadas, com principal exemplo: prestadores de serviços).

02.04. **Perda Operacional**

Conforme definição estabelecida no § 1º do art. 34 da Resolução nº 4.557, de 2017, define-se perda operacional como o valor quantificável associado aos eventos de risco operacional mencionados no item 02.01 e 02.02. Devem constar da base de dados de risco operacional as perdas operacionais associadas

ao risco de crédito, ao risco de mercado, ao risco social, ao risco ambiental e ao risco climático, independentemente de também constarem de outras bases de dados.

Conforme definição estabelecida no art. 3º da Circular BCB nº 3.979, de 30 de janeiro de 2020, e alterações promovidas pela Resolução BCB nº 556, de 1º de abril de 2026, as perdas operacionais devem ser registradas e mensuradas de forma consistente com os registros contábeis da instituição, observando-se os seguintes conceitos:

I. Valor bruto da perda: valor quantificável associado ao evento de risco operacional, incluindo provisões e despesas, antes de eventual recuperação;

II. Valor recuperado: recurso financeiro efetivamente recebido de terceiros com o propósito de ressarcir ou indenizar a instituição por uma perda operacional, desde que devidamente comprovado e registrado contabilmente;

III. Perda líquida: corresponde ao valor da perda efetiva deduzido dos valores recuperados, incluindo provisões para contingências e suas respectivas reversões.

Não serão considerados como recuperação valores provenientes de partes relacionadas, valores não registrados contabilmente como receita ou efeitos positivos decorrentes de dedutibilidade fiscal.

02.04.01. Perda Efetiva

A perda efetiva decorre da manifestação de evento de risco operacional que causou perda financeira ou contábil para a empresa, refletindo diretamente no seu resultado.

02.04.02. Perda não Efetiva ou Potencial

Situação em que os eventos de risco operacional não causaram perda efetiva para a empresa, por conta da intervenção de agente interno ou externo, antes da efetivação da perda.

02.05. **Incidente Operacional**

Ocorrência de eventos de não-conformidade associados aos riscos operacionais (conforme definições 02.01 e 02.02), com origem em um ou mais fatores de risco (conforme definição 02.03) e podendo ou não incidir em perdas operacionais (conforme definição 02.04).

02.06. **Incidente Operacional Relevante**

Incidente operacional que:

- Incidiu ou poderia vir a incidir em perdas financeiras relevantes;
- Afetou ou poderia afetar de forma relevante processos negócios;
- Causou ou poderia causar danos aos dados ou informações sensíveis ou ainda ter impacto significativo para nossos clientes ou imagem da Instituição.

Na intranet da área de Controles Internos divulgamos critérios para orientação quanto a relevância de um incidente operacional.

02.07. Risco cibernético

Trata-se de uma subcategoria do risco de segurança da informação, explicado no item 02.02.09, mas dada a sua relevância, algumas vezes é tratado de forma separada. Representa a possibilidade de ocorrência de perdas resultantes de incidentes cibernéticos.

02.08. Incidentes Cibernéticos

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.

02.09. Incidente relevante de segurança cibernética

Incidente que afeta processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes.

02.010. Gestão da Continuidade de Negócios

Consiste em um conjunto de estratégias para assegurar a continuidade das atividades da instituição e limitar perdas decorrentes da interrupção dos processos críticos de negócio. Fazem parte da gestão da continuidade estratégia:

- A política de Continuidade de Negócios com o objetivo de estabelecer a estrutura organizacional e as principais diretrizes e regras;
- Os planos de continuidade de negócios que estabeleçam procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como as ações de comunicação necessárias; e
- Análise de Impacto nos Negócios (BIA - *Business Impact Analysis*), cujo objetivo é identificar os principais processos críticos e ativos que o suportam, determinar os principais fatores para implementação de planos de emergências e garantir que os principais sistemas sejam restaurados primeiro no caso de uma interrupção.
- Testes e revisões dos planos de continuidade de negócios com periodicidade adequada.

03. ABRANGÊNCIA / ÁREAS ENVOLVIDAS

03.01. Abrangência da Estrutura de Risco

A estrutura de gerenciamento de risco deve ser:

- Compatível com o modelo de negócio, com a natureza das operações e com a complexidade dos produtos, dos serviços, das atividades e dos processos atuais do BOCOM BBM;
- Proporcional à dimensão e à relevância da exposição aos riscos, segundo critérios definidos pela instituição na Declaração de Apetite por Riscos;
- Adequada ao perfil de riscos e à importância sistêmica do BOCOM BBM; e

- Capaz de avaliar os riscos decorrentes das condições macroeconômicas e dos mercados em que o BOCOM BBM atua.

Além disso, deve ser adequada ao segmento de classificação, nos termos do art. 2º da Resolução nº 4.553, de 2017 do Banco Central, ao qual o Banco se enquadra atualmente. As informações descritas estão adequadas para o Segmento 3 (S3). Caso o BOCOM BBM venha a ser enquadrado nos Segmento 1 (S1) ou no Segmento 2 (S2) será necessário realizar a revisão deste documento.

A estrutura de gerenciamento do risco operacional do BOCOM BBM deve prever:

- políticas que estabeleçam critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional;
- implementação de estrutura de governança de TI consistente com os níveis de apetite por riscos estabelecidos na RAS;
- sistemas, processos e infraestrutura de TI que:
    a) assegurem integridade, segurança e disponibilidade dos dados armazenados, processados ou transmitidos e dos sistemas de informação utilizados;
    b) contenham mecanismos de proteção e segurança de redes, sítios eletrônicos, servidores e canais de comunicação com vistas a reduzir a vulnerabilidade a ataques digitais;
    c) adotem procedimentos para monitorar, rastrear e restringir acesso a dados sensíveis, redes, sistemas, bases de dados e módulos de segurança;
    d) monitorem as falhas na segurança dos dados e as reclamações dos usuários finais a esse respeito; e
    e) sejam adequados às necessidades e às mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse;

03.02. **Abrangência da política**

A política se aplica ao Conglomerado BOCOM BBM e as suas PARTES INTERESSADAS. As PARTES INTERESSADAS são funcionários, estagiários, acionistas, clientes, contrapartes, fornecedores e as comunidades em que atuamos.

03.03. **Estrutura Organizacional**

Compõem a estrutura de gerenciamento de risco operacional o Comitê de Risco, o Comitê de Risco Operacional e Controles Internos e as áreas de Risco, Controles Internos e Segurança da Informação.

Além disso, o Compliance e Auditoria Interna, de forma independente, autônoma e imparcial, atuam na avaliação da qualidade e da efetividade dos sistemas e processos de controles internos, gerenciamento de riscos e governança corporativa da instituição do BOCOM BBM.

04. RESPONSABILIDADES

04.01. **Responsáveis pela execução das atribuições desta política**

Quanto à execução, as unidades abaixo têm as seguintes responsabilidades:

04.01.01. Conselho de Administração/Comitê de Risco/Diretoria

- Aprovar anualmente da política de gerenciamento de risco operacional para as instituições do BOCOM BBM;
- Fixar os níveis de apetite de risco operacional do BOCOM na RAS; e
- Realizar a tomada de decisões estratégicas para o controle de Risco Operacional.

04.01.02. Comitê de Risco Operacional e Controles Internos

- Divulgar da cultura orientada ao gerenciamento dos Riscos;
- Definir papéis e responsabilidades de cada integrante da estrutura de Risco Operacional;
- Dar ciência ao Comitê de Risco sobre o cumprimento de suas recomendações e indagações sobre o adequado funcionamento do sistema de gerenciamento de risco operacional;
- Analisar os incidentes relevantes que tenham ocorrido, e caso necessário, decidindo ações a serem tomadas no sentido de mitigar riscos incorridos;
- Avaliar os níveis de apetite por risco operacional fixados na RAS e as estratégias para o seu gerenciamento;
- Analisar situações relevantes de exposição da instituição a riscos operacionais, propondo adequações necessárias à organização; e
- Analisar situações não previstas nessa política.

04.01.03. Controles Internos

- Propor uma política de gerenciamento de riscos operacionais e sugerir alterações quando forem necessárias para serem aprovadas junto ao Conselho de Administração e Diretoria;
- Difundir a cultura de conscientização de risco operacional, a fim de garantir que todos os funcionários tenham plena consciência da importância do gerenciamento de risco operacional.

Com relação aos macroprocessos e processos:

- Identificar, juntamente com as áreas de negócios, cada macroprocesso/processo existentes no BOCOM BBM;
- Buscar elaborar, em conjunto com os gestores das áreas, procedimentos contendo a descrição dos (macro)processos, bem como a identificação de riscos operacionais inerentes aos mesmos e respectivos controles;
- Buscar estabelecer, em conjunto com os gestores das áreas, os indicadores chaves de risco;
- Avaliar os potenciais efeitos dos riscos operacionais aos quais o BOCOM BBM está exposto e reportar suas conclusões interna e externamente, quando necessário;

As avaliações são priorizadas e frequentemente são realizadas quando:

a. Ocorreu um incidente operacional relevante no banco ou em outros bancos;
b. Houve a identificação da exposição do Banco a um risco operacional relevante;
c. Há alterações significativas em procedimentos de alguma operação;
d. Há alterações significativas nos sistemas operacionais;
e. Quando novos produtos são lançados;
f. Quando regulação com impacto relevante é emitida ou atualizada;
g. Por solicitação do órgão regulador ou da diretoria.

Com relação aos eventos de riscos operacionais:

- Gerir a base de dados de registros de eventos de risco operacional;
- Monitorar periodicamente os riscos operacionais identificados com objetivo de verificar se eventuais mitigadores adotados estão sendo efetivos e/ou se há aumento de frequência de incidentes relativos a estes riscos;
- Elaborar relatórios de avaliação dos incidentes operacionais relevantes, identificando os controles estabelecidos para correção de falhas identificadas e eventuais perdas operacionais.

Com relação aos processos terceirizados:

- Identificar os riscos e controles existentes nos processos cujos serviços sejam terceirizados;
- Manter a Política de Seleção, Contração e Gestão de Fornecedores atualizada no que tange aos critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional..

Com relação a continuidade operacional:

- Gestão da continuidade dos negócios contemplando as estratégias a serem adotadas para assegurar condições de contingência das atividades mais críticas e mitigar graves perdas decorrentes de risco operacional;

Com relação aos reportes Regulatórios:

- Em conjunto com a área de Compliance, encaminhar relatórios para os órgãos de administração e para disponibilidade à CVM, até o último dia útil de abril de cada ano, contendo os eventos de risco operacional, bem como sua avaliação de risco e o andamento/conclusão dos eventuais mitigadores;
- Em conjunto com a área de Compliance, comunicar os Incidentes Relevantes de Segurança Cibernética, conforme prazos e público previstos nas normas vigentes e nas políticas internas. Os incidentes devem ser comunicados à BSM mensalmente.
- Encaminhar ao Banco Central do Brasil o Demonstrativo de Risco Operacional (DRO), documento de código 5050, com periodicidade semestral, relativamente às datas-bases de 30 de junho e 31

de dezembro, contendo as informações da base de dados de risco operacional, conforme estabelecido na Circular BCB nº 3.979, de 30 de janeiro de 2020, e na Instrução Normativa BCB nº 700, de 13 de janeiro de 2026, devendo, para o BOCOM BBM, enquadrado no Segmento 3 (S3), ser realizado a partir da datas-bases de 2026.

Com relação aos limites estabelecidos na RAS:

- Responsável por calcular, avaliar, reportar e quando necessário, garantir o reenquadramento dos indicadores de risco operacional e os indicadores de tecnologia da informação presente na RAS. A descrição dos indicadores, bem como o cálculo e o acompanhamento estão descritos no procedimento de Gerenciamento de Apetite de Risco.

04.01.04. Tecnologia da Informação

- Prestar o suporte tecnológico necessário para o desenvolvimento dos trabalhos de acompanhamento e controle de risco operacional;

04.01.05. Segurança da Informação

- Auxiliar, em sinergia com a área de Controles Internos, na identificação integrada dos riscos à Instituição;
- Analisar os incidentes de risco cibernéticos dando ciência ao Comitê de Risco de eventuais ações mitigatórios ou impactos aos processos da Instituição.
- Realizar a revisão das medidas de segurança e de sigilo de dados, especialmente depois da ocorrência de falhas e previamente a alterações na infraestrutura ou nos procedimentos;
- Realizar de testes que assegurem a robustez e a efetividade das medidas de segurança de dados adotadas;
- Elaborar relatórios que indiquem procedimentos para correção de falhas identificadas;

04.01.06. Auditoria Interna

- Avaliar periodicamente a qualidade, integridade, consistência e governança da base de dados de risco operacional, incluindo os processos de identificação, coleta, tratamento, agregação e reporte das informações.
- Verificar a aderência dos processos de gerenciamento de risco operacional e da base de dados às normas e regulamentações vigentes, bem como às políticas internas da instituição.
- Avaliar previamente as solicitações de descarte de eventos da base de dados de risco operacional, emitindo parecer sobre a adequação, fundamentação e inexistência de exposição residual associada aos eventos propostos para exclusão.
- Reportar eventuais deficiências identificadas e acompanhar a implementação de planos de ação corretivos.

04.01.07. Gestores dos processos

- Manter a ciência dos riscos inerentes aos seus processos, avaliando-os quanto à probabilidade de ocorrência e seus possíveis impactos;
- Auxiliar na elaboração dos mapeamentos de processos;
- Informar sobre alterações em processos, rotinas e controles que possam eventualmente causar mudanças na avaliação de exposição a risco;
- Gestão dos negócios observando as diretrizes da alta administração, tais como a definição do Apetite a Risco; e
- Difundir a cultura de conscientização de risco operacional, a fim de garantir que os todos funcionários tenham plena consciência da importância do gerenciamento de risco operacional.

04.01.08. Demais funcionários da Instituição

É responsabilidade de todos os colaboradores, quando identificadas ocorrências relacionadas aos riscos operacionais, a imediata comunicação à área de Controles Internos para as providências cabíveis.

04.02. **Responsáveis pelo monitoramento da execução das atribuições desta política**

É de responsabilidade do Gestor da área de Controles Internos o monitoramento da execução das atribuições desta política.

04.03. **Responsáveis pela manutenção desta política**

É de responsabilidade da área de Controles Internos a manutenção desta política.

05. ALÇADAS

O Comitê de Risco Operacional e Controle Internos, a Diretoria e o Conselho de Administração devem aprovar esta política.

O Comitê de Risco Operacional e Controles Internos deve analisar situações não previstas nessa política e avaliar se será necessário à aprovação do Conselho de Administração.

06. DIRETRIZES:

06.01. **Princípios**

06.01.01. Melhores Práticas

A área de Controles Internos, responsável pela gestão de risco operacional, analisa e acompanha as melhores práticas de controle a serem adotadas para garantir segurança e confiabilidade dos processos.

06.01.02. Gestão integrada de Risco

Identificado um risco operacional, a área de Controles Internos deve buscar analisar o eventual efeito sob demais riscos que o Banco gerencia. Atualmente os principais riscos que o BOCOM BBM busca mensurar, avaliar, monitorar, reportar, controlar e mitigar são:

- risco de crédito;
- risco de mercado
- risco de liquidez;
- risco estratégico;
- risco regulatório;
- risco reputacional;
- risco de segurança da informação;
- risco social;
- risco ambiental;
- risco climático; e
- risco operacional, conforme tratado nessa política.

O gerenciamento de riscos deve ser integrado, possibilitando a identificação, a mensuração, a avaliação, o monitoramento, o reporte, o controle e a mitigação dos efeitos adversos resultantes das interações entre os riscos mencionados.

06.01.03. Transparência de Informações

A descrição da estrutura de gerenciamento de risco operacional é evidenciada por meio desta política, que fica disponível através do site institucional do Banco.

06.01.04. Cultura Orientada à Risco

A cultura de gerenciamento de riscos operacionais é disseminada em todas as áreas da instituição bem como para as nossas partes relacionadas. Sempre que possível devem ser realizados treinamentos para reforçar a importância do gerenciamento dos riscos operacionais.

06.02. **Fases do Gerenciamento de Risco Operacional**

O processo de gestão do risco operacional do BOCOM BBM está dividido metodologicamente duas fases: Preventiva e Reativa.

06.02.01. Fase Preventiva

Objetivo

Esta fase tem como objetivo identificar os eventos de risco operacionais antes da sua materialização e a criação de métodos que permitam evitar, mitigar, transferir ou aceitar o risco.

Etapas

Deve compreender as seguintes etapas:

I. Identificação: identificar eventos de risco operacional, apontando as áreas de incidência, causas e potenciais impactos financeiros.
II. Avaliação: quantificar a exposição ao risco operacional com o objetivo de avaliar o impacto nos negócios.
III. Controle: registrar o comportamento dos riscos operacionais, limites, indicadores e eventos de perda operacional, bem como implementar mecanismos de forma a garantir que os limites e os indicadores de risco operacional permaneçam dentro dos níveis definidos.
IV. Mitigação: criar e implementar mecanismos para mitigar o risco operacional, buscando reduzir as perdas.
V. Monitoramento: identificar as deficiências do processo de gestão do risco operacional.

Ferramentas

Exemplos de ferramentas que auxiliam na mitigação de riscos operacionais na fase preventiva:

- Definição de Políticas e Códigos de Ética e Conduta;
- Mapeamento de Processos e elaboração de Fluxogramas;
- Formalização de Manuais operacionais;
- Treinamentos;
- Estabelecimento de Monitorações;
- Implantação de controles de acesso (físicos e lógicos), instalação de programas antivírus, backup periódico de dados;
- Testes de Continuidade; entre outros

06.02.02. Fase Reativa

Objetivo

Tem como objetivo o tratamento de eventos de risco operacionais já materializado, podendo os mesmos terem ou não ocorrido em perdas operacionais.

Etapas Gerais

I. Recepção do Registro de ocorrência de um incidente;
II. Análise de suas causas e dos impactos sobre os processos de negócio;
III. Identificação do evento com outros tipos de risco (ex: risco cibernético ou socioambiental);
IV. Orientação acerca das ações que deverão ser tomadas para a solução de curto prazo e para evitar que novos incidentes ocorram.

06.03. **Registro de Incidente**

06.03.01. Quem pode realizar um registro de incidente?

Ocorrido um incidente, qualquer colaborador pode fazer o reporte do mesmo. O registro será feito via formulário eletrônico, disponível no browser de todos os colaboradores, e estará sujeito à

avaliação/aprovação do gestor da área reportada, à classificação de risco pelo gestor da área impactada e à classificação da probabilidade de ocorrência pelo gestor da área causadora.

Vale mencionar que a área de Controles Internos também poderá classificar a probabilidade de ocorrência considerando as informações históricas na base de incidentes.

06.03.02. Base de Dados de Incidentes

Para cada registro de incidente, devem ser armazenadas as seguintes informações:

- O código interno de identificação do evento de risco operacional;
- A categoria de risco operacional, conforme item 02.02.
- Os fatores de risco, conforme item 02.03, indicando o nome do processo, sistema ou qual fator externo.
- A identificação da unidade de negócio em que se verificou a ocorrência, conforme o Anexo I, item 014.01 desta política;
- As datas de ocorrência e de descoberta;
- A descrição do evento ocorrido, sempre que possível informando a causa raiz;
- A solução de curto prazo;
- Os controles mitigadores para evitar que o evento ocorra novamente;
- As áreas impactadas;
- Os processos impactados;
- O valor bruto acumulado da perda (quando aplicável);
- O valor acumulado da perda recuperado por seguro ou por outros meios (quando aplicável);
- A fonte do ressarcimento, para eventos de recuperação de perda (quando aplicável);
- A indicação, com base em critérios consistentes e passíveis de verificação, da Categoria Nível 1 e da Categoria Nível 2 em que se enquadra o evento de risco operacional, conforme o Anexo II desta política;
- A associação, quando aplicável, aos demais tipos risco aos quais o Banco está sujeito: risco de crédito; risco de mercado; risco socioambiental; risco de liquidez; risco de regulatório; risco de reputacional e risco cibernético.

06.03.03. Tratamento de Perdas

Para a formação da base de dados de perdas internas serão consideradas as perdas de risco operacional materializadas na forma de despesa.

O registro e tratamento das perdas operacionais devem observar os conceitos de valor bruto da perda, valor recuperado e perda líquida definidos na seção 02.04 desta política, assegurando consistência com os registros contábeis da instituição e com as exigências regulatórias aplicáveis.

06.03.04. Agregação de Eventos de Risco Operacional

Os eventos de risco operacional devem ser registrados de forma individualizada, sendo admitida sua agregação apenas quando compartilharem uma mesma causa raiz, com base em critérios consistentes, rastreáveis e passíveis de verificação.

A agregação de eventos deve observar:

I. a existência de vínculo causal comum entre os eventos;
II. a consistência na classificação do risco;
III. a manutenção de documentação que comprove os critérios utilizados para agregação.

É vedada a agregação de eventos que não possuam relação direta entre si.

Quando aplicável, deve ser mantida identificação que permita relacionar os eventos individualizados ao evento agregador, assegurando a rastreabilidade das informações e a transparência da base de dados.

A adoção de critérios de agregação não deve comprometer a qualidade das informações utilizadas para fins de monitoramento de risco, reporte regulatório ou apuração de capital.

06.03.05. Solicitação de informações adicionais

Após o registro na base de dados de Controles Internos, os incidentes serão analisados e terão suas causas raízes identificadas.

É válido ressaltar que além de Controles Internos, as áreas de Risco, Segurança da Informação, Auditoria Interna e o Comitê de Risco Operacional e Controles Internos também são notificadas quanto ao registro de incidente. E cada um desses núcleos pode solicitar mais informações, caso julgue necessário, quer aos envolvidos no evento, quer ao funcionário que efetuaram o reporte.

06.04. **Reporte de Fraudes**

O BOCOM BBM tem como postura repudiar toda e qualquer forma de atividade fraudulenta por parte de seus funcionários, prestadores de serviços, agentes e corretores. Por atividade fraudulenta entende-se falsificação, desvio de recursos, roubo, uso pessoal de ativos, corrupção ativa e passiva, apropriação indébita, pagamentos e recebimentos questionáveis, improbidade administrativa, entre outras.

Pensando sempre no objetivo de proporcionar bons resultados, com total confiabilidade, segurança e transparência, as fraudes devem ser comunicadas à Gerência de *Compliance* de forma que a mesma inicie as investigações pertinentes. Ressalta-se que, por seu teor sensível, as suspeitas de fraudes serão tratadas de forma sigilosa.

06.05. Incidentes de Segurança Relevantes

Identificado um incidente de danos à integridade da informação, vazamento de dados ou ataques cibernéticos, a área de controles Internos deverá acionar a área de Segurança da Informação. Esta área é responsável pelo direcionamento desses eventos ao Comitê de Segurança da Informação e acompanhamento de eventuais tratamentos estabelecidos. A área de Segurança da Informação tem como papel reafirmar o nosso compromisso com a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações sensíveis e por adotar medidas para reduzir a nossa exposição à ataques cibernéticos.

Os incidentes de segurança considerados relevantes devem ser notificados ao Banco Central e à Superintendência de Relações com o Mercado e Intermediários (SMI).

06.06. Incidentes que acionam o Plano de Continuidade de Negócios

Qualquer evento que tenha provocado o acionamento de plano de continuidade de negócios deve ser reportado aos órgãos de administração e à SMI.

O reporte deve compreender as causas do acionamento, indicando os processos críticos afetados. Ademais, os mitigadores adotados ou que se pretende adotar, tempo consumido na solução do evento e qualquer outra informação relevante.

07. CONSIDERAÇÕES FINAIS

Este documento é de uso estritamente interno, não devendo ser disponibilizado a terceiros sem que o Gestor da área de Controles Internos seja consultado.

08. LEGISLAÇÃO/REGULAÇÃO RELACIONADA

- Roteiro do Programa de Qualificação Operacional (PQO), de 02/01/2025
- Resolução CMN nº 5.076, de 18 de maio de 2023;
- Resolução CMN nº 4.557, de 23 de fevereiro de 2017;
- Circular BCB nº 3.979 de 30 de janeiro de 2020;
- Instrução Normativa BCB n° 33 de 29 de outubro de 2020;
- Resolução BCB nº 356, de 28 de novembro de 2023;
- Resolução CMN nº 4.893, de 26 de fevereiro de 2021;
- Resolução CVM nº 35, de 26 de maio de 2021;
- Resolução CMN nº 4.943, de 15 de setembro de 2021;
- Resolução CMN nº 4.968, de 25 de novembro de 2021;
- Instrução Normativa BCB nº 700, de 13 de janeiro de 2026;
- Resolução BCB nº 556, de 1º de abril de 2026;

09. REFERÊNCIA INTERNA

- Declaração de Apetite de Risco;

- Política de Controles Internos;
- Política de Gerenciamento de Risco de Mercado;
- Política de Gerenciamento de Risco de Crédito;
- Política de Gerenciamento de Risco de Liquidez;
- Política de Gestão da Continuidade Operacional;
- Política de Gerenciamento de Capital;
- Política de Divulgação de Informações;
- Política de Proteção de Dados;
- Política de Segurança da Informação;
- Política de Backup e Restore;
- Política de Aprovação de Produtos; e
- Política de Avaliação de Processos.

010. BIBLIOGRAFIA

- COSO 2017;
- Sound Practices for the Management and Supervision of Operational Risk;
- International Convergence of Capital Measurements and Capital Standards (Basiléia II);
- International Regulatory Framework for Banks (Basiléia III);
- Políticas e Procedimentos de Risco Operacional do Bank of Communications.

011. GLOSSÁRIO

- Bacen – Banco Central do Brasil;
- RAS: Risk Appetite Statement (Declaração de Apetite por Riscos).

012. CONTROLE DE VERSÕES

Versão	Data	Histórico	Autores
1.	27/06/2007	Criação do Documento	Risco Operacional
2.	10/12/2008	Revisão do Documento	Risco Operacional
3.	14/12/2009	Revisão do Documento	Risco Operacional
4.	31/12/2010	Revisão do Documento	Risco Operacional
5.	13/12/2011	Revisão do Documento	Risco Operacional
6.	03/12/2012	Revisão do Documento	Risco Operacional
7.	04/12/2013	Revisão do Documento	Risco Operacional
8.	13/12/2014	Revisão do Documento	Risco Operacional
9.	29/12/2015	Revisão do Documento	Risco Operacional
10.	30/12/2016	Revisão do Documento	Controles Internos e Risco Operacional
11.	26/12/2017	Revisão do Documento	Controles Internos e Risco Operacional
12.	27/03/2018	Revisão do Documento	Controles Internos e Risco Operacional
13	31/12/2018	Revisão do Documento	Controles Internos e Risco Operacional
14	31/12/2019	Revisão do Documento	Controles Internos e Risco Operacional
15	31/01/2021	Revisão do Documento	Controles Internos e Risco Operacional
16	31/01/2022	Revisão do Documento	Controles Internos e Risco Operacional
17.	31/01/2023	Revisão do Documento	Controles Internos e Risco Operacional
18.	02/08/2023	Revisão do Documento	Controles Internos e Risco Operacional
19.	02/01/2024	Revisão do Documento	Controles Internos e Risco Operacional
20.	02/01/2025	Revisão do Documento	Controles Internos e Risco Operacional
21.	09/06/2025	Revisão do Documento	Controles Internos e Risco Operacional
22.	12/06/2026	Revisão do Documento	Controles Internos e Risco Operacional

013. APROVAÇÕES

_____

Tatiana Ferro – Gerente de Controles Internos e Risco Operacional

_____

Monique Verboneen – CRO (Chief Risk Officer)
(Chief Risk Officer)

014. ANEXOS

014.01. **Unidades de Negócio**

Finanças Corporativas
Negociação e Vendas
Varejo
Comercial
Pagamentos e Liquidações
Serviços de Agente Financeiro
Administração de ativos
Corretagem de Varejo

014.02. Categorias de Risco Operacional

Nível 1	Nível 2
Fraudes Internas	Roubo e fraude (origem interna)
	Atividade não autorizada

Nível 1	Nível 2
Fraudes Externas	Roubo e fraude (origem externa)
	Segurança de sistemas
	Outros tipos de fraudes de origem externa

Nível 1	Nível 2
Demandas trabalhistas e segurança deficiente do local de trabalho	Relações de trabalho
	Diversidade e discriminação
	Segurança do local de trabalho

Nível 1	Nível 2
Práticas inadequadas relativas a clientes, produtos e serviços	Adequação de produto a cliente, divulgação de informações sobre produtos e serviços, desrespeito ao dever fiduciário
	Práticas impróprias de negócios e em mercados
	Falhas no produto
	Seleção, patrocínio e exposição
	Atividades de assessoramento

Nível 1	Nível 2
Danos a ativos físicos próprios ou em uso pela instituição	Desastres e outros eventos

Nível 1	Nível 2
Situações que acarretem a interrupção das atividades da instituição	Interrupção de atividades

Nível 1	Nível 2
Falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI)	Falhas em sistemas, processos ou infraestrutura de TI

Nível 1	Nível 2
Falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da instituição	Captura, execução e manutenção de transações
	Monitoramento e reporte
	Aquisição de clientes e documentação
	Gestão de contas correntes e de não correntistas
	Contrapartes em transações
	Representantes e fornecedores