Política Regulatória
de
Gestão de Risco Operacional

Banco Société Générale Brasil S.A. “BSGB”

Novembro/2025

THE FUTURE IS YOU SOCIETE GENERALE

ÍNDICE

1. INTRODUÇÃO

1.1. Objetivo

Esta Política estabelece a governança e os princípios gerais relativos à gestão do Risco Operacional com base nos padrões mínimos definidos pelo Grupo Société Générale (Grupo SG). Ela fornece uma **Estrutura de Gestão de Risco Operacional** e um conjunto de metodologias aplicáveis às exposições de risco operacional dentro do escopo, consistente com os normativos locais "Política de Gestão Integrada de Riscos" e com a "Declaração de Apetite por Riscos", bem como com a Resolução Conselho Monetário Nacional Nº 4.557/2017 publicada pelo Banco Central do Brasil. Os padrões, estrutura e práticas descritos nesta Política fornecem a base para gerir o Risco Operacional de forma abrangente, eficaz e consistente.

1.2. Escopo

Esta Política se aplica a todos os eventos de risco operacional dentro do escopo do Banco Société Générale Brasil S.A., referenciado nesta política simplesmente como "BSGB".

Todos os colaboradores[1] de todas as unidades de negócios e funções de suporte do BSGB, independentemente da linha de defesa à qual pertençam na estrutura de gestão de risco operacional devem aderir aos requisitos descritos nesta Política.

1.3. Governança da Política

A manutenção e atualização desta Política é da área de Gestão de Risco Operacional, a sua aprovação é responsabilidade do Comitê de Riscos do BSGB.

O Diretor de Riscos (CRO[2]) do BSGB é responsável por assegurar a aderência às Políticas e diretrizes internas, para o monitoramento do risco operacional.

Essa Política deverá ser revisada e atualizada no mínimo anualmente ou quando ocorrer quaisquer alterações significativas nas diretrizes internas do Grupo SG, Société Générale Américas (SG AMER) e/ou nos requisitos regulatórios, a fim de assegurar a integridade e adequação dos processos e atividades associadas à gestão do risco operacional.

1.4. Exceções e Violações da Política

Exceções são situações em que algumas disposições desta Política não são cumpridas, com autorização prévia explícita de indivíduos ou grupos designados.

Violações são situações em que algumas disposições desta Política não são cumpridas, sem que haja uma autorização explícita.

Qualquer exceção à Política pode ser aprovada temporariamente pelo CRO do BSGB, que pode consultar outros departamentos relevantes, bem como deve consultar os responsáveis regionais para suportar sua análise e decisão, conforme necessário. Exceções temporárias a esta Política aprovadas CRO e/ou Comitê de Riscos do BSGB, devem ser reportadas ao Comitê de Riscos do SG AMER.

Exceções permanentes que exijam alteração desta Política devem ser aprovadas previamente pelo Comitê de Riscos do BSGB e reportadas e/ou submetida (a depender do nível de criticidade da exceção) à aprovação do Comitê de Riscos do SG AMER.

Todas as exceções (temporárias ou permanentes) devem ser devidamente documentadas. As causas raízes das exceções e violações a esta Política devem ser gerenciadas conforme as diretrizes da Política Regional de Gestão de Risco Operacional.

1.5. Definição de Risco Operacional

Risco Operacional é o risco de perdas ou incidentes resultantes direta ou indiretamente de falha, deficiência ou inadequação de processos internos, pessoas e sistemas ou de eventos externos.

[1] **Colaboradores do BSGB:** são considerados colaboradores os (funcionários efetivos, estagiários, jovens aprendizes, VIEs, colaboradores terceirizados (consultores e contratados).
[2] ***CRO:*** *Chief Risk Officer – Diretor de Riscos*

Diferentemente dos outros tipos de risco (Risco de Mercado, Crédito e Liquidez), o risco operacional não é adquirido de forma voluntária e não é baseado em objetivos estratégicos e de negócios, pois são inerentes a qualquer produto, processo ou atividade. Sendo assim, os riscos oriundos de pessoas, sistemas, processos e eventos externos não podem ser totalmente eliminados.

Processos internos inadequados ou falhos, pessoas, sistemas e eventos externos podem resultar em consequências inesperadas ou indesejadas, com materialização de risco operacional com:

(i) **Impacto financeiro**: perda financeira, provisão ou ganho e/ou

(ii) **Impacto não financeiro**: descumprimento de exigências regulatórias e/ou legais, repercussão negativa (local, regional e/ou global) perante os clientes, parceiros e fornecedores, quase incidente, incidente operacional ou de segurança com impacto direto nas atividades vitais e críticas do BSGB (incluindo pagamentos), deterioração do clima social de uma equipe ou de uma ou mais unidade de negócio ou de suporte, eventos que afetem a saúde de um ou mais colaborador(es), conforme Matriz de Avaliação de Severidade de Impacto.

Em consonância com as categorias de risco operacional estabelecidas pelo Acordo de Basileia, o Grupo SG dispõe de uma taxonomia para classificação do risco operacional, a qual é composta por referências de tipos de eventos e situações que podem gerar risco operacional, agrupadas em categorias intermediárias, que por sua vez são agrupadas em sete categorias de eventos de risco, conforme abaixo:

1. **Erros na avaliação de risco/determinação do preço (incluindo risco de modelo):**
Qualquer erro no processo de avaliação da exposição ao risco (mercado/crédito) relacionado ao preço ou valor de uma operação, ligado, por exemplo, à falta de informação, problema de modelagem, uso incorreto de um modelo, avaliação incorreta de garantia/aval ou fiança (preço errado ou pacote inoperante), seja na constituição da operação ou na gestão do nível de risco durante toda a duração da transação.

2. **Erros de execução:**
Erro de processamento em qualquer estágio da operação (iniciação, notificação/relatório ou conclusão da transação), como erros de entrada, erros de confirmação, erro no processo de liquidação, reconciliação incorreta, procedimentos inadequados para identificação/resolução de exceções, condições inadequadas de retenção de documentos, títulos, ações, contratos, etc.

3. **Fraude e outras atividades criminais:**
Qualquer descumprimento deliberado das leis, regulamentos ou procedimentos existentes por um colaborador do BSGB ou por pessoas externas ao BSGB, incluindo o roubo de dinheiro, valores mobiliários ou ativos (físicos ou intelectuais) pertencentes ao Grupo SG ou mantidos pelo Grupo SG em nome de terceiros, transações fictícias ou não autorizadas, uso não autorizado de informações privilegiadas ou confidenciais, fraudes ou qualquer outra atividade criminosa que impacte os ativos ou instalações do Grupo SG, incluindo interferência maliciosa nos sistemas de informação.

4. **Perda de capacidade/ambiente operacional:**
Qualquer incidente (exceto cibernético) que afete os ativos do negócio e temporariamente comprometa a capacidade operacional do banco: destruição de edifícios, máquinas, perda ou desaparecimento de um fornecedor chave, destruição de dados referenciais e/ou transacionais, perda de equipes ou indivíduos-chave etc.

5. **Interrupção de Sistemas:**
Qualquer problema operacional ou técnico com o *hardware* ou *software* dos sistemas de TI ou dos equipamentos de comunicação: não conformidade com os requisitos, falta de manutenção, introdução acidental de vírus de computador, falta de segurança no ambiente físico, procedimentos inadequados de acesso/autorização etc.

6. **Compliance e outras disputas com as autoridades:**
Qualquer violação não intencional das leis, regulamentos e normas estabelecidas pelas autoridades ou por outras organizações terceiras às quais os envolvidos em uma atividade devem aderir, assim como a interpretação deliberada ou exploração de

omissões ou ambiguidades nessas leis e normas, que posteriormente são julgadas pelas autoridades supervisoras competentes como contrárias, se não ao sentido literal, ao menos à essência da norma.

7. **Disputas Comerciais:**
Qualquer disputa entre o banco e terceiros – clientes, contrapartes, prestadores de serviços, fornecedores, acionistas, etc. (excluindo funcionários) relacionada a: tipo de produtos oferecidos, técnicas de venda dos produtos, legibilidade/conformidade legal dos contratos, cumprimento dos termos de um acordo entre as partes (contrato, mandato, etc.), gestão do relacionamento, má execução de uma instrução (erro, atraso, etc.) ou qualquer outra negligência ou dano consequente que o banco tenha sofrido contra um terceiro, dando origem a uma disputa entre o banco e o terceiro.

1.6. Princípios de Gestão de Risco Operacional

O princípio fundamental é que o risco operacional é responsabilidade de todos os colaboradores do BSGB, sem exceção. Em outras palavras, todos os colaboradores e partes interessadas devem ser gestores de risco operacional, independentemente de sua função no BSGB.

A estrutura de Gestão de Risco Operacional opera sob os seguintes princípios-chave:

- **Funções e Responsabilidades:** definir os papéis e responsabilidades para atendimento à Estrutura de Gestão de Risco Operacional.
- **Atender os requerimentos regulatórios:** assegurar que todos os requerimentos regulatórios sejam atendidos, de forma a agregar valor e eficiência aos negócios e processos internos.
- **Comunicação eficiente:** assegurar transparência nas comunicações e no relato dos incidentes operacionais que possam trazer impactos significativos ao BSGB (financeiro, regulatório, imagem e reputacional).
- **Adotar e compreender**: a Estrutura de Gestão de Risco Operacional na 1ª linha de defesa.
- **Fornecer Supervisão independente:** estabelecer e implantar processos e controles para mitigação dos riscos inerentes às atividades da 1ª. linha de defesa, de forma independente da 2ª linha de defesa.
- **Fornecer Orientação:** fornecer orientação e aconselhamento às Unidades de Negócio no dia a dia para identificar, gerenciar e mitigar proativamente o risco operacional.
- **Escalar Riscos:** escalar riscos críticos e riscos emergentes na instituição e regionalmente para a Entidade responsável pelo grupo na região das Américas.
- **Avaliar eventos**: analisar eventos internos e externos que impactam o ambiente de risco operacional para garantir que controles apropriados estão implantados.
- **Governança e Relatórios:** garantir o escalonamento de não conformidade com os limites e padrões de risco através da estrutura de governança e relatórios.
- **Agregar riscos**: agregar informação de risco operacional no BSGB.
- **Otimizar os níveis de recursos:** garantir que os recursos sejam mantidos em níveis ótimos para atingir os principais objetivos de gestão de riscos.

1.7. Objetivos da Estrutura de Gestão de Risco Operacional

O BSGB gerencia o risco operacional avaliando as exposições ao risco operacional e aplicando uma infraestrutura de controle e monitoramento para garantir que os riscos operacionais permaneçam dentro dos limites determinados para o BSGB, e pelos negócios.

Para gerenciar adequadamente o Risco Operacional, o BSGB avalia os objetivos e as atividades das pessoas, processos e sistemas, buscando potenciais áreas de exposição a perdas internas ou riscos intrínsecos. Para medir o risco operacional de forma holística, o

BSGB procura considerar fatores operacionais decorrentes de riscos ou incidentes que surgem externamente à estrutura de controle do banco, incluindo riscos associados a fornecedores/prestadores de serviços, bem como fatores políticos, regulatórios e outros fatores ambientais.

A estrutura de Gestão de Risco Operacional abarca não só o risco operacional em si, conforme definido previamente no subitem 1.5 desta Política, mas também inclui os seguintes subtipos de risco operacional, para os quais o BSGB dispõe de Políticas locais e/ou regionais que regem a gestão dos riscos abaixo listados:

- Risco de Segurança da Informação e Segurança Cibernética;
- Risco de Tecnologia da Informação;
- Risco de Dados (qualidade dos dados e governança dos dados);
- Risco de Terceiros;
- Risco de Fraude;
- Continuidade de Negócios e Recuperação de Desastre.

Nota: a equipe de Gestão de Risco Operacional local conta com o suporte e/ou atuação parcial ou integral de times locais e regionais especialistas nos subtipos de risco operacional acima referenciados, para o cumprimento das suas respectivas estruturas de risco conforme política própria aplicável ao tema.

1.8. Estrutura de Gestão de Risco Operacional

A estrutura de gestão de risco operacional estabelece diretrizes, processos e controles para identificação, análise, mensuração, monitoramento e mitigação do risco operacional associado às atividades realizadas pelas unidades de negócios e pelas funções de suporte do BSGB, bem como seus papéis e responsabilidades, de forma compatível com a natureza e a complexidade de seus produtos, serviços, atividades de negócios, processos e sistemas.

A estrutura da gestão de risco operacional no BSGB, prevê:

- Constituição da base de dados e histórico de perdas operacionais e provisões, incluindo: (i) despesas relacionadas a eventos de perda operacional; (ii) eventos relacionados a risco de mercado e a risco de crédito;
- Elaboração de *dashboard* mensal para a Diretoria com os indicadores de risco operacional, incluindo as ações corretivas para as deficiências encontradas nos controles e processos, e informação sobre perdas operacionais significativas;
- Monitoramento mensal e sistemático dos indicadores de risco operacional para assegurar a consistência com os limites e patamares definidos na Declaração de Apetite por Riscos (RAS - *Risk Appetite Statement*), e escalonamento para o CRO e membros do Comitê de Riscos do BSGB referente a quaisquer violações aos alertas e/ou limites estabelecidos, conforme diretrizes da Política da Gestão Integrada dos Riscos do BSGB;
- Disseminação da cultura de riscos e do conteúdo desta Política a todos os funcionários da instituição em seus diversos níveis de atuação, e aos prestadores de serviços terceirizados relevantes;
- Implantação do plano de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para mitigação dos riscos e das perdas significativas decorrentes de risco operacional.

A estrutura, prevista acima, também inclui:

- Identificação, análise, classificação e monitoramento do risco operacional, e dos riscos social, ambiental e climático, relacionado aos serviços terceirizados relevantes, contratados para o funcionamento regular da instituição, prevendo os respectivos planos de contingência, de acordo com a Política de Gerenciamento de Riscos de Terceiros do BSGB;

- Tópicos relacionados ao gerenciamento do risco social, ambiental e climático de forma integrada, em cumprimento a Resolusão CMN Nº 4.943/21, e de acordo com o disposto na Política Regulatória de Responsabilidade Social, Ambiental e Climática (PRSAC) do BSGB:
    - Registro de dados referentes às perdas operacionais reportadas, causadas por danos sociais e ambientais oriundos dos produtos e transações fechadas com os clientes, incluindo valores, tipo, localização e setor econômico objeto da operação;
- Identificação e avaliação prévia dos potenciais impactos sociais e ambientais durante o processo de aprovação de novos produtos ou serviços pelo Comitê de Novos Produtos, inserida no processo de análise do risco reputacional realizada pela área de Compliance.

2. GOVERNANÇA DE RISCO OPERACIONAL

2.1. Estrutura de Governança de Risco Operacional

2.1.1. Comitês

a. Comitês Regionais

O Risco Operacional é gerenciado por meio de governança organizada em três níveis de comitês:

1º nível: Comitês Operacionais

2º nível: Comitês de Gestão

3º nível: Comitê do Conselho do Grupo SG (*Board Committee*)

Os comitês que compõem cada um dos três níveis e suas atribuições, são estabelecidos na Política Regional de Gestão de Risco Operacional e, regionalmente são realizados Comitês Executivos e Estratégico para deliberação acerca do risco operacional e de seus subtipos, referenciados acima no subitem 1.7.

Todas as decisões tomadas nestes Comitês são cascateadas pelas áreas especialistas correspondentes do SG AMER às Entidades do Grupo SG da região de AMER, na qual inclui-se o BSGB.

b. Comitês Locais "BSGB"

- **Comitê de Riscos**
  O objetivo do Comitê de Riscos do BSGB é revisar e discutir aspectos relevantes no que diz respeito (i) ao gerenciamento dos riscos ao qual o Banco Société Générale Brasil ("BSGB") está exposto de acordo com a Resolução CMN 4.557/2017 e (ii) ao alinhamento do perfil de riscos do BSGB com seu apetite por riscos, seu planejamento e objetivos estratégicos. O Comitê de Riscos do BSGB consolida e agrega as informações, incluindo aquelas provenientes dos demais Comitês que fazem parte da Governança do BSGB, referentes ao seu perfil de riscos, com destaque para os riscos atuais relacionados às suas atividades, os riscos emergentes e as deficiências existentes no gerenciamento de riscos.

- **Comitê de Novos Produtos (Comitê Técnico)**
  O comitê de novos produtos do BSGB é realizado de forma centralizada pela área de Gestão Risco Operacional. O processo segue as diretrizes da política regional do SG AMER, a qual aplica-se ao BSGB e considera as exigências regulatórias locais aplicáveis.

As Atas dos Comitês são registradas por escrito e arquivadas para comprovar a efetividade e servir de futuras referências aos processos, sempre que necessário.

2.1.2. Governança de Riscos Não Financeiros

O SG AMER mantém uma área independente para governança dos **Riscos Não Financeiros**, enquadrada na 2ª linha de defesa, que reporta à Diretoria de Riscos (AMER), ligada à Presidência do Grupo SG. Esta área, oferece suporte e diretrizes para o gerenciamento do risco operacional e, de forma independente supervisiona a gestão e qualidade das práticas de gestão de risco operacional no BSGB, bem com atua em conjunto com a área de Gestão de Risco Operacional do BSGB em determinadas ações requeridas pela estrutura de gestão de risco operacional. Suas principais atribuições são:

- Definir e implementar a governança de risco operacional na região de AMER;
- Analisar o ambiente de negócios sob a perspectiva do risco operacional e a efetividade dos controles implantados de acordo com o perfil de risco do Grupo SG;
- Promover a cultura de gestão de risco operacional no Grupo SG;
- Coordenar e participar dos projetos relacionados aos sistemas de informação, impactos regulatórios e implementação de novos produtos;
- Definir metas conjuntas e esforços colegiados para atingi-los;
- Desenvolver expertise e recomendar boas práticas.

2.1.3. Gestão de Risco Operacional BSGB

Localmente, a gestão de risco operacional está sob responsabilidade da área de Gestão de Risco Operacional, que é uma estrutura apartada das unidades de negócios e funções de suporte, e está sob a gestão do COO[3] . Essa área assessora as unidades de negócios e funções de suporte no cumprimento das estruturas de risco operacional e seus subtipos e regulamentações aplicáveis, realiza monitoramento e reportes pertinentes à gestão de risco operacional.

As deliberações relativas à gestão de risco operacional e seus subtipos devem ser submetidas ao CRO e ao Comitê de Riscos do BSGB.

3. ORGANIZAÇÃO DE RISCO OPERACIONAL E AS TRÊS LINHAS DE DEFESA

A gestão de risco operacional no BSGB é realizada por áreas segregadas e independentes das unidades de negócios e das funções de suporte, sob supervisão do CRO do BSGB, de forma integrada e contínua.

3.1. Definição das Linhas de Defesa

Todos os colaboradores do BSGB são responsáveis pela identificação, mensuração e mitigação do risco operacional associado às suas atividades. As funções e responsabilidades são segregadas de acordo com a definição e organização das 3 linhas de defesa:

- **1ª Linha de Defesa (1LOD):**
  Composta pelos colaboradores que realizam atividades que geram e tomam riscos de qualquer natureza: financeiro, operacional, regulatório, imagem, reputação etc., relacionado a originação e negociação (unidades de negócios) e funções de suporte, e são responsáveis pela realização dos processos específicos para identificação, mensuração e análise do risco operacional associado às suas atividades, e pela realização dos controles de supervisão permanente definidos para mitigação dos riscos inerentes.

  A 1LOD do BSGB também conta com a área de Gestão de Risco Operacional.

[3] **COO**: *Chief Operating Officer – Diretor de Operações*

- **2ª. Linha de Defesa (2LOD):**
  Função de gerenciamento de riscos do BSGB, composta pelas áreas de Riscos e de Compliance locais e regionais (SG AMER) que monitora e desafia de forma independente as atividades da 1LOD e a qualidade das práticas de gestão de risco operacional. Sob a responsabilidade do CRO do BSGB e/ou CRO Regional, a 2LOD deve assegurar a função de análise e de desafio eficaz da estrutura de gestão dos riscos operacionais em sua identificação e avaliação, por meio dos seguintes programas: RCSA, Declaração de Apetite por Riscos (RAS) e Revisão de Incidentes de Risco Operacional significativos.

- **3ª linha de defesa (3LOD):**
  Composta pela Auditoria Interna, responsável pela supervisão independente das atividades realizadas pela 1ª e 2ª. linhas de defesa.

3.2. Funções e Responsabilidades das Linhas de Defesa

3.2.1. Primeira Linha de Defesa (1LOD)

Os colaboradores das unidades de negócios e funções de suporte do BSGB, devem desempenhar o 1º nível de controle no desempenho de suas atividades, a fim de reduzir a exposição do BSGB ao risco operacional, seguindo as seguintes premissas:

1LOD – Linhas de Negócios e Suporte:

- Identificar, avaliar, mitigar, monitorar, escalar e reportar os riscos operacionais em suas unidades, assim como a gestão contínua desses riscos;
- Garantir que as políticas, procedimentos, padrões e equipe específicos da unidade sejam suficientes para gerenciar os riscos operacionais em produtos e processos;
- Dispor de uma equipe adequada e bem treinada sobre risco operacional, para atuar com qualidade e segurança;
- Implantar processos eficientes para maximizar a produtividade e reduzir os riscos de intervenção manual;
- Revisar periodicamente os processos operacionais para que os manuais/procedimentos de produtos e das atividades sejam atualizados de forma tempestiva a fim de assegurar a integridade das informações;
- Assegurar um alto nível de qualidade na execução dos Controles de Supervisão Permanente;
- Reportar eventos/incidentes operacionais, com perda financeira ou não, que possam trazer impactos significativos para o BSGB, incluindo risco socioambiental, e participar da implantação dos planos de ação corretivos;
- Participar ativamente do processo de "Autoavaliação dos Riscos e Controles" (RCSA – *Risk and Control Self Assessment*), contribuindo com a identificação e detalhamento dos processos e atividades para mapeamento e classificação dos riscos inerentes para cálculo do risco residual baseado nos controles ou outros mitigantes implantados;
- Reportar sobre qualquer novo produto ou alterações significativas nos produtos existentes, para a assegurar a análise preliminar dos riscos (incluindo risco socioambiental) e impactos;
- Engajar todos os Fornecedores no Programa de Gerenciamento de Riscos de Terceiros, para identificação e análise dos riscos inerentes a contratação dos serviços, a fim de evitar a ocorrência de eventos que possam impactar a continuidade dos negócios, imagem e reputação do BSGB.

1LOD – Gestão de Risco Operacional:

- Aconselhar e assessorar os gerentes das unidades de negócio (1LOD) e as demais áreas que participam desse exercício durante a execução do Programa de Autoavaliação de Riscos (RCSA) a completar a avaliação em conformidade com as diretrizes do Programa;

- Investigar todos os eventos e incidentes operacionais, registrar os incidentes nas ferramentas corporativas de gestão de incidentes e contribuir com a definição dos planos de ação corretivos para assegurar melhorias nos processos;
- Monitorar o progresso das ações corretivas definidas nos diferentes processos de gerenciamento e controle do Risco Operacional (*RCSA*, Coleta de Perdas, Supervisão Permanente) e reportar ao Comitê de Riscos do BSGB;
- Organizar treinamentos, quando necessário, para todos os colaboradores sobre Risco Operacional, incluindo tópicos relacionados à Segurança da Informação e Segurança Cibernética, Continuidade dos Negócios e Comitê de Novos Produtos;
- Produzir mensalmente os indicadores de performance e de riscos relacionados a Gestão do Risco Operacional, incluindo:
    - Qualidade de execução e reporte dos Controles de Supervisão Permanente;
    - Investigação e formalização dos incidentes operacionais que resultaram na materialização dos riscos, acompanhamento dos planos de ação e atualização da base de perdas operacionais;
    - Status do *RCSA* e dos planos de ação em andamento;
    - Monitoramento do Programa de Gerenciamento dos Riscos de Terceiros;
    - Monitoramento do processo de aprovação/revisão de novos produtos, incluindo status do processo, condições precedentes e controle dos CAPS (limites) relacionados aos produtos aprovados com limitação de volume;
    - Processos relacionados a gestão de crise e continuidade dos negócios;
    - Coleta e Reporte para área de Riscos das métricas de apetite por Risco Operacional estabelecidas na RAS (*Risk Appetite Statement*) sob a sua responsabilidade estabelecida no documento de Declaração de Apetite por Riscos (RAS) do BSGB.

3.2.2. Segunda Linha de Defesa (2LOD)

Dedicada ao gerenciamento do risco operacional, é responsável por assegurar a eficácia dos processos e controles implantados na 1ª. linha de defesa incluindo as seguintes funções:

- implementar e executar os processos, programas, sistemas e controles estabelecidos pela Governança Regional e Global do SG, envolvendo a gestão de Risco Operacional;
- Analisar periodicamente a qualidade de execução dos Controles de Supervisão Permanente, realizados pela 1ª. linha de defesa, a fim de assegurar que os riscos estão sendo mitigados de forma efetiva e monitorar as anomalias e planos de ação desencadeados durante o processo;
- Promover campanhas de revisões periódicas nos controles a fim de assegurar o correto mapeamento das atividades e processos e os riscos associados, de acordo com a estrutura organizacional;
- Analisar e validar os incidentes operacionais significativos e contribuir com a definição dos planos de ação corretivos para assegurar melhorias nos processos;
- Deliberar sobre as ações corretivas definidas nos diferentes processos de gerenciamento e controle do Risco Operacional (RCSA, Coleta de Perdas, Supervisão Permanente);
- Validar e deliberar mensalmente sobre os indicadores de performance e de riscos relacionados à Gestão de Risco Operacional;
- Modificar os componentes da Estrutura de Gestão de Risco Operacional em resposta ao ambiente em mudança (negócios e regulatório) e às lições aprendidas;
- Definir caminhos de decisão e escalonamento para gestão de risco operacional em casos de violações, informações e aprovações;

- Direcionar e coordenar com os gestores de risco operacional da 1ª linha de defesa, para garantir a implementação consistente e sustentável da Estrutura de Gestão de Risco Operacional;
- Reforçar e direcionar a cultura de Gestão de Risco Operacional estabelecida pela alta administração e pelo Comitê Executivo Regional;
- Fornecer orientação especializada sobre desenvolvimento/conteúdo de treinamentos, incluindo a identificação de treinamentos sugeridos para Risco Operacional;
- Fornecer supervisão dos processos e governança de gestão de risco operacional, para garantir que estejam funcionando conforme planejado, que os objetivos sejam alcançados e que ações apropriadas sejam tomadas para tratar e corrigir lacunas.

Neste contexto, a Alta Administração do BSGB tem como principais atribuições:

- Definir a governança sobre a gestão do risco;
- Monitorar o perfil de risco do BSGB e reportar para a governança regional (SG AMER) e da Matriz (Société Générale S.A., em Paris);
- Priorizar planos de ação, conforme a necessidade;
- Disponibilizar os recursos necessários para realização das atividades relacionadas a gestão do Risco Operacional;
- Definir as ações necessárias para enquadramento das métricas de apetite por risco definidas na RAS;
- Realizar a aprovação da Política de Gestão de Risco Operacional anualmente;
- Participar dos Comitês específicos para tomada de decisões estratégicas em relação a gestão do risco operacional, em cumprimento às Políticas locais e globais e à regulamentação local.

3.2.3. Terceira Linha de Defesa (3LOD) _ Auditoria Interna

Atua de forma independente e autônoma, como 3ª. linha de defesa, na avaliação periódica das atividades desempenhadas pela 1ª. e 2ª. linhas de defesa, a fim de assegurar conformidade com as políticas e estratégias definidas e com a regulamentação em vigor, no que tange a gestão e governança do risco operacional no BSGB.

Durante as missões de Auditoria são avaliadas a efetividade e eficiência dos sistemas e processos de controles internos e gerenciamento do risco operacional, incluindo análises específicas sobre:

- Integridade da declaração de perda operacional;
- Pertinência dos resultados de RCSA e os planos de ação definidos;
- Implantação, atualização e efetividade dos Controles de Supervisão Permanente;
- Implantação, atualização e efetividade dos planos de contingência para assegurar a continuidade dos negócios do BSGB;
- Negociação de novos produtos ou alteração nos produtos existentes, de acordo com as diretrizes da política aplicável ao tema;
- Monitoramento e implantação dos planos de ação corretivos;
- Aderência da Gestão de Risco Operacional às diretrizes locais e globais do SG.

3.3. Risco Jurídico

No BSGB todos os contratos passam pela análise do Departamento Jurídico para observância ao arcabouço legal e regulatório, incluindo a formalização de contratos com prestadores de serviços terceirizados e contratação de serviços de processamento, armazenamento de dados e computação em nuvem, em atendimento a Resolução CMN Nº 4.893/21.

Em relação à contratação de Advogados Externos, o Departamento Jurídico deve garantir que as diretrizes padrão para o departamento Jurídico, bem como quaisquer outras diretrizes locais e regionais aplicáveis ao BSGB sejam devidamente respeitadas. Tais serviços devem ser contratados somente quando não houver nenhum advogado interno disponível ou quando os advogados internos não tiverem *expertise* para tratar de uma questão jurídica específica.

4. EXECUÇÃO DA ESTRUTURA DE GESTÃO DE RISCO OPERACIONAL

Esse processo estruturado de Identificação, Mitigação, Monitoramento e Reporte é utilizado pela Gestão de Risco Operacional para avaliar e gerenciar riscos operacionais, controles e processos, buscando potenciais áreas de exposição a perdas internas ou riscos intrínsecos. A estrutura de gestão de risco operacional garante que os riscos operacionais permaneçam dentro dos limites determinados pela empresa e pelos negócios, tendo seusos componentes atuandode forma independente e em conjunto.

A integração à do processo acima citado na estrutura de gestão do risco operacional e as responsabilidades das partes interessadas constituem um ciclo contínuo para o sucesso robusto da gestão de risco operacional, conforme destacado pelos reguladores. Os reguladores esperam que o objetivo geral deste processo seja assegurar que a gestão e os negócios estejam considerando se os controles apropriados estão implementados e funcionando efetivamente para mitigar o risco a um nível aceitável (refletindo seu apetite ao risco).

As fases do ciclo de vida do processo estruturado são:

- **Identificar e Medir** – identifica, define e mede o risco de forma eficaz e o mais precisamente possível. A identificação de risco baseia-se em riscos intrínsecos, ou riscos provenientes de objetivos de negócios, mudanças estratégicas e causas emergentes internas/externas;
- **Mitigar e Controlar** – mitiga e controla o risco operacional por meio da formação e utilização de limites de risco e controles regidos pelo seu programa, padrões, políticas e procedimentos que definem responsabilidades;
- **Monitorar e Testar** – monitora e testa os níveis de risco operacional continuamente e em intervalos designados para garantir alinhamento ao apetite por risco, níveis de tolerância, políticas e padrões;
- **Reportar e Revisar** – realiza tarefas de revisão e reporte continuamente e em intervalos selecionados. Esses relatórios são distribuídos ao Comitê Executivo Regional, reuniões de comitês, gestão e partes interessadas do negócio para revisão das atividades rotineiras ou quando atenção imediata for necessária.

4.1. Componentes-chave da Estrutura de Gestão de Risco Operacional

4.1.1. Programa de identificação e avaliação dos riscos

As ferramentas de identificação e mensuração de risco operacional possibilitam oferecer à Alta Administração do BSGB, uma medida transversal e contínua deste risco em suas diferentes formas. As principais ferramentas que suportam este processo são descritas abaixo e utilizadas pelo BSGB:

- **Autoavaliação de Riscos e Controles (RCSA):** o RCSA é realizado periodicamente no BSGB, seguindo as diretrizes globais e regionais. No BSGB, o processo é realizado e formalizado na ferramenta global para autoavaliação de riscos. Durante este

processo, são avaliados os riscos inerentes a cada atividade/processo realizado pelas unidades de negócios e funções de suporte, a efetividade dos controles implantados para mitigação dos riscos e o cálculo do risco residual. Este processo é de responsabilidade da 1ª. Linha de defesa e revisado pela área de Gestão de Risco Operacional do BSGB e pela equipe de Gestão de Riscos Não Financeiros Regional. Além disso, a área de Gestão de Risco Operacional do BSGB é responsável por assegurar a efetividade do processo, coerência com a metodologia e validação final.

A análise dos resultados do RCSA é realizada pela área de Gestão de Risco Operacional do BSGB e pela equipe de Gestão de Riscos Não Financeiros Regional. O resultado do processo é apresentado no Comitê de Riscos do BSGB e os riscos residuais são rigidamente analisados, a fim de obter excelente qualidade na implantação e no acompanhamento regular dos planos de ação.

- **Coleta de Incidentes de Risco Operacional:** a Coleta de Incidentes de Risco Operacional refere-se à coleta de dados internos relacionados a perdas, ganhos, quase perdas e incidentes significativos sem impacto financeiro no âmbito do risco operacional. Os incidentes de risco operacional devem ser declarados de forma contínua, ou seja, assim que o incidente de risco for descoberto, sem aguardar o valor final do impacto. As declarações de incidentes de risco operacional com impacto financeiro igual ou maior ao limiar estabelecido pelo Grupo SG e/ou com impacto não financeiro significativo devem ser feitas na ferramenta de gestão de incidentes operacionais e de conformidade do Grupo SG.

  Os incidentes operacionais com impacto financeiro inferiores a este limiar estabelecido regionalmente, também são reportados, coletados e mitigados pelas áreas responsáveis e o histórico destes reportes é mantido em sistema local no módulo dedicado a este propósito, e são reportados no *Dashboard* de Risco Operacional e ao Comitê de Riscos do BSGB.

4.1.2. Processos para mitigação do risco

- **Controles de Supervisão Permanente**, relacionados à Biblioteca dos Controles Normativos definidos pelo Grupo SG e associados às atividades e processos realizados pelas unidades de negócios e funções de suporte. Os controles são realizados de forma periódica e declarados no Sistema Global de Supervisão de Controles Permanentes.
- O monitoramento da performance dos controles é realizado pela área de Risco Operacional do BSGB, e pela área de testes de controle, subordinada à equipe de Riscos Não Financeiros Regional e à Governança Regional de Riscos;
- **Controles periódicos**, realizados pela **auditoria interna** ou a área global de **Inspeção Geral**. Estes controles são agendados de acordo com uma avaliação dos riscos envolvidos e abrangem todas as categorias do risco operacional. É de responsabilidade da auditoria interna efetuar verificações independentes quanto à estrutura adotada pelo BSGB para Gestão do Risco Operacional;
- **Controles de Compliance**, que incluem procedimentos para garantir a conformidade regulatória, como prevenção a lavagem de dinheiro (PLD), conheça seu cliente (KYC), sanções e embargos, políticas específicas sobre antissuborno e corrupção e programa de cultura e conduta. Esses controles são essenciais para proteger o BSGB contra desenquadramentos regulatórios, determinados tipos de fraudes internas e externas e risco de imagem e reputação;
- **Controles globais antifraude** para monitoramento das atividades das mesas de operações, monitorados diariamente por um time dedicado em Bangalore-India;
- **Controle de Supervisão Permanente (*front office*)** sobre as atividades das mesas de operações, monitorados mensalmente pela área regional de Risco Operacional e formalizados no Sistema Global de Gestão de Riscos Operacionais e de Conformidade, estabelecido para controles de *front office*. O resultado da performance destes controles é compartilhado com a área de Gestão de Risco Operacional do BSGB, para monitoramento e reporte local;
- **Procedimentos de controle jurídico**, que ajudam a evitar litígios comerciais;

- Procedimentos para atualização dos **Planos de Continuidade dos Negócios** e **BIA (*Business Impact Analysis*)**, que mitigam riscos de perdas de ambientes, operacionais e interrupção nos sistemas, seguindo as diretrizes internas do BSGB e das Políticas Regionais aplicáveis. A Política de Gestão de Crise e Continuidade de Negócios do BSGB é revisada anualmente e publicada internamente no repositório "Políticas, Normas e Procedimentos Internos", acessível aos colaboradores de todos os níveis.

- Procedimentos e processos envolvendo **Segurança da Informação e Segurança Cibernética**, para assegurar a integridade, confidencialidade e disponibilidade das informações do BSGB, bem como o monitoramento de incidentes e planos de ação para redução dos riscos, conforme descrito na Política Regulatória de Segurança Cibernética do BSGB, em cumprimento a Resolução CMN Nº 4.893/21;

- Procedimentos e processos envolvendo o **Controle das Informações Confidenciais**, para assegurar o adequado tratamento e controle de informações relevantes e não públicas a que tenham acesso os administradores, empregados e colaboradores do BSGB, conforme descrito na Política Regulatória de Segurança da Informação do BSGB;

- Processo de aprovação de **Novos Produtos,** que garante que todos os riscos inerentes a implantação de novos produtos ou alteração de produtos já existentes, sejam identificados, avaliados, mensurados e mitigados até um nível aceito por todas as partes envolvidas antes da comercialização do produto, em conformidade com a política regional aplicável ao BSGB;

- Programa de **Gerenciamento de Riscos de Terceiros**, para analisar, identificar, mensurar, gerenciar, controlar e mitigar os riscos envolvidos na contratação de serviços de terceiros, incluindo critérios de decisão quanto à terceirização de serviços e seleção dos prestadores, de acordo com a Política de Gerenciamento de Riscos de Terceiros do BSGB, em cumprimento a Resolução CMN Nº 4.557/17.

4.1.3. Monitoramento e reporte dos indicadores de risco

O principal instrumento para monitoramento contínuo do risco operacional é a produção, divulgação e acompanhamento dos indicadores de performance (KPIs) e dos indicadores chaves de risco (KRIs). O objetivo é alertar a Alta Administração e o CRO sobre os assuntos que representam um nível de risco acima do definido na RAS (*Risk Appetite Statement*) ou uma tendência de aumento de exposição ao risco.

Além das ferramentas já implantadas pelo BSGB para monitoramento dos KRIs, os relatórios descritos abaixo são produzidos de forma periódica para informar formalmente a performance dos indicadores de riscos do BSGB para a alta Administração do BSGB nos Comitês específicos:

- ***Dashboard* de Riscos do BSGB (mensal):** que reporta os principais indicadores de riscos para monitoramento dos níveis de apetite por riscos definidos na RAS (*Risk Appetite Statement*) do BSGB;

- ***Dashboard* de Auditoria Interna do BSGB (mensal)**: que monitora os pontos de auditoria, estatísticas e prazos para fechamento dos planos de ação, o qual é divulgado para os membros da Diretoria do BSGB;

- ***Dashboard* de Atrasos Regulatórios do BSGB (mensal)**: que monitora os atrasos e substituições em reportes regulatórios incorridos no conglomerado bem como suas causas. Apresentado pelo Compliance no Comitê de Riscos do BSGB;

- **Monitoramento da RAS (mensal):** os indicadores de risco operacional são monitorados para assegurar aderência aos níveis de apetite por risco operacional definidos na RAS, de acordo com a estratégia de negócios do BSGB.

Qualquer violação das métricas é reportada, em conformidade com as diretrizes do documento de Declaração de Apetite por Riscos do BSGB "RAS", para o CRO e aos membros do Comitê de Riscos do BSGB, para análise e definição das ações corretivas, quando aplicável, conforme diretrizes da Política de Gestão Integrada de Riscos.

  - **Apuração da RAS:** mensalmente, a área de Gestão de Risco Operacional apura as métricas da RAS sob seu escopo, a partir de informações coletadas, registradas ou recebidas:

- Nos sistemas local e global para declaração de incidentes operacionais;
- Nos sistemas de registro de incidentes de Tecnologia da Informação;
- Do time regional de Tecnologia e Serviços , relacionados a incidentes de ciber e de vazamento de dados;
- Nos sistemas de Gestão de Continuidade de Negócios e dos resultados de testes de recuperação de desastres;
- Nos sistemas de gestão de terceiros.

- **Reporte das métricas da RAS:** as métricas apuradas mensalmente são reportadas por um colaborador(a) da área de Gestão de Risco Operacional e validadas pelo(a) Head de Risco Operacional ou por seu/sua backup para esta demanda no sistema global, no módulo dedicado para este propósito.
- **Deficiências e Dependências Críticas da Produção e Reporte das Métricas da RAS:**
  - A maior parte das informações são obtidas em sistemas estáveis e confiáveis.
  - Existe dependência de de Infraestutrura de Tecnologia para a apuração de alguns indicadores.

5. CAPITAL REQUERIDO PARA O RISCO OPERACIONAL

O cálculo da parcela de ativos ponderados pelo risco (RWA), relativa ao cálculo do capital requerido para o risco operacional do Conglomerado é realizado pelo departamento de Financeiro (DFIN) e utiliza a metodologia de “Abordagem Padronizada” de que trata a Resolução CMN Nº 4.958/2021, atualizada em 27/12/2024.

7. PRAZOS DE ARQUIVAMENTO

O prazo de retenção para os documentos, informações e dados a que esta Política se refere, é de 10 (dez) anos.

Essa Política ficará disponível para todos os colaboradores do BSGB, em intranet própria, e, caso haja dúvidas em relação ao seu conteúdo e aplicação, os colaboradores deverão entrar em contato com a área de Gestão de Risco Operacional.

8. TREINAMENTO OBRIGATÓRIO

Treinamentos mandatórios poderão ser organizados para todos os colaboradores do BSGB, incluindo prestadores de serviços relevantes, a fim de reforçar as diretrizes e os processos implantados para a Gestão do Risco Operacional, de forma presencial ou online, através da plataforma eletrônica.

Para efeito desta Política, prestadores de serviços relevantes são definidos como recursos especializados contratados para sustentar o funcionamento regular da entidade, que são alocadas nas unidades de negócios e funções de suportedo BSGB.

9. INDICADOR DA RAS

Os indicadores de risco operacional relacionados a esta política regulatória definidos na RAS do BSGB (*Risk Appetite Statement*), são monitorados conforme periodicidade definida para cada métrica para assegurar aderência aos níveis de apetite de risco e em linha com a estratégia de negócios do BGSB.

Qualquer violação das métricas é reportada para o Diretor de Riscos (CRO) e ao Comitê de Riscos do BSGB bimestralmente, para análise e definição das ações corretivas, quando aplicável, conforme diretrizes da Política de Gestão Integrada de Riscos do BSGB.

Quando houver excessos ou violações dos limites aprovados na RAS, a área de Riscos deve ser acionada para verificar os procedimentos relacionados que estão descritos na RAS do BSGB.

O processo de coleta de dados, cálculo e divulgação estão definidos em procedimento interno específico quanto as métricas da RAS de risco não financeiro para o escopo que cabe à área de Gestão de Risco Operacional.

10. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

No caso de identificação de falhas e/ou violações sobre os tópicos tratados nesta Política, o assunto será escalado para o COO e para o CRO e será aberto um incidente operacional para investigação, análise dos impactos e definição de planos de ação mitigadores.

O incidente e o monitoramento dos planos de ação definidos para mitigação do risco, deverão ser reportados para a Diretoria do BSGB, bem como às áreas de gestão de riscos no SG AMER, quando aplicável.

No caso de envolvimento de colaboradores do BSGB, será necessário analisar a aplicação de medidas disciplinares, de acordo com a recomendação do Comitê de Ética.