Política Corporativa de Gestão de Riscos

PBG-POL-GRI-001-V02

Sumário

1. OBJETIVO

Estabelecer os princípios, diretrizes, competências e responsabilidades aplicáveis ao sistema de gerenciamento de riscos, controles internos e integridade/conformidade (compliance) no âmbito da PBG S.A., assegurando que a Companhia disponha de estrutura apropriada para identificar, avaliar, priorizar, tratar, monitorar e reportar os riscos a que esteja exposta, em níveis compatíveis com seu apetite e tolerância a riscos, com sua estratégia de negócios e com a legislação e regulamentação aplicáveis.

Esta Política também tem por objetivo:

- disciplinar a governança do tema em nível corporativo;
- orientar a articulação entre gestão de riscos, controles internos, compliance e auditoria interna;
- estabelecer a prestação de contas da Diretoria ao Conselho de Administração; e
- servir como política corporativa de referência para os manuais, procedimentos, matrizes e instrumentos operacionais vinculados a esta matéria.

2. ÁREA RESPONSÁVEL (OWNER)

A área de Gestão de Riscos é responsável pela gestão desta Política, cabendo-lhe zelar por sua atualização, orientar as áreas quanto à sua aplicação e coordenar, em articulação com as instâncias competentes, o sistema corporativo de gerenciamento de riscos, controles internos e integridade/conformidade.
RISC

A área de Compliance atuará de forma complementar, especialmente no tratamento dos riscos regulatórios, de integridade, conduta e conformidade, observadas as competências específicas previstas nesta Política.

A área de Controles Internos será responsável por apoiar a implementação, monitoramento e aprimoramento contínuo dos controles internos relacionados à gestão de riscos da Companhia, promovendo a efetividade dos processos de controle, a mitigação de riscos operacionais e o fortalecimento do ambiente de governança corporativa, em alinhamento às diretrizes estabelecidas nesta Política.

As áreas de Gestão de Riscos, Compliance e Controles Internos deverão possuir estrutura mínima, recursos adequados, independência técnica e profissionais capacitados para o desempenho de suas atribuições, garantindo condições necessárias para cumprimento das diretrizes, processos, monitoramentos e responsabilidades previstos nesta Política, observadas a complexidade, porte e necessidades da Companhia.

3. ABRANGÊNCIA

Esta Política aplica-se à Estrutura Corporativa e às Unidades de Negócio do Portobello Grupo, bem como aos membros dos órgãos de governança, à Diretoria Estatutária, às áreas corporativas, às áreas operacionais e aos demais agentes internos envolvidos no sistema de gerenciamento de riscos, controles internos e integridade/conformidade da Companhia.

Aplica-se, igualmente, aos processos de identificação, avaliação, priorização, tratamento, monitoramento, reporte e revisão de riscos, bem como à manutenção e avaliação dos controles internos e à articulação com o Programa de

Integridade/Conformidade da Companhia.

4. DEFINIÇÕES

Para fins desta Política, são considerados os seguintes termos e definições:

- **Portobello Grupo ("PBG"):** Conjunto de empresas controladas pela PBG S.A.
- **Risco:** efeito da incerteza sobre os objetivos da Companhia, que pode afetar negativamente ou positivamente o desempenho, a continuidade dos negócios, a geração de valor, a reputação, a conformidade e a sustentabilidade institucional.
- **Gerenciamento de riscos:** processo contínuo e estruturado de estabelecer contexto, identificar, analisar, avaliar, priorizar, tratar, monitorar e reportar riscos.
- **Apetite a risco:** nível de risco que a Companhia está disposta a assumir na busca de seus objetivos.
- **Tolerância a risco:** limite específico aceitável de variação ou exposição em relação ao nível de risco definido pela Companhia para determinado objetivo, processo ou exposição.
- **Controle interno:** políticas, normas, procedimentos, práticas, atividades, registros, sistemas e mecanismos voltados a prevenir, detectar, corrigir ou reduzir a probabilidade e/ou o impacto da materialização de riscos.
- **Risco inerente:** risco existente antes da consideração dos controles e respostas aplicáveis.
- **Risco residual:** risco remanescente após a consideração dos controles e respostas existentes e das medidas de tratamento adotadas.
- **Risk Owner:** responsável pela gestão do risco, inclusive quanto à sua avaliação, ao acompanhamento de indicadores e à implementação ou articulação das respostas cabíveis.
- **Control Owner:** responsável pelo desenho, execução, documentação, monitoramento e aperfeiçoamento do controle interno sob sua responsabilidade.
- **Programa de Integridade/Conformidade (Compliance):** conjunto de diretrizes, mecanismos, controles, processos e ações voltados à prevenção, detecção e resposta a desvios, ilícitos e descumprimentos legais, regulatórios e normativos.

5. FUNDAMENTOS DE GOVERNANÇA

A Companhia adota estrutura de governança baseada em clara definição de papéis entre o Conselho de Administração, o Comitê de Auditoria, a Diretoria Estatutária e as funções de segunda e terceira linhas, com vistas a assegurar adequada segregação entre supervisão, gestão, monitoramento e avaliação independente.

O gerenciamento de riscos integra o sistema de governança corporativa da Companhia e deve operar de forma articulada com:

- o planejamento estratégico;
- a alocação de capital;
- a tomada de decisão;
- os controles internos;
- o Programa de Integridade/Conformidade;
- a auditoria interna;
- a gestão de crises;
- e os demais normativos corporativos aplicáveis.

As análises técnicas realizadas pelas áreas de Gestão de Riscos, Controles Internos, Compliance, Auditoria Interna e demais áreas de suporte possuem natureza instrutória e de assessoramento, sem afastar a competência deliberativa dos órgãos societários competentes, observando o devido dever de diligência e os seus ônus, conforme definido legalmente.

6. PRINCÍPIOS E DIRETRIZES

O sistema de gerenciamento de riscos, controles internos e integridade/conformidade da Companhia observará, de forma permanente, os seguintes princípios:

- **Alinhamento estratégico:** a gestão de riscos deve apoiar a formulação, execução e revisão da estratégia da Companhia;
- **Proporcionalidade:** a estrutura, a profundidade e os instrumentos de gerenciamento devem ser adequados ao porte, ao risco e à complexidade das atividades da Companhia;
- **Integração:** riscos, controles internos e compliance devem ser tratados de forma coordenada e não fragmentada;
- **Tempestividade:** os administradores e gestores devem ter acesso tempestivo às informações relevantes sobre os riscos a que a Companhia está exposta;
- **Accountability:** os responsáveis por riscos, controles e decisões de tratamento devem prestar contas de suas atuações;
- **Rastreabilidade:** o sistema deve permitir adequada documentação, evidência, monitoramento e revisão das decisões e medidas adotadas;
- **Melhoria contínua:** o sistema deve ser periodicamente revisto e aperfeiçoado;
- **Independência de supervisão:** a supervisão do sistema deve preservar a distinção entre execução, monitoramento e avaliação independente.

A gestão de riscos na Companhia tem caráter contínuo e cíclico e deve buscar:

- apoiar a tomada de decisão pelos administradores;
- reduzir a probabilidade de materialização de eventos indesejados;
- mitigar impactos adversos;
- preservar valor e continuidade dos negócios; e
- fortalecer a integridade, a conformidade e a resiliência institucional da Companhia.

7. DIRETRIZES DO GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS

7.1 Riscos abrangidos

A Companhia adotará política e estrutura de gerenciamento para, no mínimo, os riscos:

- estratégicos;
- operacionais;
- financeiros, de crédito e de liquidez;
- de reporte e divulgação;

- regulatórios e de integridade/conformidade, incluindo desvios de conduta e atos de natureza ilícita;
- tecnológicos, de segurança da informação e cibernéticos;
- socioambientais, inclusive climáticos;
- e outros riscos materialmente relevantes à luz do contexto da Companhia.

As categorias e taxonomias de risco serão detalhadas em manual, matriz, dicionário de riscos ou documento operacional vinculado, observado o disposto nesta Política, a ser criado após aprovação da presente política, com acompanhamento do comitê de auditoria.

7.2 Apetite, tolerância e limites aceitáveis de exposição

A Companhia manterá diretrizes formais para definição, revisão, monitoramento e reporte do apetite, da tolerância e dos limites aceitáveis de exposição a riscos.

O apetite, a tolerância e os limites aceitáveis de exposição deverão:

- ser compatíveis com a estratégia, a capacidade financeira, a estrutura operacional e o perfil de risco da Companhia;
- considerar, conforme aplicável, a materialidade das exposições, os impactos potenciais sobre liquidez, continuidade dos negócios, reputação, conformidade regulatória e geração de valor;
- orientar a avaliação, a priorização, o tratamento e o monitoramento dos riscos;
- subsidiar decisões relevantes da administração; e
- ser submetidos à aprovação do Conselho de Administração e revistos periodicamente, ou sempre que houver alteração relevante no contexto da Companhia.

A superação dos limites aceitáveis de exposição deverá ser tempestivamente reportada às instâncias competentes, acompanhada da avaliação de suas causas e, quando cabível, de plano de ação para reenquadramento da exposição, devendo eventuais exceções ser justificadas, documentadas e submetidas à alçada competente.

7.3 Estrutura organizacional e instrumentos

O sistema de gerenciamento de riscos, controles internos e integridade/conformidade da Companhia será sustentado, entre outros, pelos seguintes instrumentos e estruturas:

- política corporativa;
- manuais, procedimentos e documentos orientadores vinculados;
- matriz de riscos;
- critérios de avaliação, priorização e tratamento;
- indicadores-chave de risco (KRIs);
- planos de ação;
- controles internos preventivos, detectivos e corretivos;
- atividades de monitoramento e reporte;
- mecanismos de integridade/conformidade;
- e avaliações periódicas de efetividade.

Os instrumentos operacionais, metodológicos e documentais específicos poderão ser detalhados em documentos próprios, sem prejuízo da observância das diretrizes previstas nesta Política.

7.4 Processo corporativo de gerenciamento de riscos

O processo corporativo de gerenciamento de riscos deverá compreender, em bases proporcionais e documentadas:

- estabelecimento do contexto;
- identificação de riscos;
- classificação e agrupamento dos riscos;
- análise e avaliação;
- priorização;
- definição e implementação da resposta ou tratamento;
- monitoramento;
- comunicação e reporte;
- e revisão periódica.

A metodologia detalhada, inclusive escalas, critérios, matrizes, parâmetros quantitativos, mapa de calor (*heat map*) e formulários, poderá ser disciplinada em manual ou procedimento específico.

7.5 Controles internos

A Companhia manterá estrutura de controles internos compatível com seus riscos, processos e obrigações regulatórias, devendo os controles:

- serem adequadamente desenhados, implementados, documentados e monitorados;
- mitigar riscos em níveis compatíveis com os limites aprovados;
- permitir evidência suficiente de sua execução e efetividade;
- serem periodicamente avaliados quanto à sua adequação.

Os controles internos deverão apoiar, entre outros objetivos:

- a eficácia e eficiência das operações;
- a confiabilidade dos relatórios e demonstrações;
- o cumprimento de leis, regulamentos e normas internas;
- e a prevenção, detecção e correção de falhas, desvios e irregularidades.

8. AVALIAÇÃO DA EFICÁCIA E PRESTAÇÃO DE CONTAS

A Diretoria Estatutária deverá, de forma periódica, avaliar formalmente:

- a eficácia desta Política e do sistema de gerenciamento de riscos;
- a adequação e efetividade do sistema de controles internos;
- e a eficácia do programa de integridade/conformidade (compliance).

Essa avaliação deverá considerar, entre outros elementos:

- a evolução do perfil de riscos da Companhia;
- a adequação da estrutura operacional disponível;
- a efetividade dos controles internos;
- o andamento e a suficiência dos planos de ação;
- a maturidade do ambiente de riscos e controles;
- a efetividade da comunicação e do reporte;
- e as conclusões relevantes das áreas de Gestão de Riscos, Controles Internos, Compliance e Auditoria Interna.

O resultado dessa avaliação deverá ser formalmente apresentado ao Conselho de Administração sempre que solicitado pelo Comitê de Auditoria, observadas a materialidade, a relevância e as necessidades de supervisão identificadas pelos órgãos de governança, em reporte que permita ao Conselho exercer suas atribuições de supervisão, nos termos desta Política e do respectivo Regimento Interno.

9. PAPÉIS E RESPONSABILIDADES

O sistema de gerenciamento de riscos, controles internos e integridade/conformidade da Companhia observará clara distribuição de competências entre as instâncias de supervisão, gestão, monitoramento e avaliação independente, assegurando adequada segregação entre o Conselho de Administração, o Comitê de Auditoria, a Diretoria Estatutária, as áreas de segunda linha e a Auditoria Interna.

As atribuições previstas neste item deverão ser exercidas de forma coordenada e complementar, sem prejuízo das competências legais, estatutárias e regimentais de cada órgão ou função.

9.1 Conselho de Administração

Compete ao Conselho de Administração:

- aprovar esta Política e suas revisões;
- definir as diretrizes gerais de gerenciamento de riscos da Companhia;
- aprovar o apetite, a tolerância e os limites aceitáveis de exposição a riscos, bem como suas revisões;
- zelar para que a Diretoria mantenha mecanismos e controles internos adequados para identificar, avaliar, monitorar e mitigar os riscos a que a Companhia esteja exposta, inclusive no que se refere ao sistema de integridade/conformidade;
- supervisionar a exposição da Companhia a riscos e a adequação dos sistemas de gerenciamento de riscos, controles internos e compliance;
- receber periódicamente, e sempre que solicitado, prestação de contas da Diretoria sobre a eficácia desses sistemas;
- deliberar sobre matérias relevantes relacionadas a riscos, controles internos e compliance submetidas à sua competência;
- e acompanhar, com apoio do Comitê de Auditoria, a implementação das medidas relevantes de mitigação e aprimoramento.

9.2 Comitê de Auditoria

Compete ao Comitê de Auditoria, observado seu regimento interno:

- assessorar o Conselho de Administração na supervisão de riscos, controles internos, compliance e auditoria interna;
- acompanhar a qualidade e a suficiência da estrutura de gerenciamento de riscos e controles internos;
- analisar reportes relevantes sobre riscos prioritários, deficiências de controle e planos de ação;
- acompanhar, quando aplicável, a avaliação da eficácia dos sistemas de gerenciamento de riscos, controles internos e compliance;
- e emitir recomendações ao Conselho de Administração sobre matérias de sua competência.

9.3 Diretoria Estatutária

Compete à Diretoria Estatutária:

- assegurar a existência e o funcionamento de estrutura operacional adequada para o gerenciamento de riscos, controles internos e compliance;
- incorporar a visão de riscos à gestão e à tomada de decisão;
- assegurar a implementação das diretrizes aprovadas pelo Conselho;
- prover recursos humanos, financeiros, tecnológicos e informacionais adequados ao funcionamento do sistema;
- assegurar que riscos relevantes sejam identificados, avaliados, tratados e reportados tempestivamente;
- assegurar a implementação e o acompanhamento dos planos de ação;
- avaliar, periodicamente, a eficácia desta Política, dos sistemas de gerenciamento de riscos, dos controles internos e do Programa de Integridade/Conformidade;
- e prestar contas ao Conselho de Administração sobre essa avaliação.

9.4 Gestão de Riscos

Compete à área de Gestão de Riscos:

- propor e manter metodologias, critérios e instrumentos de gerenciamento de riscos;
- coordenar os ciclos corporativos de identificação, avaliação, priorização e monitoramento de riscos;
- consolidar a matriz e o mapa de riscos corporativos;
- apoiar a definição e a revisão do apetite, da tolerância e dos limites aceitáveis de exposição a riscos;
- monitorar a implementação e a evolução dos planos de ação relativos a riscos e controles;
- produzir reportes gerenciais e de governança;
- apoiar a disseminação da cultura de riscos;
- e coordenar a atualização desta Política e dos instrumentos complementares sob sua gestão.

9.5 Controles Internos

Compete à área de Controles Internos:

- mapear processos, riscos associados e controles-chave, em articulação com as áreas responsáveis e com a área de Gestão de Riscos;
- avaliar o desenho e a suficiência dos controles internos existentes, considerando sua capacidade de mitigar os riscos identificados;
- realizar testes de efetividade dos controles internos, conforme metodologia, periodicidade e critérios definidos pela Companhia;
- avaliar o ambiente de controles internos, identificando fragilidades, oportunidades de melhoria e eventuais necessidades de revisão ou implementação de controles;
- acompanhar a adequação e a efetividade dos controles internos, em articulação com as áreas responsáveis pelos processos;
- monitorar a implementação e a evolução dos planos de ação relacionados a deficiências, fragilidades ou melhorias de controles internos;
- produzir reportes gerenciais e de governança sobre o ambiente de controles internos, testes realizados, deficiências identificadas e evolução dos respectivos planos de ação;
- apoiar a disseminação da cultura de controles internos, em alinhamento com a cultura de gestão de riscos da Companhia.

9.6 Compliance

Compete à área de Compliance:

- supervisionar os aspectos de integridade/conformidade relacionados a esta Política;
- identificar, avaliar e acompanhar riscos de integridade/conformidade;
- apoiar a interpretação desta Política no âmbito do Programa de Integridade;
- articular-se com as áreas responsáveis por terceiros, investigações, canal de denúncias, due diligence e treinamentos, quando aplicável;
- monitorar a aderência a leis, regulamentos e normas internas sob sua esfera de atuação;
- e reportar riscos, desvios e necessidades de aprimoramento às instâncias competentes.

9.7 Auditoria Interna

Compete à Auditoria Interna:

- avaliar, de forma independente, a adequação e a eficácia da governança, do gerenciamento de riscos e dos controles internos;
- reportar seus trabalhos ao Comitê de Auditoria e às instâncias competentes;
- considerar os riscos prioritários na elaboração de seu plano;
- e acompanhar, conforme sua metodologia, a implementação de ações corretivas decorrentes de auditorias.

9.8 Gestores, Risk Owners e Control Owners

Compete aos gestores, Risk Owners e Control Owners, conforme suas atribuições:

- identificar e avaliar os riscos sob sua responsabilidade;
- executar e evidenciar os controles atribuídos;
- propor e implementar respostas e planos de ação;
- acompanhar indicadores e mudanças na exposição ao risco;
- reportar riscos emergentes, falhas de controle e eventos relevantes;
- e contribuir para a disseminação da cultura de riscos em suas respectivas áreas.

9.9 Colaboradores

Compete aos colaboradores, naquilo que lhes couber:

- observar esta Política e os instrumentos complementares aplicáveis;
- cooperar com os processos de identificação, avaliação, tratamento e monitoramento de riscos;
- comunicar situações de risco, falhas de controle, desvios e irregularidades pelos canais competentes;
- e atuar com diligência, integridade e responsabilidade na execução de suas atividades.

10. MONITORAMENTO E CONSEQUÊNCIAS

O Comitê de Auditoria acompanhará a efetividade desta Política e assessorará o Conselho de Administração na supervisão do sistema de gerenciamento de riscos, controles internos e integridade/conformidade, sem prejuízo do monitoramento operacional realizado pela Diretoria Estatutária, pelas áreas de Gestão de Riscos e Controles Internos, pela área de Compliance e pelos responsáveis pelos riscos e controles, no âmbito de suas atribuições.

Para fins de monitoramento, poderão ser considerados, entre outros elementos:

- matriz de riscos;
- indicadores-chave de risco;
- planos de ação;
- relatórios de riscos e controles;
- avaliações de maturidade;
- relatórios de compliance;
- relatórios de auditoria interna e auditoria independente;
- e registros de não conformidade, incidentes ou desvios relevantes.

O descumprimento das diretrizes estabelecidas nesta Política resultará na adoção das medidas administrativas cabíveis, nos termos das normas internas da Companhia e da legislação aplicável.

11. DISPOSIÇÕES FINAIS

Esta Política complementa as disposições do Estatuto Social e deverá ser interpretada em conjunto com a legislação aplicável, com o Regimento Interno do Conselho de Administração e com os demais normativos internos da Companhia relacionados à governança corporativa, controles internos, integridade/conformidade e gestão de riscos.

Os procedimentos detalhados de gestão, avaliação, classificação, heat map, KRIs, testes, walkthroughs, documentação técnica, formulários e demais instrumentos operacionais são disciplinados por manuais, procedimentos e outros documentos vinculados a esta Política.

Situações não previstas neste documento serão avaliadas com base nos princípios estabelecidos nesta Política, nas normas societárias vigentes e nas melhores práticas de governança corporativa.

A aplicação das regras desta Política deverá sempre observar a situação econômico-financeira da Companhia, de modo a preservar a proporcionalidade e a razoabilidade das decisões, bem como evitar a obsolescência deste instrumento normativo e assegurar sua contínua atualização.

A presente Política entra em vigor na data de sua aprovação pelo Conselho de Administração e será revisada periodicamente, ou sempre que houver alteração relevante no contexto regulatório, estatutário ou nas práticas de governança adotadas pela Companhia.

Controle de Alterações:

Data	Versão	Elaboração (Owner)	Validação	Aprovação	Resumo das alterações
Junho/2026	02	Gestão de Riscos	Julho/2026 - DEX	17/07/2026 - COA	-