Política Corporativa

PL-GRCI-PBG 01

Gestão de Riscos Corporativos

1. OBJETIVO

Esta Política estabelece as normas e competências para a função de Gestão de Riscos Corporativos na Portobello, possibilitando o estabelecimento do contexto, identificação, avaliação, priorização, monitoramento, tratamento e comunicação destes riscos.

2. ABRANGÊNCIA

Esta Política abrange todas as Unidades de Negócios e áreas da organização, e aplica-se a todos os *stakeholders* (colaboradores efetivos e temporários, terceiros, estagiários, aprendizes, líderes, diretores, procuradores, conselheiros e franqueados etc.) da Portobello Grupo.

3. REFERÊNCIAS

- ISO 31000:2018 – *Risk Management Guidelines*
- COSO ERM:2017 - Gerenciamento de Riscos Corporativos Integrado com Estratégia e Performance
- Gestão de Riscos Corporativos IBGC:2017
- Estatuto Social da PBG S/A
- Código de Conduta Ética da Portobello Grupo
- Regimento Interno do Comitê de Auditoria (PBG)
- Regimento Interno da Auditoria Interna (PBG)
- Código Brasileiro de Governança Corporativa – Companhias Abertas
- Regulamento do Novo Mercado da B3 S.A.

4. ATRIBUIÇÕES E RESPONSABILIDADES

Esta seção tem como objetivo indicar as atribuições e responsabilidades de cada *stakeholder* envolvido no processo de gestão de riscos.

4.1 Compete ao Conselho de Administração:

- Aprovar as políticas corporativas e diretrizes que afetam a organização como um todo;
- Aprovar a Matriz de Riscos estratégicos e critérios de Gestão de Riscos da Portobello, incluindo possíveis alterações e revisões;
- Validar a análise realizada pela área de Gestão de Riscos referente ao contexto interno e externo da Portobello, monitorando os principais riscos em que a Companhia está exposta;
- Validar o apetite ou a tolerância aos riscos, com base na definição da área de Gestão de Riscos;
- Aprovar os níveis de alçada, que define as responsabilidades para aprovação e tratamento dos riscos;
- Dar o direcionamento estratégico e apoiar a Diretoria na implementação das ações estratégicas referente à Gestão de Riscos na Portobello;
- Assegurar que a gestão identifique, mitigue e monitore os riscos da organização, bem como a integridade do sistema de controles internos;
- Assegurar que o Comitê de Auditoria e o Comitê Executivo de Riscos monitorem e contribuam para mitigação dos riscos da organização, bem como a integridade dos processos e procedimentos de Controles Internos;
- Validar o resultado das avaliações dos Riscos Corporativos Prioritários e deliberar sobre eles;

• Assegurar a estruturação e validação do Plano de Auditoria e seus respectivos resultados, que é responsabilidade do Comitê de Auditoria; e,
• Avaliar as recomendações do Comitê Executivo de Riscos e Comitê de Auditoria relacionadas aos processos de Gestão de Riscos, Controles Internos, Auditoria e Compliance.

4.2 Compete ao Comitê de Auditoria

• Assessorar o Conselho de Administração no monitoramento de atividades de Auditorias, Controles Internos, Gestão de Riscos e *Compliance*, incluindo a qualidade dos seus trabalhos, estrutura existente, plano de trabalho e resultados obtidos;
• Suportar o Conselho de Administração na supervisão da estrutura operacional e das atividades de gerenciamento de riscos pela gestão da organização, incluindo todas as classificações dos riscos aplicáveis, em linha com as diretrizes, políticas estabelecidas e normas regulatórias;
• Avaliar e monitorar a exposição da Companhia a riscos que podem afetar a continuidade dos negócios bem como a integridade do sistema de Gestão de Riscos e Controles Internos;
• Envolver as áreas de Gestão de Riscos e Controles Internos, Auditoria Interna e *Compliance* na avaliação dos riscos associados a projetos estratégicos, parcerias ou transações de fusões e aquisições, de forma independente, segundo as normas do *The IIA* (*Institute of Internal Auditors*);
• Validar formalmente o Plano de Auditoria estruturado pela área de Auditoria Interna e estruturar reporte para o Conselho de Administração;
• Recomendar o orçamento da Auditoria Interna, inclusive no que diz respeito à contratação de serviços profissionais externos para apoio na execução do Plano Anual da Auditoria Interna;
• Aprovar o Regulamento Interno (*Audit Charter*) e o Plano Estratégico da Auditoria Interna;
• Suporte ao conselho na contratação ou substituição do auditor independente e supervisão da sua atuação, estrutura, independência perante a organização, qualidade e resultados dos seus trabalhos;
• Aprovar os resultados obtidos durante a Auditoria e preparar o reporte para o Conselho de Administração;
• Assessorar na avaliação de planos de ação para mitigação de riscos e melhoria de processos e controles;
• Assessorar nas avaliações e classificações dos Riscos Corporativos Prioritários; e,
• Solicitar, a qualquer tempo, esclarecimentos ou informações adicionais aos auditores internos, aos auditores independentes, à diretoria ou a qualquer colaborador da Companhia, que serão disponibilizadas a todos os seus membros.

4.3 Compete à Diretoria Corporativa

• Estabelecer a estrutura operacional de Gestão de Riscos e Controles Internos dentro da Companhia;
• Suportar as decisões do Conselho de Administração e Comitê Executivo de Riscos no que se refere à mitigação dos riscos;
• Implementar, monitorar e executar todas as atividades de Controles Internos, incluindo a manutenção de sua respectiva documentação nos padrões SOX (Sarbanes-Oxley), nas áreas de sua responsabilidade e em todas as áreas de negócio das respectivas Unidades de Negócios (*BUs*), de acordo com as definições realizadas pela área de Gestão de Riscos e Controles Internos;
• Suportar a área de Gestão de Riscos e Controles Internos na avaliação do nível de apetite e tolerância a riscos de acordo com as diretrizes estratégicas definidas, relacionando risco x retorno;
• Suportar na estruturação dos planos de ação para os riscos não mitigados e controles não efetivos e reportar as áreas de Gestão de Riscos e Controles Internos, Auditoria Interna e de Compliance;

• Estabelecer comunicação com os líderes das áreas de Gestão de Riscos e Controles Internos, Compliance e Auditoria Interna, referente aos riscos corporativos e controles inefetivos;
• Acompanhar o processo de gerenciamento de riscos e controles, subsidiando recursos (humanos, financeiros e tecnológicos) e monitorando a implementação de ações para o tratamento de riscos; e,
• Efetuar reporte junto a Gestão de Riscos ao Conselho de Administração acerca do gerenciamento dos Riscos Corporativos Estratégicos e Prioritários.

4.4 Compete ao Comitê Executivo de Riscos

• Reunir-se trimestralmente (ou conforme necessidade) para deliberar sobre assuntos relacionados a Gestão de Riscos da Portobello Grupo;
•Emitir parecer para o Conselho de Administração sobre o ambiente de Risco no qual a Portobello está inserida e sugerir o nível de Apetite e Tolerância a Riscos do Grupo;
•Definir quais os Riscos Prioritários após avaliação do Mapa de Riscos, e encaminhar sugestão para o Conselho de Administração;
•Auxiliar a Companhia com uma visão estratégica, concentrando nas incertezas voltadas para o futuro e auxiliando o Conselho de Administração nas tomadas de decisão;
•Revisar e deliberar sobre a Política de Gestão de Riscos Corporativos do Grupo (governança, metodologia, processos, sistemas entre outros); e
•Aprovar a inclusão de riscos emergentes na Matriz de Riscos.

4.5 Compete à Gestão de Riscos e Controles Internos

• Conhecer, transmitir e treinar os colaboradores da Portobello, a fim de difundir a cultura de Gestão de Riscos e Controles Internos;
• Propor e manter os conceitos e metodologias aplicadas na Gestão de Riscos;
• Estabelecer e manter atualizada as documentações internas orientadoras de Gestão de Riscos;
• Revisar periodicamente o plano de trabalho da área de Gestão de Riscos, incluindo a revisão da política de Gestão de Riscos do Grupo;
• Monitorar a adequação aos requerimentos dos órgãos reguladores, normas e boas práticas referentes à Gestão de Riscos e Controles Internos (CVM, SEC, *IIA*, IBGC, *COSO*, entre outros);
• Monitorar periodicamente o contexto interno e externo do Grupo, visando entender o ambiente de risco no qual a Portobello está inserida;
• Planejar, mensalmente, agenda de integração entre as áreas (*Compliance*, Auditoria Interna, Gestão de Riscos e Controles Internos) para tratar de assuntos relevantes relacionados aos riscos do Grupo;
• Estruturar e atualizar a Matriz de Riscos Corporativos da Portobello;
• Atualizar e revisar o Dicionário de Riscos junto aos Executivos da Companhia sempre que houver atualizações no planejamento estratégico do Grupo ou sempre que fatos relevantes ocorrerem;
• Propor os critérios para avaliação, mapeamento e classificação de riscos;
• Propor o apetite ou a tolerância aos riscos, visando indicar os parâmetros para análise de Impacto dos Riscos Corporativos para validação e aprovação do Conselho de Administração;
• Revisar e propor os critérios de probabilidade e impacto definidos no *Risk Assessment Criteria (RAC)* para validação e aprovação do Conselho de Administração;
• Suportar a diretoria executiva na identificação e definição dos *Risk Owners*;
• Suportar e monitorar o processo de identificação e avaliação dos riscos das Companhias com os líderes das Unidades de Negócios (*BUs*) e *Risk Owners*;

• Analisar periodicamente resultado das avaliações dos Riscos Corporativos, suportar a Diretoria Corporativa na classificação dos Riscos Corporativos Prioritários após estruturação do *Risk Assessment* Corporativo e reportar o resultado para validação do Conselho de Administração;
• Acompanhar, deliberar e reportar sobre mudanças na criticidade dos riscos (quando aplicável);
• Revisar e monitorar os riscos, controles, planos de ação e os *Key Risk Indicators* (*KRIs*) mensalmente;
• Monitorar e acompanhar os riscos emergentes identificados pelos *Control*/*Risk Owners*;
• Suportar o Comitê Executivo de Riscos e o Comitê de Auditoria na identificação de oportunidades de aprimoramento nos processos internos de gerenciamento de riscos e controles internos;
• Assegurar, em conjunto com as demais áreas, a adequação e o fortalecimento dos controles internos, buscando mitigar os riscos de acordo com a complexidade de seus negócios;
• Apoiar os *Control Owners* em discussões a respeito de Controles Internos e elaboração de planos de ação aos riscos, bem como orientações sobre normas, procedimentos, controles e registros que compõem o ambiente de Controles Internos;
• Realizar avaliações periódicas dos controles internos através da realização de *walkthroughs*, testes de design (*ToD*) e eficiência de controles (*ToE*) em ciclos iniciais, de Interin e de final de ano, a fim de apoiar as áreas na verificação de que os controles internos estejam efetivos no Q4, de acordo com as normas do *PCAOB*;
• Analisar e avaliar os fluxos internos dos processos da empresa, identificando necessidades e oportunidades de melhoria, do ponto de vista de controles, com o objetivo de mitigar os riscos conhecidos da Companhia;

4.6 Compete à Auditoria Interna

• Avaliar de forma independente, a estrutura de Controles Internos, identificando fragilidades, inconformidades, erros e ilicitudes e reportar a área, de acordo com os padrões e normas definidos pelo *The IIA* (*Institute of Internal Auditors*);
• Assegurar que a estrutura de Gestão de Riscos e Controles Internos está operando de forma eficaz e reportar ao Comitê de Auditoria as suas avaliações;
• Elaborar e validar junto ao Comitê de Auditoria o plano plurianual de Auditoria;
• Inserir no plano de auditoria os processos vinculados aos riscos prioritários;
• Revisar e atualizar o plano anual de auditoria observando mudanças no negócio, riscos, processos, sistemas de informação e controles, sempre que se fizer necessário;
• Comunicar ao Comitê de Auditoria sobre alterações significativas e eventuais impactos da limitação de recursos no cumprimento do plano anual de auditoria;
• Suportar a área de Gestão de Riscos na elaboração da Matriz de Riscos;
• Implementar, manter e comunicar um programa de avaliação e melhoria da qualidade capaz de mensurar todos os aspectos que envolvem a auditoria interna, incluindo a conformidade com as Normas e Orientações Internacionais para a Prática Profissional de Auditoria Interna - IPPF, com o Código de Ética do *IIA* e a avaliação da eficiência e eficácia da auditoria interna, devendo comunicar ao Comitê de Auditoria o resultado das avaliações internas e da avaliação independente conduzida por terceiros (externo) pelo menos uma vez a cada 5 anos.

4.7 Compete ao *Compliance*

• Supervisionar a concepção e a implementação pela organização do sistema de gestão de *compliance*;
• Identificar e gerenciar riscos de *compliance* relacionados às obrigações da Companhia, suas atividades,

produtos, serviços e aspectos pertinentes das suas operações;
• Identificar e gerenciar riscos de *compliance* relacionados aos parceiros de negócio, como, por exemplo, os fornecedores, agentes, distribuidores, consultores e contratados;
• Documentar a avaliação dos riscos de *compliance*;
• Acompanhar investigações internas relacionadas à indícios de irregularidades;
• Acompanhar a execução de ações corretivas relacionadas à riscos de *compliance* determinadas pela Auditoria Interna.

4.8 Compete ao Comitê de Ética

• Assegurar a efetividade do sistema de compliance;
• Converter princípios e valores em normas sobre condutas admitidas e não admitidas;
• Acompanhar as ocorrências que envolvam condutas éticas praticadas pelos colaboradores da Companhia e de suas empresas controladas até a sua completa solução, coordenando as investigações de ilícitos ou irregularidades e recomendando penalidades a serem executadas pelos gestores imediatos, garantindo a equidade das sanções aplicadas;
• Assegurar medidas para elevar o nível de confiança (interna e externa), a imagem e a reputação da organização;
• Proteger o patrimônio físico e intelectual da organização;
• Supervisionar as atividades relacionadas aos canais de denúncias; e,
• Identificar oportunidades de melhoria dos processos internos relacionados ao Sistema de Gestão de Compliance.

4.9 Compete aos *Risk Owners*

• Avaliar os riscos nos formulários e ferramentas aplicáveis, quando solicitado pela área de Controles Internos e Gestão de Riscos;
• Revisar o risco identificado, bem como detalhar os fatores de risco, avaliação do risco, resposta e criticidade do risco e demais métricas aplicáveis;
• Estabelecer indicadores para monitoramento dos riscos e metas para implementação dos planos de ação de resposta aos riscos;
• Acompanhar e realizar reportes periódicos do(s) risco(s) sob sua responsabilidade, bem como os resultados dos indicadores (*KRIs*) a ele(s) atrelados;
• Estabelecer e implementar planos de ação, quando aplicável, necessários para tratamento dos riscos prioritários juntamente com as demais áreas envolvidas, indicando os responsáveis e o prazo de finalização;
• Informar a área de Gestão de Riscos sobre as mudanças na probabilidade e/ou impacto do risco ou sobre qualquer alteração na característica do mesmo;
• Informar a área de Gestão de Riscos ao identificar riscos emergentes não mapeados e tratados; e
• Disseminar a cultura da gestão de risco na Unidade de Negócio (*BUs*).

4.10 Compete aos *Control Owners*

• Revisar continuamente os processos sob sua responsabilidade e manter atualizada a documentação de processos e controles (*flowcharts* e *RaCM*);
• Executar e documentar, com evidências, todos os controles internos, de acordo com as definições na

RaCM sob sua responsabilidade (para verificação das áreas de Controles Internos e Auditoria);
• Estabelecer indicadores para monitoramento dos riscos e metas para implementação dos planos de ação de resposta aos riscos;
• Suportar a implementação dos planos de ação, quando aplicável;
• Informar ao *Risk Owner* sobre mudanças na probabilidade e/ou impacto do risco ou sobre qualquer alteração na característica do mesmo; e
• Informar ao *Risk Owner* tempestivamente ao identificar riscos emergentes não mapeados e tratados.

4.11 Compete aos colaboradores e *key users*

• Disponibilizar informações suporte na identificação ou avaliação de riscos novos e existentes no ambiente de Controles Internos;
• Cumprir com orientações e diretrizes internas referentes a identificação e gestão dos riscos corporativos;
• Comunicar a um nível organizacional mais elevado, ou mediante os canais de comunicação disponibilizados pela Companhia, quaisquer problemas na operação, no descumprimento do Código de Conduta Ética, ou em outras infrações às políticas ou procedimentos definidos que venha a tomar conhecimento.

5. DIRETRIZES

5.1 Princípios Gerais

Gestão de Riscos é um processo cíclico e contínuo, utilizado para identificar, entender e responder aos riscos que exponham a Portobello na busca por seus objetivos estabelecidos, além de gerar valor aos sócios e demais *stakeholders*. Visa assegurar que os responsáveis pela tomada de decisão, tenham acesso tempestivo as informações suficientes, quanto aos riscos dos quais está exposta, aumentando a probabilidade de alcance dos objetivos e reduzindo os riscos a níveis aceitáveis.

5.2 Processo de Gestão de Riscos

A Gestão de Riscos é um processo estruturado e segue as etapas demonstradas a seguir:

5.2.1 Estabelecimento do Contexto

Na etapa de estabelecimento do contexto duas atividades são realizadas, a fim de garantir o entendimento do ambiente no qual o Grupo está inserido.

a) **Entendimento do Grupo e seu contexto:** A fim de definir uma estrutura de Gestão de Riscos adequada, o contexto externo (ambiente financeiro, econômico, regulatório, relações com *stakeholders*, etc.) e interno (modelo de governança, estrutura organizacional, objetivos estratégicos, estrutura de capital, etc.) do Grupo devem ser analisados através do estudo dos materiais corporativos, entrevistas com os gestores e executivos e fontes de informações externas.

b) **Definir Capacidade, Apetite e Tolerância ao Risco do Grupo:** O Apetite ou Tolerância aos Riscos do Grupo são sugeridos pela área de Gestão de Riscos e aprovadas pelo Conselho de Administração, visando determinar parâmetros para análise de Impacto dos Riscos Corporativos da Portobello.

5.2.2 Identificação de Riscos

Após a contextualização dos fatores internos e externos relevantes para o entendimento da exposição aos riscos da Portobello, realiza-se a etapa de identificação e registro de riscos. Esta etapa é conduzida de maneira colaborativa e sistemática, através de reuniões com líderes e gestores da Companhia, para que de acordo com seus conhecimentos das operações, e pontos de vista forneçam uma visão realista e adequada dos Riscos Corporativos.

O objetivo desta etapa é compreender e registrar os riscos baseados nos eventos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos estratégicos.

Apesar de estar relacionada há um processo amplo de avaliação de riscos é importante ressaltar que a identificação de riscos pode ocorrer a qualquer momento e deve ser analisada tempestivamente pela área de Gestão de Riscos da Companhia, para que esta avalie junto aos gestores relacionados se há necessidade de discussão imediata do tema junto ao Comitê Executivo de Riscos, Conselho de Administração e Diretoria da Companhia.

5.2.3 Classificação dos Riscos (Dicionário de Riscos)

Os Riscos Corporativos na Portobello podem ser divididos nas seguintes categorias:

• **Riscos estratégicos:** associados com as decisões estratégicas do Grupo para atingir os seus objetivos de negócio e/ou decorrentes da falta de capacidade ou habilidade da empresa para proteger-se ou adaptar-se a mudanças no ambiente. Estão relacionados à Governança, inteligência competitiva e modelos de negócio que podem afetar a continuidade do negócio.

• **Riscos de reporte:** relacionados com falhas no processo de captura dos detalhes financeiros ou contábeis que possam impactar a integridade dos demonstrativos da Companhia e o atual reflexo de sua saúde financeira.

• **Riscos operacionais:** decorrentes da falta de consistência e adequação dos sistemas de informação, processamento e controle operacional, bem como de falhas no gerenciamento de recursos e nos controles internos que tornem impróprio o exercício das atividades da Companhia.

• **Riscos regulatórios ou de *compliance*:** aqueles associados ao ambiente regulatório que podem resultar em sanções legais ou regulatórias, perdas financeiras ou de reputação por fraudes, falha no cumprimento de leis, acordos, regulamentos, Código de Conduta e/ou das documentações normativas da Portobello.

• **Riscos de tecnologia da informação e *cybersecurity*:** referem-se à probabilidade de exposição da Companhia a perdas financeiras, interrupção de atividades ou danos à reputação resultantes de falhas, erros, violações ou ataques aos seus sistemas e ativos tecnológicos.

5.2.4 Análise e Avaliação de Riscos

A análise de riscos desenvolve a compreensão dos riscos identificados, devendo fornecer subsídios preliminares para o posterior processo de avaliação de riscos. Começa com a apreciação das causas e das fontes

de risco, suas consequências positivas e negativas, e a probabilidade e impacto de que essas consequências possam acontecer, caso o mesmo se materialize.

Para apoiar essas avaliações, a área de Gestão de Risco deve sugerir critérios de análises que estabeleçam níveis aceitáveis dentro das variáveis de probabilidade e impacto que serão construídas e revisadas a cada rodada de *Risk Assessment* de acordo com o cenário atual interno e externo e uma visão de materialidade das Demonstrações Financeiras da Portobello, e devem ser aprovados pelo Conselho de Administração.

5.2.4.1 Escalas de Impactos e Probabilidade

a) **Análise do Impacto:** é a consequência com efeitos positivos ou negativos sobre os objetivos, podendo ser expresso, qualitativa ou quantitativamente;

b) **Análise da probabilidade:** é a avaliação qualitativa e/ou quantitativa da possibilidade de ocorrência do evento. Pode ser feita com base em um histórico da materialização do risco, estrutura de controles e/ou percepção do *Risk Owner*.

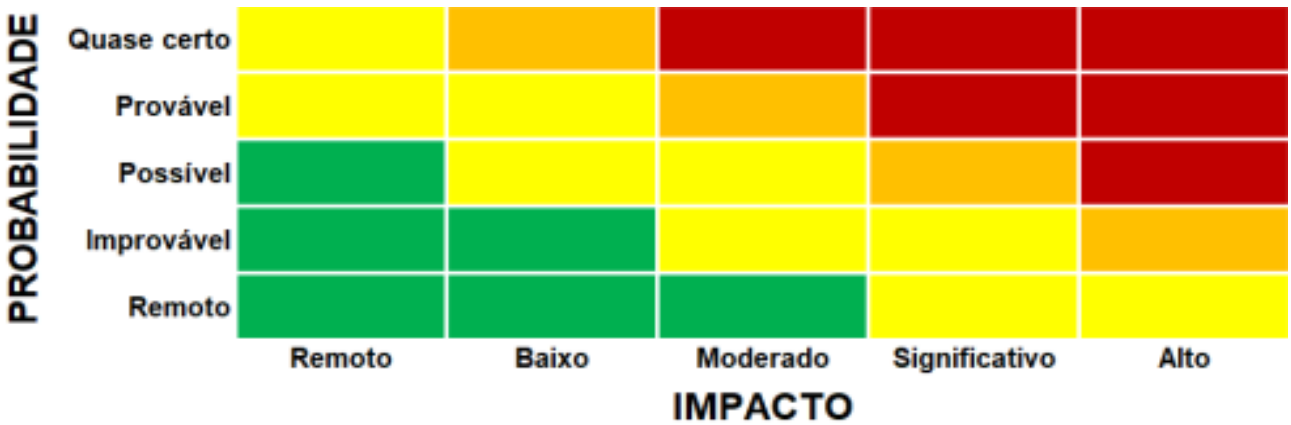
5.2.5 Priorização dos riscos

A finalidade desta etapa é auxiliar o processo de tomada de decisões do Conselho de Administração, pontuando o direcionamento e priorização das iniciativas necessárias para responder às principais ameaças as quais a Companhia está exposta.

Após obtenção do resultado da avaliação de Impacto e Probabilidade de cada risco, cabe a área de Gestão de Riscos consolidar todos os riscos em uma Matriz de Riscos e exibi-los graficamente em um *Heat Map*.

Esta visualização gráfica de priorização e tratamento dos eventos ajudará a área de Gestão de Riscos a definir os riscos prioritários da Portobello, que deverão ser validados formalmente pelo Conselho de Administração.

Exemplo de representação gráfica da "Matriz de Riscos" ou "*Heat Map*"



Os Riscos Corporativos posicionados na região **vermelha** são classificados como **Riscos Muito Altos** e os Riscos Corporativos posicionados na região **laranja** são classificados como **Riscos Altos**. Ambos demandam ação gerencial prioritária para eliminar as causas e os fatores de riscos ou reduzir sua severidade e/ou frequência.

Os Riscos Corporativos da região **amarela** são classificados como **Riscos Médios** que representam as perdas frequentes e normalmente incorporadas ao custo da operação, mas que requerem monitoramento. Os da região **verde** são os **Riscos Baixos** considerados aceitáveis, não havendo necessidade de monitoramento ou ações de mitigação.

5.2.6 Tratamento de Riscos

Envolve a seleção de uma ou mais opções para mitigar os riscos e a priorização no cronograma de implementação. Pode ser necessário que a Portobello decida implementar medidas ou controles compensatórios, até ser implementada uma solução definitiva. Uma vez implantadas as medidas, o tratamento do risco fornece novos controles ou modifica os riscos existentes gerando um ambiente mais robusto e transparente.

A etapa de tratamento dos riscos envolve a definição por parte da gestão de uma resposta para os riscos identificados de modo a trazer a exposição a um determinado risco a um nível que seja aceitável para a organização. Essas respostas podem variar, conforme o apetite a riscos do Grupo. Entre as possibilidades de tratamentos temos:

a) **Eliminar risco:** esta opção é possível mediante a eliminação do processo ou ação que gera o evento de risco;

b) **Diminuir risco:** esta opção requer a criação de controles que minimizem a potencial exposição do evento de risco, seja reduzindo o Impacto no negócio e/ou a Probabilidade de ocorrência;

c) **Transferir risco:** esta opção permite continuar com uma operação de um processo de risco, com a garantia que caso se materialize a responsabilidade financeira ou de resposta aos danos está como responsabilidade de terceiros;

d) **Aceitar risco:** esta opção permite continuar operando com a atual estrutura de controles existentes; ou aceitar a materialização potencial do risco, devido a não existência ou impossibilidade de implementação de um tratamento do ponto de vista econômico ou operacional.

5.2.7 Monitoramento, Análise Crítica e Melhoria Contínua

Consistem na verificação, supervisão e observação crítica e contínua dos riscos, a fim de identificar mudanças no nível de criticidade, Probabilidade e/ou Impacto, identificar riscos emergentes, bem como monitorar o nível e desempenho requerido ou esperado dos planos de ação e indicadores.

Para que o processo de gestão de riscos seja efetivo, os riscos identificados e priorizados serão acompanhados e analisados periodicamente, com base nas diretrizes definidas neste documento.

Adicionalmente, para fins de melhoria contínua, a Portobello deverá conduzir anualmente (ou pontualmente, caso aplicável) uma avaliação de maturidade do ambiente de Gestão de Riscos (*Risk Assessment*) para identificação de melhorias e desenvolvimento dos planos de ação. A área de Controles Internos e Gestão de Riscos comunicará à Diretoria Corporativa, Conselho de Administração, Comitê Executivo de Riscos e Comitê de Auditoria os resultados das avaliações, bem como as ações de melhoria recomendadas.

5.2.8 Comunicação dos Riscos

Tem como premissa a implementação de processos contínuos e interativos que permitem fornecer, compartilhar ou obter informações, além de propiciar o diálogo com as partes interessadas, sobre a situação geral de riscos e as medidas tomadas pela Portobello para mitigação e tratamento dos mesmos. Esse reporte deverá ser feito mensalmente na agenda de integração entre as áreas, sobre responsabilidades da área de Gestão de Riscos, conforme calendário de gestão de riscos previsto.

A cultura de Gestão de Riscos também deve ser difundida na Portobello, através da realização de palestras, treinamentos periódicos e ações de comunicação para os colaboradores. Adicionalmente, a documentação orientadora sobre Gestão de Riscos e quaisquer outras informações relevantes deve ser disponibilizada prontamente para todos colaboradores.

A comunicação dos riscos deve assegurar o adequado conhecimento dos envolvidos de forma a permitir a efetividade das medidas de prevenção, detecção e correção dos riscos:

a) Riscos estratégicos, reporte, tecnologia da informação e *cybersecurity*: são acompanhados pela área de Gestão de Riscos e Controles Internos e devem ser reportados para Diretoria Corporativa e Conselho de Administração;

b) Riscos regulatórios e de *Compliance*: são acompanhados pela área de *Compliance* e devem ser reportados para Diretoria Corporativa e Conselho de Administração;

c) Riscos operacionais: são acompanhados pela área de Gestão de Riscos e Controles Internos e devem ser reportados à Diretoria Corporativa e ao Conselho de Administração.

Obs.: A Auditoria Interna, por premissa, verifica de forma independente, dentro do seu plano plurianual de auditoria ou através de solicitações realizadas pelo CA, quaisquer tipos de riscos, processos ou investigações especiais mencionadas acima ou não, que são prerrogativas de sua função.

5.2.9 Framework GRC

Abaixo encontra-se o Framework GRC da Portobello Grupo, definindo as responsabilidades e escopo de atuação das principais diretorias/áreas envolvidas na estrutura de governança corporativa:

	Reporte Subordinação	Relação com COAUD	Base legal	Atuação	Escopo
Grupo de Controle	Autodeterminação	Interação e Independência	Acordo de Acionistas e Lei das S/A	Colegiado c/ Membro Representante do Bloco	Controle Societário, diretrizes e rumo estratégico assegurando o cumprimento do objeto social
Conselho de Administração (CA)	Acionistas (AGO)	Assessoramento	Lei das S/A	Colegiado	Direcionamento estratégico da organização
Conselho Fiscal	Acionistas (AGO)	Cooperação e respeito às alçadas	Lei das S/A	Colegiado	Fiscalização para reporte aos acionistas
Comitê de Governança Estratégica	CA	Interação e Independência	Boa prática de governança	Colegiado	Proposição do plano estratégico
Diretoria Estatutária	CA	Interação e Independência	Lei das S/A	Colegiado e interdependente	Gestão da organização conforme o direcionamento estratégico
Comitê de Sustentabilidade	CA	Cooperação	Boa prática de governança	Colegiado	Gestão do Plano de Sustentaiblidade, Riscos e Orçamento Matricial
Comitê de Auditoria	CA	-	Reg. Novo Mercado e Boa prática de Governança	Colegiado	Assessoramento ao Cons. de Adm. (DFs e GRC),
Comitê Executivo de Riscos	CEO	Cooperação	Boa prática de governança	Colegiado	Estratégia e Gestão de Riscos, integração com o negócio e orçamento
Comitê de Ética	CEO	Cooperação	Reg. Novo Mercado	Colegiado	Gestão do Código de Ética e Conduta
Auditoria Independente (Externa)	Comitê de Auditoria	Colaboração e Independência	Lei das S/A	Independente	Confiabilidade das demonstrações financeiras
Auditoria Interna	Comitê de Auditoria	Proximidade, Orientação e Confiança	Reg. Novo Mercado	Interdependente	Avaliação para aperfeiçoamento dos sistemas de GRC
Gestão de Riscos e Controles Internos	VP de Finanças	Cooperação	Reg. Novo Mercado e Boa prática de Governança	Interdependente	Gestão do ambiente de controle, ERA, suporte à Gestão de Riscos e ações de mitigação
Compliance	Jurídico Corporativo	Cooperação	Reg. Novo Mercado	Interdependente	Gestão da conformidade, integridade e da ética

6. DISPOSIÇÕES GERAIS

Os colaboradores são responsáveis por conhecer e compreender todos os documentos orientadores que lhes forem aplicáveis. De forma similar, os Líderes são responsáveis por garantir que todos os colaboradores de suas equipes compreendam e sigam os documentos orientadores aplicáveis.

Os colaboradores que tiverem questionamentos ou dúvidas a respeito desta Política, incluindo seu escopo, termos ou obrigações, devem procurar seus respectivos Líderes e, se necessário, a área de Controles Internos e Gestão de Riscos.

Falhas e/ou violações no cumprimento ou relatos de conhecimento de violação desta política poderão resultar em ação disciplinar para qualquer colaborador envolvido.

7. DEFINIÇÕES

Apetite ou Tolerância aos riscos: nível máximo ao qual a Portobello está disposta a se expor, manter, assumir ou buscar em relação ao(s) risco(s) para cumprir seus objetivos e agregar valor aos *stakeholders*.

Avaliação de riscos: processo estabelecido pela PBG que permite direcionar o cálculo na análise dos riscos corporativos.

Classificação dos riscos: Forma de agrupar e identificar os riscos, podendo ser classificados entre Estratégico, de Reporte, Operacional, Regulatório e *Compliance*, de TI e *Cybersecurity* e Reputação e Imagem.

Controle: políticas, normas, procedimentos, métodos e mecanismos criados com o objetivo de proporcionar um grau de confiança razoável na eficácia e eficiência das operações, nos relatórios financeiros e no cumprimento das exigências regulatórias, além do atingimento dos objetivos de negócio, prevenindo, detectando e corrigindo eventos indesejáveis.

Control owner* (Dono do controle)*: responsável por desenhar, atualizar, executar, monitorar e suportar a implementação dos planos de ação dos controles, de forma a mitigar a materialização dos riscos.

CVM: Comissão de Valores Mobiliários.

Dicionário de Riscos: base de informações que classifica e categoriza os riscos em uma linguagem comum. Inclui as classificações dos riscos dentro da taxonomia, auxiliando e fortalecendo a cultura de riscos na Portobello.

Evento: incidente, ocorrência ou mudança, internas ou externas à Portobello, que venha a impactar ou alterar as circunstâncias ou as chances de alcance dos objetivos da Portobello. Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas e várias consequências. Um evento pode também ser esperado, mas não ocorrer, ou inesperado e ocorrer.

Executivos: líderes com delegação de tomada de decisão estratégica. Inclui o Presidente do Grupo, Diretores das Unidades de Negócios e demais membros do Conselho de Administração.

Gestão de Riscos: atividades, fundamentos metodológicos e definições organizacionais coordenadas para orientar e apoiar a PBG na implementação, monitoramento e melhoria contínua no que se refere aos seus riscos.

Gestores: coordenadores e gerentes responsáveis pela comunicação e monitoramento da execução do plano de ação em equipes e seus resultados.

***Heat Map* (Mapa de Risco):** representação gráfica de exposição do Impacto vs Probabilidade dos riscos identificados pela Portobello.

Impacto: consequência da materialização do evento de risco nos objetivos.

IBGC: Instituto Brasileiro de Governança Corporativa.

***Institute of Internal Auditors – IIA* (Instituto de Auditores Internos):** organização que defende e promove conferências educacionais e desenvolve padrões, orientações e certificações para a profissão de Auditor Interno.

***Key Risk Indicator – KRI* (Indicador de Risco-Chave):** indicador que sinaliza as mudanças no nível de risco da Portobello e/ou de suas Unidades de Negócios. Auxilia a Portobello a reduzir perdas e minimizar a exposição, lidando com o fator de risco antes do evento se materializar.

***Key Users* (Usuários chave):** especialistas com domínio de suas atividades e dos processos em seu setor, sendo representante da área em projetos da Portobello.

Nível de risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos.

Organização: pessoa ou grupo de pessoas que tem suas próprias funções com responsabilidades, autoridades e relacionamentos para alcançar os objetivos da Portobello. O conceito de organização inclui, mas não está limitado a Companhia, corporação, empresa, parte ou combinação deles, seja ela incorporada ou não, pública ou privada.

PBG S/A: Portobello Grupo Sociedade Anônima.

Plano de ação: conjunto de medidas adotadas para tratar os riscos identificados, de forma a evitar sua materialização ou reduzir a probabilidade e/ou o impacto dessa materialização, levando esses fatores a níveis compatíveis com o apetite a riscos da Portobello. Pode abranger quaisquer áreas da Portobello e passar por criação, melhoria e/ou auditoria de processos e controles, utilização de sistemas e instrumentos específicos de identificação e proteção.

Probabilidade: medida da possibilidade de ocorrência de um evento de risco.

Public Company Accounting Oversight Board – PCAOB **(Conselho de Supervisão Contábil de Empresa Aberta):** é uma corporação sem fins lucrativos estabelecida pelo Congresso para supervisionar as auditorias de empresas públicas, a fim de proteger os investidores e promover o interesse público na preparação de relatórios de auditoria informativos, precisos e independentes.
Resposta ou tratamento ao risco: decisão de mitigar, evitar, compartilhar ou aceitar um risco.

Risco: fatores ou eventos incertos que podem causar impactos negativos, dificultando ou impossibilitando o cumprimento dos objetivos da empresa ou de seus processos. Em geral, o risco é medido em termos de impacto e de probabilidade. O risco também possui a definição da ISO 31000: “é o efeito da incerteza sobre os objetivos”.

Risk owner **(Dono do risco):** tem o papel de notificar a área de Gestão de Riscos e Controles Internos em relação a alterações em risco(s) ou inclusão de novo(s) risco(s) sob sua responsabilidade, garantindo que o risco seja gerenciado adequadamente.

Risco inerente: risco a que uma organização está exposta sem considerar ações de resposta/tratamento que possam reduzir a probabilidade de ocorrência ou impacto (mitigação).

Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco.

Securities and Exchange Commission – SEC **(Comissão de Valores Mobiliários):** Agência americana independente responsável por proteger os investidores do mercado de capitais.

The Committee of Sponsoring Organizations - COSO **(Comitê de Organizações Patrocinadoras**): entidade sem fins lucrativos que se propõe a liderar a geração de conhecimento por meio do desenvolvimento de estruturas e diretrizes sobre Controles Internos, gerenciamento de riscos corporativos e prevenção de fraudes financeiras.

INFORMAÇÕES DE CONTROLE

Esta Política passará a vigorar a partir da sua data de publicação e deve ser revisada anualmente ou a qualquer tempo, sempre que necessário.

O conteúdo da presente Política poderá ser alterado apenas mediante aprovação do Conselho de Administração, sempre que o referido órgão entender necessário ou em decorrência de alterações regulatórias.

Criação: 28/04/2022
Última revisão: 14/08/2023

Responsável	Área
Elaboração	**Gestão de Riscos e Controles Internos**
Revisão	**Diretoria Estatutária, Comitê Executivo de Riscos e Comitê de Auditoria**
Aprovação	**Conselho de Administração**