PORTO SEGURO S.A.

CNPJ/MF nº 02.149.205/0001-69

NIRE 35.3.0015166.6

Companhia Aberta – CVM nº 01665-9

POLÍTICA DE GESTÃO DE RISCOS

ÍNDICE

1. OBJETIVO 4

2. ABRANGÊNCIA 4

3. REFERÊNCIA NORMATIVA 4

4. ESTRUTURA DE GESTÃO DE RISCOS 4

4.1. Definições 4

4.2. Missão 4

4.3. Objetivos e Estratégia 5

4.4. Modelo de 3 linhas 5

5. PROCESSO DE GESTÃO DE RISCOS 6

5.1. Identificação / Avaliação de Riscos 6

5.2. Mensuração de Riscos 7

5.3. Tratamento de Riscos 7

5.4. Monitoramento e Reporte de Riscos 8

6. AVALIAÇÃO DE RISCOS E CONTROLES DE PROCESSOS, METODOLOGIAS E FERRAMENTAS 8

7. PROCESSO DE GESTÃO DE RISCOS E ALINHAMENTO AO APETITE POR RISCO 8

7.1. Capacidade de Tomada de Risco 9

8. POLÍTICAS CORRELATAS DE GERENCIAMENTO DE RISCOS 9

9. TAXONOMIA DE RISCOS 11

9.1. Risco de Subscrição 11

9.2. Risco de Crédito 11

9.3. Risco de Mercado 11
9.4. Risco de Liquidez 11
9.5. Risco Operacional 11
9.6. Risco de Modelo 12
9.7. Risco de Capital 12
9.8. Risco Socioambiental e Climático 12
9.9. Risco Cibernético 12
9.10. Risco de Terceiros 12
9.11. Demais Riscos 12
10. PAPÉIS E RESPONSABILIDADES 12
10.1. Conselho de Administração 12
10.2. Diretoria Executiva 13
10.3. Gestores das Unidades Operacionais e de Negócios (Primeira Linha) 13
10.4. Comitê de Risco Integrado (CRI) 14
10.5. Gerência de Gestão de Riscos Corporativos 15
10.6. Controles Internos 15
10.7. Auditoria Interna 16
11. VIGÊNCIA 16
12. APROVAÇÃO 16
13. ANEXO I - REGIMENTO INTERNO DO COMITÊ DE RISCO INTEGRADO 17

1. OBJETIVO

Esta Política Corporativa de Gestão de Riscos da Porto (“Política”) estabelece o conjunto de princípios, diretrizes, estratégias, ações, papéis e responsabilidades necessários à identificação, avaliação, tratamento e controle dos riscos inerentes às atividades da Porto Seguro S.A. e Controladas (“Grupo Porto”).
Para os fins desta Política, entende-se por “Controladas” todas as pessoas jurídicas que sejam controladas por, ou estejam sob o controle comum da Porto Seguro S.A. (CNPJ n.º 02.149.205/0001-69), considerando-se, para tanto, a definição de controle prevista nos artigos 116 e 243, § 2º, da Lei n.º 6.404/1976.

2. ABRANGÊNCIA

Esta Política se aplica a todos os empregados, administradores, estagiários, jovens aprendizes, prestadores de serviços, bem como qualquer outra pessoa que tenha poderes para representar quaisquer empresas do Grupo Porto (“Colaboradores”).

3. REFERÊNCIA NORMATIVA

Servem de referência para os procedimentos descritos nesta Política as disposições descritas nos seguintes normativos:

- Resolução CNSP nº 416/2021;
- Circular Susep nº 638/2021;
- Circular Susep nº 648/2021;
- Resolução CMN nº 4.557/2017;
- Resolução CMN nº 4.893/2021;
- Resolução Normativa ANS nº 518/2022;
- Regulamento do Novo Mercado;
- Código das Melhores Práticas de Governança Corporativa do Instituto Brasileiro de Governança Corporativa (IBGC);
- Código Brasileiro de Governança Corporativa – Companhias Abertas.

4. ESTRUTURA DE GESTÃO DE RISCOS

4.1. Definições

A estrutura de gestão de riscos (EGR) é definida como o conjunto de componentes que fornecem os fundamentos e arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de uma organização.
Por sua vez, a gestão de riscos é definida como o conjunto de atividades coordenadas para identificar, avaliar mensurar, tratar e monitorar os riscos de uma organização, tendo por base a adequada compreensão dos tipos de risco, de suas características e interdependências, das fontes de riscos e de seu potencial impacto sobre o negócio.
O objetivo da gestão de riscos não é eliminar os riscos, mas gerenciá-los de acordo com o apetite por risco estabelecido, para maximizar as oportunidades e minimizar os efeitos adversos.

4.2. Missão

A missão do processo de gestão de riscos do Grupo Porto é:

(i) assegurar que o apetite por riscos do Grupo Porto esteja alinhado com sua capacidade e ao plano de negócios;
(ii) reduzir a ocorrência de eventos inesperados e perdas operacionais, assim como fomentar as oportunidades de negócio;
(iii) identificar, mensurar, gerenciar, monitorar e reportar os riscos que afetam o cumprimento dos objetivos estratégicos, operacionais e financeiros do Grupo Porto;
(iv) integrar a gestão de riscos à estratégia do Grupo Porto e nos processos de tomada de decisão;
(v) preservar a solvência do Grupo Porto, ao definir limites para que os riscos não superem o apetite por risco estabelecido;
(vi) proteger a marca e a reputação do Grupo Porto, fomentando valores fundamentais do Grupo;
(vii) promover cultura sólida de consciência e de tomada de riscos por todos os Colaboradores;
(viii) melhorar a criação de valor e atingir um melhor perfil de risco-retorno com a utilização eficaz do capital; e
(ix) suportar os processos de tomada de decisão, ao fornecer informações confiáveis, oportunas e consistentes.

4.3. Objetivos e Estratégia

O gerenciamento dos riscos é altamente estratégico no Grupo Porto, devido a crescente inovação dos serviços e produtos ofertados, assim como resultado da globalização dos negócios, aumento das tecnologias e regulamentações envolvidas, tornando suas atividades de gestão cada vez mais complexas. Neste contexto e com foco na sustentabilidade e continuidade dos negócios (longo prazo), o Grupo Porto trabalha continuamente na melhoria das estruturas e ferramentas de gestão de risco, assim como no aprimoramento de seu gerenciamento e controle.

4.4. Modelo de 3 linhas

A abordagem de três linhas é a base da EGR do Grupo Porto, em que há:

Primeira linha (Unidades Operacionais) – As diversas unidades operacionais e de negócios que lidam diretamente com os negócios e com a exposição aos riscos do Grupo Porto. Dessa forma é esperado que as unidades de negócio adotem procedimentos e controles adequados para que sua gestão esteja alinhada com os apetites e as diretrizes definidas pela organização.
Segunda linha (Funções de Controle) – As funções de controle têm como responsabilidade orientar e supervisionar se os processos e controles definidos pela primeira linha estão de acordo com as diretrizes organizacionais. As funções de controle estão relacionadas principalmente à área de Gestão de Riscos Corporativos, Compliance e Controles Internos.
Terceira linha (Auditoria Interna) – A função de auditoria interna atua de forma mais ampla e independente na verificação da aderência às diretrizes ao avaliar a eficácia do ambiente de gestão e controle de riscos (supervisão sobre a primeira e segunda linha).
Conforme descrito acima, a governança de gerenciamento de riscos conta com a participação de todas as áreas, tendo por finalidade proteger o resultado do Grupo Porto e seus acionistas, contribuir para sua sustentabilidade e valor, envolvendo aspectos relacionados à transparência e prestação de contas.
Refletindo o compromisso com a gestão de riscos, o Grupo Porto possui a área de Gestão de Riscos Corporativos cuja missão é garantir que os riscos sejam efetivamente identificados, mensurados, mitigados, acompanhados e reportados de forma independente.

A EGR também conta com o apoio de Comitês específicos, tais como o Comitê de Riscos Integrado (CRI) e o Comitê de Auditoria.
O CRI tem como objetivo fornecer subsídios e informações ao Conselho de Administração em assuntos referentes à gestão de riscos, propondo planos de ação e diretrizes, avaliando o cumprimento das normas de gestão de riscos e acompanhando os indicadores-chave de riscos em todas as sociedades que compõem o Grupo Porto. Neste sentido destaca-se a revisão e aprovação anual da Política Corporativa de Gestão de Riscos, zelo pelo cumprimento das demais políticas e prover recomendações relacionadas ao apetite e limites de exposição por tipo de risco.
O funcionamento do CRI, incluindo suas atribuições, composição, reuniões e convocações assim como disposições gerais é definido em regimento interno, o qual é aprovado pelo Conselho de Administração da Porto Seguro S.A. e se encontra no anexo I desta política.
Adicionalmente ao CRI, há o Comitê de Auditoria, o qual possui como objetivo principal fornecer suporte à Administração do Grupo Porto na atuação da Governança Corporativa, voltada à transparência dos negócios.
De forma resumida, a EGR é pautada nos seguintes aspectos:

- Segregação de funções: controle x unidades operacionais e de negócios.
- Decisões colegiadas e em diversos níveis hierárquicos.
- Normas, procedimentos, competências e responsabilidades documentados e claramente definidos.
- Visão integrada dos riscos por meio de estrutura específica para o gerenciamento de risco.
- Referência às melhores práticas de gestão de riscos.

Ressalta-se que é de responsabilidade da Diretoria zelar pela adequação da EGR. Adicionalmente, a avaliação da EGR pela Diretoria é realizada, no mínimo anualmente, ou em face de mudanças significativas no perfil de riscos, por meio das informações e relatórios gerados a partir do Inventário de Riscos, assim como pela Auditoria Interna no exercício de suas atribuições.

5. PROCESSO DE GESTÃO DE RISCOS

De forma geral, a maneira como os riscos podem afetar o Grupo Porto são dinâmicos, variando de acordo com a evolução dos ambientes internos e externos em relação ao Grupo. É essencial que o processo de gestão de riscos seja realizado de forma recorrente, de forma a garantir a adequação do gerenciamento dos riscos ao longo do tempo. Esse processo é representado por um ciclo, conforme ilustrado abaixo:

5.1. Identificação / Avaliação de Riscos

O primeiro passo consiste na identificação e avaliação dos eventos que podem afetar a organização. Esta etapa é relevante uma vez que eventos/riscos não identificados não podem ser mensurados, tratados e monitorados.

O resultado desta etapa é denominado de perfil de riscos, o qual reflete as exposições de uma organização a riscos, considerando os riscos assumidos, suas causas, interdependências e potenciais impactos.
Por sua vez, é necessária a elaboração e manutenção de um inventário de riscos que descreva cada risco identificado, indique sua categoria, suas causas e possibilite atribuir responsabilidades em relação à sua gestão.
No Grupo Porto, para a identificação dos eventos de risco são utilizadas uma combinação de estratégias, incluindo a avaliação de eventos já materializados assim como de eventos não materializados, mas que, entretanto, podem vir a ocorrer. Entre outras estratégias, destacam-se:

- **Avaliação de indicadores chaves de riscos** - realizado o acompanhamento periódico pelas áreas operacionais e de negócio assim como pelas funções de controle.

- **Avaliação do fluxo do processo** – Realizado periodicamente o processo de avaliação dos riscos e controles (Mapeamento de Riscos e Controles ou RCSA - Risk and Control Self Assessment) junto às diversas unidades operacionais e de negócios (primeira linha).

- **Banco de Dados de Perdas Operacionais (BDPO)** – A base de dados de perdas operacionais representa uma importante fonte, contendo os riscos materializados, e sua finalidade é retroalimentar o perfil de risco do Grupo.

- **Avaliações junto ao Nível Executivo** – Nas diversas reuniões, fóruns e comitês são debatidos os riscos e principais preocupações que podem vir a impactar os objetivos estabelecidos.

5.2. Mensuração de Riscos

A mensuração permite a atribuição do nível de risco aos riscos identificados no perfil, definida no item anterior.
O nível de risco é definido como “a magnitude de um risco, expressa em termos da combinação de sua probabilidade e impacto”. Sua mensuração é realizada por meio de métodos qualitativos e/ou quantitativos, a depender da disponibilidade de dados estruturados e históricos disponíveis.
Em detalhes, os métodos quantitativos envolvem o uso de técnicas matemáticas e/ou estatísticas para estimar, a partir de dados de sua operação e/ou de mercado, a probabilidade de ocorrência dos principais riscos a que se encontra exposta e o correspondente valor de perda, devendo ser baseados em fórmulas analíticas, simulações estocásticas ou estresse de projeções econômico-financeiras.
Por sua vez, os métodos qualitativos envolvem a utilização da experiência e opinião de especialistas, sendo, portanto, essencial o envolvimento das unidades operacionais e de negócios em sua definição.
Normalmente, as técnicas quantitativas geram maior precisão nas análises e são utilizadas em riscos que podem gerar maior impacto, visto requerer maior esforço em sua mensuração.
No Grupo Porto, os riscos são avaliados minimamente de forma qualitativa, sendo que, para os riscos considerados de maior relevância, são realizadas avaliações quantitativas por meio de metodologias específicas, detalhadas nas políticas mencionadas no item 8 desta política.
Vale ressaltar que, independentemente da metodologia utilizada na mensuração dos riscos, é necessário que as mesmas sejam documentadas pelas unidades operacionais, de negócios e/ou de controle responsáveis, incluindo as fontes de dados utilizadas, no caso de metodologias quantitativas.

5.3. Tratamento de Riscos

A etapa de tratamento de riscos consiste na definição das ações que deverão ser adotadas, para cada risco, visando manter suas exposições dentro dos limites estabelecidos nas políticas e procedimentos, além de ações para avaliação da efetividade de tais medidas.
Dentre das estratégias adotadas, destacam-se:

- **Evitar:** consiste geralmente em não realizar uma operação, sendo adequada quando o Grupo Porto conclui que determinada operação possui um Nível de Risco muito elevado. Entretanto, antes de se adotar esta alternativa, poderão ser avaliadas outras estratégias, com implicação na avaliação da relação risco x retorno da operação.

- **Mitigar:** significa agir para reduzir a probabilidade e/ou o impacto de um risco, trazendo seu Nível de Risco para um patamar considerado aceitável. Permite a proteção contra efeitos negativos dos riscos de uma determinada operação sem obrigatoriamente desistir desta, podendo assim maximizar a relação risco x retorno.

- **Compartilhar:** ocorre quando uma organização repassa parte de um risco para outra que, mediante contrato, obriga a indenizá-la caso o risco se materialize.

- **Aceitar:** ocorre quando não se adota nenhuma ação em relação ao risco, seja pela inexistência no mercado de um controle específico para a operação ou pelo alto investimento necessário para implementação de controle. Normalmente a organização adota esta estratégia para operações que apresentam baixo Nível de Risco.

5.4. Monitoramento e Reporte de Riscos

Esta etapa consiste na definição de indicadores ou variáveis para o monitoramento dos níveis de exposição aos principais riscos, de forma a aferir que as exposições se encontram dentro dos limites estabelecidos no Apetite por Riscos e a alinhado com as diretrizes internas estabelecidas nesta Política ou nas políticas específicas.
Conforme a característica e relevância dos riscos, são definidas diferentes periodicidades para o monitoramento dos riscos.
Em linhas gerais, são previstos reportes periódicos do nível de risco de forma a avaliar sua aderência ao apetite por risco definido pelo Conselho de Administração. Caso sejam identificadas situações de desenquadramento, é previsto que as unidades operacionais e de negócios (primeira linha) responsáveis justifiquem os motivos, ações de tratamento previstas e prazos para reenquadramento.
Ressalta-se que os níveis de exposição ao risco e sua aderência aos respectivos limites estabelecidos são acompanhados, no mínimo, trimestralmente pela Diretoria.

6. AVALIAÇÃO DE RISCOS E CONTROLES DE PROCESSOS, METODOLOGIAS E FERRAMENTAS

A avaliação dos processos, metodologias e ferramentas relacionados à EGR é realizado por pessoa, setor ou entidade competente que não tenha participado ativamente da definição ou elaboração dos mesmos e que não seja diretamente envolvida em sua execução, incluindo os seguintes componentes:

- Inventário e perfil de risco que descreva cada risco identificado, indique sua categoria, causas e possibilite atribuir responsabilidades em relação à sua gestão.

- Metodologias qualitativas e/ou quantitativas para mensuração de riscos e, quando for o caso, das respectivas fontes de dados.

- Estimação do Nível de Risco, com base nas metodologias estabelecidas, para cada um dos riscos identificados.

- Tratamentos e controles, compatíveis com cada Nível de Risco e com as prioridades estabelecidas pelo Grupo Porto, visando manter as exposições a riscos dentro dos limites definidos em suas políticas e procedimentos, além de mecanismos para avaliação da efetividade de tais medidas.

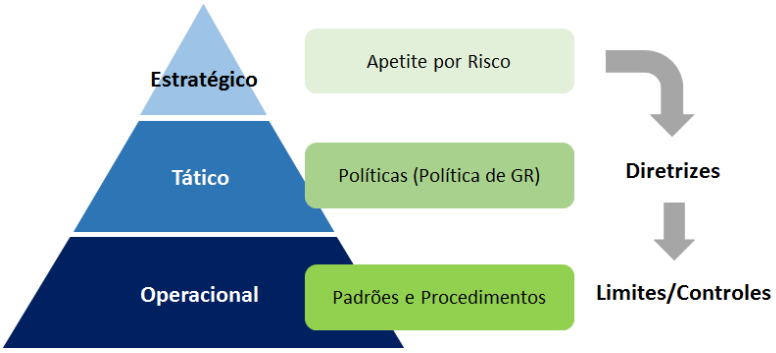
- Indicadores ou variáveis para o monitoramento dos níveis de exposição aos principais riscos.

- Mecanismos de comunicação que viabilizem o desenvolvimento das atividades previstas nos componentes anteriores, possibilitem o efetivo reporte de exposições a riscos e, no caso de eventuais desvios em relação aos limites estabelecidos, permitam a adoção tempestiva das medidas cabíveis.

- Apetite por Risco, com base nas metodologias e cálculos estabelecidos.

7. PROCESSO DE GESTÃO DE RISCOS E ALINHAMENTO AO APETITE POR RISCO

O Apetite por Risco é a diretriz fundamental em termos de gestão de riscos para uma organização, pois todas as políticas e procedimentos que definem como os riscos devem ser gerenciados derivam deste, conforme ilustrado abaixo.



O apetite por risco do Grupo é definido e aprovado pelo Conselho de Administração e refere-se aos perfis e níveis de riscos que a Porto se dispõe a admitir na realização dos seus objetivos, formalizado anualmente na Declaração de Apetite de Risco (RAS).
No Grupo Porto o apetite é avaliado de maneira qualitativa, descrevendo os riscos que são admitidos pelo Grupo, assim como de forma quantitativa, por meio dos valores de perda máximo apurados para cada tipo de risco).

7.1. Capacidade de Tomada de Risco

Um fator-chave na determinação do apetite por risco é a capacidade de tomada de risco de uma empresa. Isso significa a capacidade de absorver as perdas decorrentes de riscos sem uma ameaça imediata à sustentabilidade do Grupo.
A capacidade de tomada de risco é definida pela disponibilidade de patrimônio, enquanto o apetite por risco define o quanto desse patrimônio poderá ser utilizado para cobrir os riscos assumidos. O perfil atual de risco não pode superar o apetite.

8. POLÍTICAS CORRELATAS DE GERENCIAMENTO DE RISCOS

Para auxiliar a estrutura de Gestão de Riscos, foram redigidas diversas políticas e procedimentos, de forma a refletir as diretrizes estabelecidas pela Administração e assegurar que o Grupo Porto possua estrutura de controle compatível com a natureza de suas operações e complexidade dos seus produtos, serviços, processos, sistemas e exposições, permitindo seu adequado gerenciamento.

As políticas descritas abaixo trazem estratégias e diretrizes para os riscos considerados relevantes pelo Grupo, estabelecendo um conjunto de princípios, limites, ações, papéis e responsabilidades necessários à identificação, avaliação, mensuração, tratamento e monitoramento dos riscos aos quais o Grupo Porto Seguro esteja exposto, a fim de garantir a aderência à legislação e às melhores práticas de mercado.

- **Política de Risco de Mercado:** Dispõe sobre as metodologias de mensuração e limites definidos por veículos de investimentos e carteiras. Inclui também critérios para ALM e papéis e responsabilidades associados ao processo de gestão de risco de mercado.

- **Política de Risco de Crédito:** Dispõe sobre as metodologias de mensuração e limites para as carteiras de investimentos e empréstimos, incluindo critérios de seleção de contrapartes, limites máximos de exposição, ativos vedados e acompanhamento de desempenho de modelos de crédito. Abrange também o risco de crédito da contratação de resseguro, incluindo critérios para contratação de ressegurador, limite máximo de exposição por contraparte e contrato.

- **Política de Risco de Liquidez:** Dispõe sobre as metodologias de mensuração e limites para o caixa das empresas, assim como para os ativos financeiros detidos nos fundos e carteiras de investimentos.

- **Política de Risco de Subscrição:** Dispõe sobre as metodologias e processos para mensuração e monitoramento do risco de subscrição, incluindo processo de formação e governança dos prêmios, cálculo e adequação das provisões, limites de retenção e práticas de aceitação e liquidação de sinistros.

- **Política de Gestão de Risco Operacional:** Dispõe sobre as diretrizes e princípios para gestão do risco operacional, incluindo identificação, avaliação e documentação dos riscos identificados e desenvolvimento do banco de dados para armazenamento das perdas operacionais materializadas.

- **Política de Gestão de Continuidade de Negócios:** Dispõe sobre os princípios e diretrizes para definição de processos críticos e planos de continuidade para manutenção de serviços essenciais em cenários de interrupção de sistemas e acessos.

- **Política de Gerenciamento de Capital:** Dispõe sobre os princípios e diretrizes adotados no gerenciamento de capital das empresas do Grupo Porto, incluindo metodologias e limites, de forma a proporcionar uma alocação eficiente e prudente de capital, garantindo os recursos necessários para crescimento dos negócios assim como capacidade de lidar com cenários adversos.

- **Instrução Normativa de Gestão de Mudanças:** Dispõe sobre os procedimentos e responsabilidades adotados no processo de gestão de mudanças do Grupo Porto.

- **Política de Risco Socioambiental e Climático:** Dispõe sobre os princípios, diretrizes, responsabilidades, bem como mecanismos de avaliação e controle adotados pela Porto no que se refere à Gestão dos Riscos Sociais, Ambientais e Climáticos (GRSAC).

- **Política de Risco Cibernético:** Dispõe sobre as diretrizes e requisitos de riscos cibernéticos para compor a proteção dos ativos tecnológicos, processos e pessoas que interagem no ambiente do Grupo Porto Seguro, visando a confidencialidade, integridade e disponibilidade dos dados.

- **Política de Prevenção a Fraudes:** Dispõe sobre as principais diretrizes e orientações para todas as áreas, atividades e negócios das empresas da Porto Seguro realizarem o combate e a prevenção a fraudes, além de estabelecer os papéis e responsabilidades de todos os envolvidos no tema.

- **Política de Risco de Modelo:** Dispõe sobre princípios, diretrizes, metodologias e processos para mensuração e monitoramento do risco de modelos, além de estabelecer os papéis e responsabilidades de todos os envolvidos no tema.

- **Política de Risco de Terceiros:** Dispõe sobre diretrizes e procedimentos para a seleção, avaliação e monitoramento de parceiros externos, como fornecedores e colaboradores terceirizados, além de estabelecer os papéis e responsabilidades de todos os envolvidos no tema.

9. TAXONOMIA DE RISCOS

A Porto, diante da complexidade e variedade de produtos e serviços oferecidos aos seus clientes em todos os segmentos de mercado, está exposta a diversos tipos de riscos, sejam eles decorrentes de fatores internos ou externos.

Com o objetivo de consolidar os eventos que podem afetar o Grupo Porto, foi adotada a seguinte taxonomia de riscos, considerados como prioritários na gestão de riscos:

9.1. Risco de Subscrição

A Porto define o risco de subscrição como sendo o risco de ocorrência de eventos que contrariem as suas expectativas e que possam comprometer significativamente o resultado das operações e o seu patrimônio decorrente de uma possível insuficiência dos prêmios e/ou provisões para fazer frente aos dispêndios financeiros com o pagamento das obrigações assumidas com os segurados.

9.2. Risco de Crédito

O risco de crédito é definido como a possibilidade de ocorrência de perdas associadas ao não cumprimento pelo tomador ou contraparte de suas respectivas obrigações financeiras nos termos pactuados e/ou desembolsos para honrar avais, fianças, coobrigações, compromissos de crédito e outras operações de natureza semelhante, devido à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas na renegociação e aos custos de recuperação.

9.3. Risco de Mercado

Risco de mercado é o risco de perdas resultantes da flutuação nos valores de mercado de posições detidas por uma instituição financeira, bem como de sua margem financeira, incluindo os riscos das operações sujeitas à variação cambial, das taxas de juros, dos preços de ações e dos preços de mercadorias (commodities).

Também abrange o risco de mercado o risco de descasamento entre ativos e passivos (ALM) de seguro.

9.4. Risco de Liquidez

Representado como:

i. A possibilidade de a instituição não ser capaz de honrar eficientemente suas obrigações financeiras esperadas e inesperadas, correntes e futuras, inclusive as decorrentes de vinculação de garantias, sem afetar suas operações diárias e sem incorrer em perdas significativas; e

ii. A possibilidade de a instituição não conseguir negociar a preço de mercado uma posição, devido ao seu tamanho elevado em relação ao volume normalmente transacionado ou em razão de alguma descontinuidade no mercado.

9.5. Risco Operacional

O risco operacional é conceituado como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas ou decorrente de fraudes ou eventos externos, incluindo-se o risco legal e excluindo-se os riscos decorrentes de decisões estratégicas e à reputação da instituição.

Contempla atividades relacionadas à Continuidade de Negócios, com o objetivo de definição de um plano de trabalho para que, em caso de interrupção, as atividades possam ser retomadas em condições pré-definidas de prazo, nível de atendimento e local de trabalho, com impacto mínimo para nossos clientes.

9.6. Risco de Modelo

O risco de modelo é definido como a possibilidade de perdas financeiras, perdas de oportunidades ou negócios insatisfatórios como consequências de decisões embasadas em resultados, relatórios ou uso inadequado de modelos, possíveis erros no desenvolvimento ou implementação.

9.7. Risco de Capital

Representado pela falta de capacidade do Grupo em cumprir suas obrigações correntes e futuras, frente aos riscos assumidos, com recursos que constituem seu patrimônio. Também está englobado nesse risco requisitos regulatórios de solvência.

9.8. Risco Socioambiental e Climático

O risco socioambiental e climático na Porto é definido como:

(i) a possibilidade de perdas devido à violação de direitos e garantias fundamentais, incluindo direitos humanos;
(ii) possibilidade de perdas devido a ocorrência de eventos associados à degradação do meio ambiente;
(iii) possibilidade de perdas devido ocorrência de eventos associados à intempéries frequentes e severas, processo de transição para economia de baixo carbono ou devido à sinistros ocorridos em seguros de responsabilidade dado falha na gestão de risco climático.

9.9. Risco Cibernético

O risco cibernético na Porto é definido como o risco de perda financeira, interrupção da comunicação ou dano à reputação do Grupo decorrente da exposição dos processos, pessoas e tecnologias a ameaças digitais.

9.10. Risco de Terceiros

O risco cibernético na Porto é definido como o risco proveniente de fatores externos, tendo origem na relação da Porto com fornecedores, prestadores de serviços e parceiros de negócios.

9.11. Demais Riscos

Adicionalmente, o grupo possui subcategorias de risco tais como: risco reputacional/imagem, e risco regulatório ou de conformidade.

10. PAPÉIS E RESPONSABILIDADES

10.1. Conselho de Administração

- Zelar pela perenidade da Companhia, dentro de uma perspectiva de longo prazo e de sustentabilidade, que incorpore considerações de ordem econômica, social, ambiental e de boa governança corporativa, na definição dos negócios e operações.

- Zelar pela adequação da EGR e do Sistema de Controles Internos (SCI), incluindo a disseminação das culturas de risco e de controle e o alinhamento das operações à política de conformidade, ao apetite por risco e à política de gestão de riscos, bem como a melhoria contínua dos processos e procedimentos relacionados.

- Possuir um entendimento geral do perfil de risco da supervisionada e compreender, para os principais riscos a que ela esteja exposta: sua natureza e potenciais impactos sobre o negócio; o atual nível de exposição e as ações adotadas para sua gestão.

- Prover as diversas unidades organizacionais com a estrutura organizacional e os recursos materiais e humanos necessários à adequada gestão dos riscos e operacionalização dos controles associados a suas respectivas atividades, incluindo pessoal experiente, capacitado e em quantidade suficiente.

- Garantir que os mecanismos de avaliação de desempenho e a estrutura remuneratória adotados pela supervisionada não incentivem comportamentos capazes de comprometer a efetividade do SCI e da EGR.

- Formular diretrizes para a gestão da Companhia e de suas controladas, que serão refletidas no orçamento anual.

- Aprovar a Política Corporativa de Gestão de Riscos.

- Analisar e aprovar o Apetite por Risco e revisá-lo sempre que ocorrer a atualização do plano de negócios.

10.2. Diretoria Executiva

- Avaliar anualmente ou sempre que houver mudança significativa no perfil de risco, a eficácia da EGR e do SCI, informando ao Conselho de Administração os resultados dessas análises e, caso necessário, as respectivas propostas de ação, bem como a adoção, o cumprimento e a manutenção dos processos destinados ao saneamento das deficiências identificadas.

- Orientar, supervisionar e garantir a elaboração, implementação e operacionalização dos processos e procedimentos relativos aos controles internos e gestão de riscos associados às atividades sob sua responsabilidade.

- Zelar pela adequação da EGR e do SCI, bem como a melhoria contínua dos processos e procedimentos a ela relacionados.

- Acompanhar de forma periódica as informações de risco às quais o Grupo esteja exposto.

- Monitorar periodicamente as exposições a risco, assim como os planos de ação ou medidas corretivas, caso necessário.

- Atestar a análise realizada para gestão de mudanças ou, atestar a justificativa do porquê seu impacto não foi considerado significativo no perfil de risco.

- Aprovar os parâmetros e limites de exposição para as atividades de negócio que impliquem em assunção de riscos relevantes.

10.3. Gestores das Unidades Operacionais e de Negócios (Primeira Linha)

- Conhecer o respectivo ambiente de riscos e controles, o que inclui o entendimento e aplicação dos controles necessários às atividades sob responsabilidade de suas áreas, assim como o entendimento e monitoramento dos respectivos riscos a que está exposto.

- Estabelecer políticas e diretrizes que conduzam à implantação e manutenção de um sistema de gestão de riscos e de controles efetivo na instituição;

- Avaliar o arcabouço legal e garantir que políticas, Instruções Normativas e manuais de procedimentos aplicáveis à área estejam aderentes, acessíveis e atualizadas;

- Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação, gerenciamento e reporte dos riscos, assim como perdas decorrentes de suas áreas e a efetividade dos controles internos inerentes.

- Avaliar os resultados da execução dos testes de controles e estabelecer o encaminhamento de ações voltadas à redução/eliminação de não conformidades.

- Auxiliar a área de Gestão de Riscos Corporativos no desenvolvimento e acompanhamento de limites de riscos, provendo acesso às informações necessárias para realização das análises;

- Em situações de desenquadramento dos limites de risco estabelecidos, justificar os motivos, ações de tratamento previstas e prazos para reenquadramento;

- Gerir e monitorar os serviços terceirizados para o funcionamento das atividades da Instituição sob sua responsabilidade, assim como conhecer os riscos a que estão expostos e seus controles. Para casos de terceiros relevantes, deve garantir o atendimento aos requerimentos internos e regulatórios.

- Apoiar a constituição de grupos de trabalhos, voltados ao diagnóstico das causas de perdas e à identificação de medidas saneadoras, avaliando e validando os resultados das análises realizadas.

- Acionar o gestor de riscos para na avaliação de mudanças que tenham potencial para alterar significativamente o perfil de risco do Grupo Porto Seguro (exemplo: implementação de novos sistemas, entre outros);

- Reportar à área de Gestão de Riscos Corporativos e de Controles Internos os resultados do RCSA (Questionário de Auto avaliação de riscos e controles), dos testes de controles, do andamento dos planos de ação, as deficiências e incidentes relevantes e não conformidades com políticas, normas e regulamentos aplicáveis.

- Auxiliar a área de Gestão de Riscos Cibernéticos na aplicação do questionário para análise de impacto nos negócios (BIA), treinamentos, testes e manutenção do Plano de Continuidade dos Negócios (PCN).

- Disseminar a cultura de gestão de riscos e contribuir ativamente para a conscientização da área;

- Orientar os colaboradores a efetuar tempestivamente a atualização da declaração de vínculos na Portonet/RH Online;

- Orientar os colaboradores a efetuar os treinamentos obrigatórios disponíveis na Portonet/Ensino a distância.

10.4. Comitê de Risco Integrado (CRI)

- Revisar e validar anualmente a Política Corporativa de Gestão de Riscos;

- Zelar pelo cumprimento das políticas e efetividade do processo de gerenciamento de riscos;

- Prover recomendações relacionadas ao apetite e limites de exposição por tipos de riscos, assim como às políticas de risco;

- Monitorar o perfil e apetite de risco da Companhia e supervisionar a observância de seus termos;

- Analisar e pontuar fatores de riscos internos e externos que podem impactar os negócios do Grupo Porto;

- Analisar os casos que lhe forem submetidos e sugerir à Diretoria as melhores soluções face às circunstâncias, riscos e custos envolvidos;

- Revisar anualmente o relatório sobre a eficácia das políticas e dos sistemas de gerenciamento de riscos e de controles internos da Companhia.

10.5. Gerência de Gestão de Riscos Corporativos

- Desenvolver e manter esta Política com diretrizes, conceitos e metodologias atualizadas para gerenciamento dos riscos, alinhadas com os requerimentos regulatórios, diretrizes da Companhia e melhores práticas;

- Coordenar a elaboração e as revisões do inventário de riscos, participando, juntamente com as diversas unidades organizacionais, da identificação, avaliação e mensuração de riscos.

- Monitorar periodicamente o inventário e as exposições a risco, assegurando o alinhamento ao apetite por risco e limites operacionais estabelecidos, avaliando mudanças internas, externas ou operacionais que possam impactar o perfil de risco da empresa, incluindo novos riscos emergentes, e reportar os resultados dessas análises às Diretorias, Comitê de Risco Integrado (CRI), Comitê de Auditoria e Conselho de Administração, conforme necessário.

- Auxiliar as diversas unidades operacionais e de negócios na identificação/avaliação de seus riscos atuais e emergentes, sejam eles oriundos de fonte interna ou externa, ocasionados pelas operações da própria supervisionada ou por outras empresas do grupo, e consolidar os resultados de forma a garantir sua consistência.

- Identificar os processos de trabalho associados aos principais riscos identificados e avaliá-los periodicamente quanto a efetividade das metodologias, ferramentas e controles utilizados para gestão dos riscos, bem como a suficiência e adequação dos recursos humanos e materiais envolvidos nesta atividade nas diversas áreas supervisionadas (1ª linha).

- Orientar quanto a estratégias e alternativas para gestão de riscos, na medida que isso não comprometa sua independência.

- Atuar junto às áreas gestoras em situações de risco ou desenquadramento de limites, obtendo justificativas e planos de ação, e acompanhar a implementação de medidas corretivas para sanar deficiências da EGR.

- Apoiar na análise de mudanças, de forma a auxiliar os gestores da primeira linha na avaliação de seus riscos e potenciais implicações;

- Orientar as unidades operacionais, de negócios (1ª Linha) e a Diretoria sobre gestão de riscos e reporte de perdas operacionais, além de encaminhá-las ao regulador, e promover a disseminação da cultura de riscos entre os colaboradores, reforçando comportamentos que favoreçam sua gestão.

- Em conjunto com as unidades de operacionais e de negócios, elaborar textos/reportes periódicos referentes a informações de risco a serem divulgadas ao mercado, submetendo-os à validação e aprovação das alçadas competentes.

10.6. Controles Internos

- Fornecer metodologia, ferramenta e procedimentos de controles internos, conforme Política de Controles Internos;

- Avaliar e testar controles relevantes que impactam as demonstrações financeiras, as obrigações regulatórias, a conformidade com os padrões éticos e de conduta;

- Elaborar relatórios com as análises de ambientes de controle das estruturas do Grupo Porto, tanto para finalidades internas quanto para atendimento das regulamentações vigentes.

10.7. Auditoria Interna

- Avaliar a adequação da EGR e do SCI, dentro de um ciclo máximo de três anos.
- Zelar pela conformidade das políticas, normas, padrões, procedimentos e regulamentações internas e externas.
- Recomendar aprimoramentos no ambiente de controles internos.

11. VIGÊNCIA

Esta Política entrará em vigor na data de sua publicação e será revisada periodicamente, sendo passível de alteração ou atualização sempre que constatada sua necessidade.

12. APROVAÇÃO

Esta Política foi revisada pelo Comitê de Risco Integrado, aprovada pelo Conselho de Administração e será divulgada ao mercado nos termos da regulamentação aplicável.

Dezembro/2024

13. ANEXO I - REGIMENTO INTERNO DO COMITÊ DE RISCO INTEGRADO

CAPÍTULO I – OBJETIVO E ATRIBUIÇÕES

Artigo 1º. Este Regimento Interno ("Regimento") disciplina o funcionamento do Comitê de Risco Integrado ("Comitê") da Porto Seguro Companhia De Seguros Gerais ("Companhia"), líder do grupo prudencial de empresas supervisionadas pela Superintendência De Seguros Privados – Susep do grupo Porto Seguro, formado pela Companhia, pela Porto Seguro Vida e Previdência S.A., Azul Companhia de Seguros Gerais, Itaú Seguros de Auto e Residência S.A. e pela Porto Seguro Capitalização S.A ("Conglomerado").

Parágrafo Único. O Comitê será único para todas as instituições autorizadas a funcionar pela Superintendência De Seguros Privados – Susep que integram o Conglomerado.

Artigo 2º. O Comitê é órgão de caráter consultivo e permanente, vinculado diretamente à Diretoria da Companhia ("Diretoria").

Artigo 3º. O Comitê tem como objetivo auxiliar a Diretoria da Companhia no desempenho de suas atribuições relativas à gestão de riscos, incluindo fornecer subsídios e informações em assuntos relacionados à gestão de riscos, propondo planos de ação e diretrizes, avaliando o cumprimento das normas de gestão de riscos, políticas internas e principais indicadores associados, em todas as sociedades que compõem o Conglomerado.

Artigo 4º. São atribuições do Comitê:

I. avaliar, periodicamente, a efetividade da Estrutura de Gestão de Riscos ("EGR"), em especial quanto:

a) a observância do Apetite por Risco e da Política de Gestão de Riscos;
b) o desempenho do Diretor responsável pelos controles internos;
c) o desempenho da unidade de gestão de riscos; e
d) a efetividade de ações adotadas para o saneamento de deficiências;

II. avaliar, sob o enfoque de riscos, o plano de negócio da Companhia e das empresas que compõem o Conglomerado e, auxiliar na definição do correspondente apetite por risco;

III. auxiliar nos processos de tomada de decisões estratégicas relacionadas à gestão de riscos;

IV. revisar a Política de Gestão de Riscos, formulando e avaliando propostas de alterações;

V. analisar os casos que lhe forem submetidos e sugerir à Diretoria as melhores soluções face às circunstâncias, riscos e custos envolvidos; e

VI. revisar os relatórios sobre a eficácia das políticas e dos sistemas de gerenciamento de riscos e de controles internos.

Parágrafo Único. O Comitê se reportará diretamente à Diretoria da Companhia e das empresas do Conglomerado mediante a submissão, preferencialmente, por correio eletrônico, das atas contendo as deliberações do Comitê, podendo, ainda, se reunir com a Diretoria sempre que necessário a critério dos membros.

CAPÍTULO II – ORGANIZAÇÃO

COMPOSIÇÃO, INVESTIDURA, MANDATO E QUALIFICAÇÃO

Artigo 5º. O Comitê será composto por no mínimo 3 (três) e, no máximo, 5 (cinco) membros, eleitos pela Diretoria, dos quais:

I. Nenhum dos membros poderá ser ou ter sido, nos 12 (doze) meses anteriores à sua eleição, diretor responsável pelos controles internos da Companhia ou de qualquer empresa que compõe o conglomerado;

II. A maioria dos membros deverá atender, concomitantemente, aos seguintes requisitos:

II.i. Não ser e não ter sido, nos 3 (três) anos anteriores à sua eleição:

a) colaborador da Companhia ou de suas controladoras, controladas ou subsidiárias, ou de qualquer empresa que compõe o Conglomerado, exceto na condição exclusiva de membro do Conselho de Administração, se aplicável, ou de Comitês do órgão de administração máximo da Companhia;

b) não ser acionista da Companhia, de suas controladoras, controladas ou subsidiárias ou de qualquer empresa que compõe o Conglomerado, com participação igual ou superior a 5% (cinco por cento) do total de ações, por empresa;

c) não ser membro do grupo de controle da Companhia, de suas controladoras, controladas, subsidiárias ou de qualquer empresa que compõe o Conglomerado;

d) não ser cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de pessoas que não atendam ao disposto “a”, “b” e “c”, supra, exceto em relação aos colaboradores mencionados no item “a” que não possuam cargos de gestão;

e) não ser vinculado a acordos de acionistas da Companhia ou de qualquer empresa que compõe o Conglomerado;

f) não receber qualquer tipo de remuneração da Companhia, de suas controladoras, controladas, subsidiárias ou de qualquer empresa que compõe o Conglomerado, que não seja relativa à participação acionária, ou, quando aplicável, à função de membro do Conselho de Administração e de seus Comitês;

g) não possuir qualquer outro tipo de vínculo com pessoas ou instituições que possa, a critério da Superintendência De Seguros Privados – SUSEP, influenciar de forma significativa seus julgamentos, opiniões e decisões; e

h) possuir comprovada experiência em gestão de riscos.

Parágrafo 1º. O prazo máximo de mandato ou de mandatos consecutivos dos membros do Comitê será de até 5 (cinco) anos, permitida a reeleição, com intervalo mínimo de 3 (três) anos para reintegração.

Parágrafo 2º. A função de membro do Comitê é indelegável.

Parágrafo 3º. A Diretoria da Companhia poderá eleger ou destituir membros do Comitê a qualquer tempo.

Parágrafo 4º. Os membros do Comitê serão remunerados de acordo com as políticas de remuneração da Companhia.

COORDENAÇÃO DO COMITÊ

Artigo 6º. A Diretoria indicará, dentre os membros do Comitê que atendam aos requisitos previstos na legislação e regulamentação em vigor, um Coordenador, a quem caberá a representação, organização e coordenação das atividades do Comitê.

O Coordenador do Comitê é responsável por:

a) assegurar a eficácia e o bom desempenho das atividades do Comitê;

b) convocar, instalar e presidir as reuniões do Comitê, nomear o Secretário da Mesa, responsável pela elaboração da ata da reunião;

c) estabelecer pautas de discussão, organizar as reuniões e garantir que a agenda seja cumprida; e

d) representar o Comitê junto a Diretoria e áreas internas da Companhia e do Conglomerado, quando solicitado, ou designar um membro que o represente.

REUNIÕES DO COMITÊ

Artigo 7º. O Comitê reunir-se-á ordinariamente a cada 3 (três) meses e, extraordinariamente, sempre que necessário, na sede da Companhia ou em qualquer outra localidade escolhida. As reuniões poderão ser

realizadas por conferência telefônica ou videoconferência, correio eletrônico ou por qualquer outro meio de comunicação que permita a identificação dos membros do Comitê e a comunicação simultânea entre todas as demais pessoas presentes à reunião.

Artigo 8º. As reuniões serão convocadas pelo Coordenador do Comitê, por carta, correio eletrônico, ou por qualquer outra forma escrita, enviada com pelo menos 48 (quarenta e oito) horas de antecedência, devendo constar o dia e o horário da reunião, bem como a ordem do dia e documentação de suporte. A convocação será dispensada sempre que estiver presente à reunião a totalidade dos membros em exercício do Comitê.

Artigo 9º. As reuniões do Comitê poderão ser instaladas quando presentes, no mínimo, a maioria de seus membros, sendo considerado como presente aquele que estiver, na ocasião, representado por um membro do Comitê, ou que tiver enviado, até o momento da instalação da reunião, seu voto por correio eletrônico ou qualquer outra forma escrita, ou, ainda, que participe da reunião por conferência telefônica ou videoconferência ou por qualquer outro meio de comunicação que permita a sua identificação e a comunicação simultânea com todas as demais pessoas presentes à reunião.

Artigo 10. Poderão participar das reuniões do Comitê, a convite do Coordenador, membros da administração, colaboradores internos e externos que possam, na avaliação do Coordenador ou de qualquer outro membro do Comitê, deter informação relevante ou contribuir para a discussão dos assuntos constantes da agenda da reunião.

Artigo 11. Será lavrada ata de cada uma das reuniões do Comitê, aprovada e assinada por todos os presentes e arquivada na sede da Companhia.

AUSÊNCIA, IMPEDIMENTO TEMPORÁRIO E VACÂNCIA

Artigo 12. Na ausência ou impedimento temporário do Coordenador do Comitê, suas funções serão exercidas interinamente por um membro por ele indicado, escolhido dentre aqueles que preenchem os requisitos legais para exercício do cargo.

Artigo 13. No caso de impedimento temporário de qualquer membro do Comitê, o membro impedido temporariamente indicará, dentre os membros do Comitê, aquele que o representará interinamente.

Artigo 14. No caso de vacância de membro do Comitê, em decorrência de destituição, renúncia, morte, impedimento comprovado, invalidez ou perda do mandato ou outras hipóteses previstas em lei, a Diretoria deverá promover a indicação de novo membro do Comitê caso se verifique que o referido órgão tenha menos de 3 (três) membros.

CONFLITOS DE INTERESSE

Artigo 15. Os membros do Comitê deverão atuar de forma isenta, sendo que, para prevenir casos de conflito de interesses aplicar-se-ão as regras abaixo:

a) Cabe a cada membro informar ao Coordenador do Comitê seu eventual conflito de interesse tão logo o assunto seja incluído na ordem do dia ou proposto pelo Coordenador do Comitê e, de qualquer forma, antes do início de qualquer discussão sobre cada tema;
b) Se o próprio membro o não se manifestar, qualquer dos presentes à reunião que tenha conhecimento do fato, deverá informá-lo ao Coordenador do Comitê;
c) Tão logo identificado o conflito de interesses, o membro do Comitê não poderá ter acesso a informações, bem como exercer voto sobre aquele determinado assunto, nem participar das discussões; e
d) Na primeira reunião que seguir o ato de sua eleição, o membro eleito deverá informar aos membros do Comitê: (a) as principais atividades que desenvolva externas à Companhia; (b) a participação em conselhos ou comitês de outras empresas, concorrentes ou não; e (c) o relacionamento comercial com a Companhia ou com empresas do Conglomerado, inclusive se prestam serviços a essas empresas, sendo que tais informações devem ser prestadas sempre que houver um novo evento que enseje a atualização desse tipo de informação.

CAPÍTULO III - DISPOSIÇÕES GERAIS

Artigo 16. Os membros do Comitê, além de observar os deveres legais inerentes ao cargo, devem pautar sua conduta por elevados padrões de ética, cumprimento das políticas da Companhia a eles aplicáveis, bem como observar e estimular as boas práticas de governança corporativa, devendo guardar rigoroso sigilo sobre qualquer informação relevante, relacionada à Companhia, se enquanto ela não for oficialmente divulgada ao mercado.

Artigo 17. As omissões deste Regimento Interno, serão resolvidas pelo Coordenador, *ad referendum* da maioria dos membros do Comitê.

Artigo 18. Este Regimento somente poderá ser alterado pela Diretoria da Companhia.

Este Regimento entra em vigor na data do início de funcionamento do Comitê e será, também, arquivado na sede da Companhia.