



PORTO SEGURO S.A.
CNPJ/MF nº 02.149.205/0001-69
NIRE 35.3.0015166.6
Companhia Aberta – CVM nº 01665-9
Código ISIN nº BRPSSAACNOR7

POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS

ÍNDICE

1. OBJETIVO	3
2. ABRANGÊNCIA.....	3
3. REFERÊNCIA NORMATIVA	3
4. ESTRUTURA DE GESTÃO DE RISCOS	3
4.1. Definições	3
4.2. Missão	4
4.3. Objetivos e Estratégia.....	4
4.4. Modelo de 3 linhas de defesa.....	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	8
5.4. Monitoramento e Reporte de Riscos	8

6.	AVALIAÇÃO DE RISCOS E CONTROLES DE PROCESSOS, METODOLOGIAS E FERRAMENTAS ..	9
7.	PROCESSO DE GESTÃO DE RISCOS E ALINHAMENTO AO APETITE POR RISCO	9
7.1.	Capacidade de Tomada de Risco	10
8.	POLÍTICAS CORRELATAS DE GERENCIAMENTO DE RISCOS	10
9.	TAXONOMIA DE RISCOS.....	11
9.1.	Risco de Subscrição	11
9.2.	Risco de Crédito	12
9.3.	Risco de Mercado	12
9.4.	Risco de Liquidez	12
9.5.	Risco Operacional	12
9.6.	Risco de Capital.....	12
9.7.	Risco Cibernético	12
9.8.	Demais Riscos	13
10.	PAPÉIS E RESPONSABILIDADES	13
10.1.	Conselho de Administração	13
10.2.	Diretoria Executiva	13
10.3.	Gestores das Unidades Operacionais e de Negócios (Primeira Linha de Defesa)	14
10.4.	Comitê de Risco Integrado (CRI)	15
10.5.	Estrutura de Gestão de Riscos e Conformidade	15
10.6.	Controles Internos.....	16
10.7.	Auditoria Interna.....	17
11.	VIGÊNCIA	17
12.	APROVAÇÃO	17

1. OBJETIVO

Esta Política Corporativa de Gestão de Riscos da Porto Seguro (“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 Seguro”).

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 Seguro (“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 517/2015;
- Manual de Orientação EGR – Orientações da SUSEP ao Mercado;
- Resolução CMN nº 4.557/2017;
- Resolução Normativa ANS nº 443/2019;
- Resolução CMN nº 4.893/2021;
- Circular Susep nº 638/2021;
- 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 estabelecido, para maximizar as oportunidades e minimizar os efeitos adversos.

4.2. Missão

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

- (i) assegurar que o apetite por riscos do Grupo Porto Seguro esteja alinhado com sua capacidade e ao plano de negócios;
- (ii) reduzir a ocorrência de eventos inesperados e prejuízos 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 Seguro;
- (iv) integrar a gestão de riscos à estratégia do Grupo Porto Seguro e nos processos de tomada de decisão;
- (v) preservar a solvência do Grupo Porto Seguro, ao definir limites para que os riscos não superem o apetite por risco estabelecido;
- (vi) proteger a marca e a reputação do Grupo Porto Seguro, fomentando valores fundamentais do Grupo Porto Seguro;
- (vii) promover uma 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 Seguro, 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 Seguro 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 de defesa

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



Primeira linha de defesa (Unidades Operacionais) – As diversas unidades operacionais e de negócios que lidam diretamente com os negócios e com a exposição aos riscos do Grupo Porto Seguro. 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 de defesa (Funções de Controle) – As funções de controle têm como responsabilidade orientar e supervisionar se os processos e controles definidos pela primeira linha de defesa 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 de defesa (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 de defesa).

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 Seguro 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 Seguro 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 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 Seguro. 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 tipos de riscos.

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.

Adicionalmente ao CRI há o Comitê de Auditoria, o qual possui como objetivo principal fornecer suporte à Administração do Grupo Porto Seguro 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 Seguro 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 Seguro, 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 de defesa).
- **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 a de 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, por meio de modelos matemáticos não triviais.

No Grupo Porto Seguro, 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, independente da metodologia utilizada na mensuração dos riscos, é necessário que as mesmas sejam documentadas pelas unidades operacionais e 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 Seguro 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:** é o que 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. 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 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.

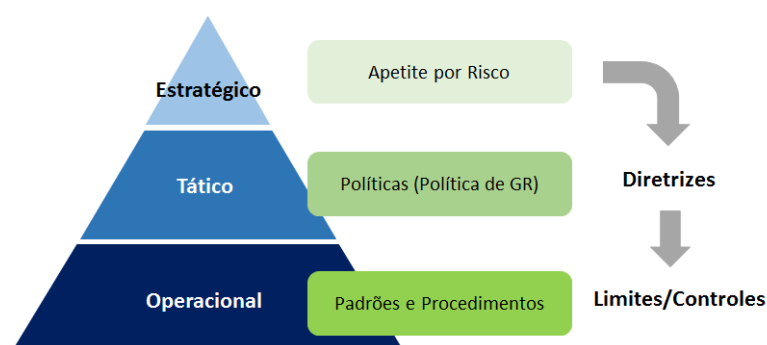
6. AVALIAÇÃO DE RISCOS E CONTROLES DE PROCESSOS, METODOLOGIAS E FERRAMENTAS

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 e suas 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 Seguro, 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 derivaram 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 Seguro se dispõe a admitir na realização dos seus objetivos, formalizado na Declaração de Apetite de Risco (RAS)

No Grupo Porto Seguro o apetite é avaliado de maneira qualitativa (descrevendo os riscos que são admitidos pelo Grupo) e quantitativa (valores 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 Seguro 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, realização de testes de controles 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 Seguro, 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 Seguro.
- **Política de Responsabilidade Socioambiental:** Dispõe sobre os princípios, diretrizes, responsabilidades assim como mecanismos adotados pelo Grupo Porto Seguro no que se refere às práticas para gestão da responsabilidade social e ambiental.
- **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.

9. TAXONOMIA DE RISCOS

A Porto Seguro, 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 Seguro, foi adotada a seguinte taxonomia de riscos, considerados como prioritários na gestão de riscos:

9.1. Risco de Subscrição

A Porto Seguro 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 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.

9.7. Risco Cibernético

O Risco Cibernético na Porto Seguro 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.

9.8. Demais Riscos

Adicionalmente, o grupo possui subcategorias de risco tais como: risco de modelo, risco socioambiental, risco reputacional/imagem, risco de terceiros 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 aos 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 de Defesa)

- 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 à diagnose 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 da Corporação Porto Seguro.
- 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. Estrutura de Gestão de Riscos e Conformidade

- 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 o inventário e o perfil de risco e os níveis de exposição, assim como seu alinhamento ao Apetite por Risco.
- 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 de defesa).
- Reportar, periodicamente e sempre que necessário, os resultados dos monitoramentos e análises de risco a Diretorias, Comitê de Risco Integrado (CRI), Comitê de Auditoria e Conselho de Administração.

- Monitorar periodicamente as exposições a risco, verificando seu alinhamento com os limites estabelecidos, bem como alterações nos ambientes interno e externo, incluindo mudanças significativas na estrutura ou nas operações da supervisionada e riscos novos ou emergentes que possam alterar significativamente o perfil de riscos das empresas.
- Orientar quanto a estratégias e alternativas para gestão de riscos, na medida que isso não comprometa sua independência.
- Participar da análise de mudanças, de forma a auxiliar na avaliação de seus riscos e potenciais implicações/necessidade de alteração na EGR.
- Atuar junto as áreas gestoras em situações de riscos e/ou desenquadramento dos limites, de forma a obter as justificativas e planos de ação necessários.
- Acompanhar a implementação de planos de ação ou medidas corretivas que visem a sanar deficiências da EGR;
- Orientar as unidades operacionais e de negócios (1ª Linha de Defesa) e Diretoria da Companhia em relação à gestão de riscos e ao reporte de perdas operacionais, assim como executar a sua avaliação e o seu encaminhamento ao regulador.
- 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.
- Promover ações de disseminação da cultura de riscos entre os colaboradores em relação aos riscos de suas operações, com o objetivo de reforçar comportamentos e atitudes que favoreçam a gestão dos mesmos.
- 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.
- Avaliar a aderência da instituição ao arcabouço legal e demais regulamentos aplicáveis às empresas do grupo Porto Seguro.
- Auxiliar as áreas de negócios no atendimento às demandas dos reguladores externos.
- Monitorar a adesão dos colaboradores aos treinamentos obrigatórios relacionados à Governança Corporativa e de Conformidade.

10.6. Controles Internos

- Realizar teste dos controles identificados, a fim de confirmar o entendimento da estrutura dos controles que mitigam os pontos de risco.
- Obter e armazenar evidência dos testes dos controles avaliados, de acordo com os critérios de amostragem e periodicidade definida.

- Para os controles avaliados por meio do questionário de auto avaliação de controles, avaliar as respostas fornecidas pelo gestor e as evidências de controles fornecidas, e tratar quaisquer dúvidas ou inconsistências verificadas.
- Reportar às alçadas competentes os riscos identificados que apresentem fragilidade ou inexistência de controle, para os quais deverão apresentar planos de ação para mitigação.
- Acompanhar/ realizar follow-up dos planos de ação com foco na adequação dos controles internos (desenho ou efetividade dos controles), incluindo pontos de auditoria interna, auditoria externa, fiscalizações e demais demandas para adequação das estruturas.
- Elaborar os relatórios que permitam a identificação e a correção tempestiva das deficiências dos controles.

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.

Setembro/2022