



Política de Gestão de Riscos Corporativos

Elaborada por:	Área de Integridade Opy
Aprovada por:	Conselho de Administração Opy
Data da 1ª aprovação:	12/2025
Vigência:	Por tempo indeterminado
Versão:	1.0

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

1. INTRODUÇÃO

A Opy Healthcare Gestão de Ativos e Investimentos S.A. (“Opy” ou “Companhia”) e suas subsidiárias (denominadas em conjunto com a Companhia como “Empresas Opy”) consideram essencial a gestão dos Riscos Corporativos, isto é, aqueles que na visão do acionista colocam em risco o retorno do investimento e a perenidade da organização, bem como aqueles que impedem a implementação do planejamento estratégico na visão da administração.

O compromisso com uma gestão eficiente dos riscos corporativos é um dos alicerces do crescimento sustentável e do alcance dos objetivos estratégicos da Companhia. Este compromisso é um valor que deve ser praticado por todos os que trabalham na Opy ou que atuem em seu nome, incluindo seus fornecedores.

Assim, a Opy estabelece os objetivos e diretrizes a seguir.

2. OBJETIVO

O objetivo da Política de Gestão de Riscos Corporativos (“Política”) é estabelecer normas e orientações para identificar, avaliar, tratar e reportar riscos conforme definição da seção “1. Introdução”. Este documento tem como principal referência metodológica o *framework* “*Enterprise Risk Management*” publicado pelo *Committee of Sponsoring Organizations* (“COSO”) em 2017.

3. ABRANGÊNCIA

A Política aplica-se a todos os colaboradores, conselheiros, membros de comitês, diretores e colaboradores da Opy e suas subsidiárias (denominadas “Empresas Opy”).

4. GLOSSÁRIO

As definições dos termos aqui utilizados estão no Glossário em anexo a esta Política. Caso haja qualquer dúvida sobre os termos utilizados ou sobre o conteúdo desta Política, entre em contato com a Área de Integridade, responsável pela Gestão de Riscos Corporativos, através do e-mail integridade@opyhealth.com.br.

5. DIRETRIZES

A Gestão de Riscos Corporativos é um processo cíclico e contínuo da Companhia, utilizado para identificar, avaliar, tratar e reportar este tipo de risco.

Tal processo visa assegurar que os responsáveis pela tomada de decisão tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a Companhia,



Política de Gestão de Riscos Corporativos

Elaborada por:	Área de Integridade Opy
Aprovada por:	Conselho de Administração Opy
Data da 1ª aprovação:	12/2025
Vigência:	Por tempo indeterminado
Versão:	1.0

aumentando a probabilidade de alcance dos seus objetivos e reduzindo os riscos a níveis aceitáveis. Deve estar, portanto, alinhado com a missão e com os objetivos estratégicos da Opy.

Os diversos departamentos de negócio, sejam corporativos ou de cada Empresa Opy, são os responsáveis por implementar e operar políticas, processos e controles adequados ao gerenciamento de risco de suas operações de maneira a cumprir o disposto nesta Política e o estabelecido na Declaração de Apetite a Risco.

A Área de Integridade deve apoiar as demais áreas no processo de identificação, avaliação e tratamento dos Riscos Corporativos. Além disso, deve realizar o reporte consolidado de tais riscos para os Órgãos de Governança, seja o Conselho de Administração, o Comitê de Auditoria, Riscos, Regulatório ou qualquer outro, garantindo a padronização e transparência das informações.

O apetite a risco da Opy é definido pelo Conselho de Administração tanto de forma quantitativa quanto qualitativa, e está estabelecido em sua Declaração de Apetite por Riscos.

6. RESPONSABILIDADES

6.1. Conselho de Administração

- Deliberar sobre as diretrizes gerais para Gestão de Riscos da Companhia, bem como avaliar periodicamente os indicadores da exposição a riscos e a eficácia dos sistemas de gerenciamento de riscos.
- Aprovar a presente Política e suas alterações.
- Aprovar os níveis de apetite a risco da Opy e as suas respectivas declarações.
- Monitorar e aprovar a revisão dos Mapas de Riscos Corporativos.
- Aprovar as respostas aos Riscos Corporativos.

Para desempenho das suas funções, o Conselho de Administração contará com o suporte do Comitê de Auditoria, Riscos, Regulatório, sem prejuízo de outros Comitês de Assessoramento competentes, nos termos dos seus respectivos Regimentos Internos.

6.2. Comitê de Auditoria, Riscos, Regulatório

- Assessorar o Conselho de Administração no desempenho de sua atuação no tocante à gestão de riscos da Opy, nos termos desta Política e dos demais documentos aplicáveis.
- Supervisionar a adequação dos processos relativos à gestão de riscos, incluindo, mas não limitado aos Mapas, Planos de Ação e Métricas de Avaliação.
- Avaliar a integração adequada dos aspectos relativos à gestão de riscos da Opy com as funções de controles internos e auditoria interna.
- Recomendar revisões nos princípios e instrumentos de gestão de riscos, visando a melhoria contínua do processo.
- Avaliar e sugerir, quando necessário, alterações na estratégia de gestão de riscos para posterior aprovação do Conselho de Administração da Opy.

6.3. Diretoria Executiva

- Garantir que a gestão de riscos esteja alinhada com os objetivos estratégicos da empresa.
- Monitorar a operacionalização dos processos de gestão de riscos, assegurando que sejam eficazes.
- Disseminar e fortalecer a cultura de gestão de riscos em toda a organização, incentivando a participação de todos os níveis hierárquicos.
- Utilizar as informações provenientes da gestão de riscos para tomar decisões mais informadas e seguras.
- Manter uma comunicação transparente com acionistas, clientes, fornecedores e outros stakeholders sobre os riscos e as medidas adotadas para mitigá-los.
- Assegurar que a Área de Integridade, responsável pela Gestão de Riscos Corporativos, disponha de recursos humanos, tecnológicos, processuais e de estrutura organizacional necessários para o cumprimento dos seus objetivos.

6.4. Área de Integridade

- Desenvolver e auxiliar na implementação das políticas, metodologias e ferramentas para o gerenciamento dos riscos, bem como promover a comunicação integrada e disseminar a cultura de gestão de riscos da Companhia.
- Definir metodologias, padrões técnicos, tecnológicos e de gestão mínimos, bem como indicadores de riscos.
- Conduzir com periodicidade pelo menos anual o processo de identificação, avaliação, tratamento e reporte dos riscos.
- Monitorar o status dos planos de ação desenhados para tratamento dos riscos.
- Apoiar os Donos (as) do Risco e demais colaboradores no processo de gestão de riscos.
- Monitorar a aderência às diretrizes definidas.

6.5. Donos do Risco e demais colaboradores indicados

- Gerenciar diretamente os riscos, identificando, avaliando, tratando, prevenindo e monitorando-os de forma integrada.
- Gerenciar os aspectos de tratamento dos riscos sob sua responsabilidade, zelando pela eficácia e tempestividade da realização, pela segurança do processo em conformidade com regulamentações externas, políticas e normas internas, monitorando indicadores, quando aplicável.
- Monitorar os planos de ação e assegurar sua efetiva e tempestiva implantação.
- Comunicar à Área de Integridade qualquer novo risco identificado ou alteração na criticidade dos riscos existentes.

7. METODOLOGIA

7.1. Identificação

O processo de identificação de Riscos Corporativos ocorre de maneira estruturada, considerando as seguintes fontes de informação:

- (i) **Fontes internas:** percepção dos executivos, conselheiros e membros de comitês de assessoramento e demais partes interessadas, planejamento estratégico, avaliação de processos críticos, relatórios de auditoria interna, denúncias protocoladas no Canal de Integridade, dentre outros.
- (ii) **Fontes externas:** relatórios dos auditores independentes, relatórios setoriais etc.

Com periodicidade mínima anual, a Área de Integridade conduzirá uma revisão da matriz de Riscos Corporativos da Opy, com base nas fontes listadas acima.

Caso algum dono de risco ou qualquer outro colaborador das Empresas Opy identifique qualquer risco novo, deve comunicar tempestivamente a Área de Integridade para que a tratativa adequada seja aplicada.

7.2. Categorização

A fim de assegurar uma gestão integrada, consistente e alinhada ao seu apetite a risco, a Companhia classifica os Riscos Corporativos em categorias, garantindo uma visão abrangente dos fatores capazes de impactar o alcance dos seus objetivos estratégicos.

As Empresas Opy classificam seus Riscos Corporativos nas seguintes categorias:

- **Estratégicos** – Riscos relacionados às decisões e diretrizes estratégicas, ao posicionamento competitivo, ao ambiente de mercado e aos fatores externos que podem afetar o cumprimento dos objetivos de longo prazo.
- **ESG** – Riscos associados a aspectos ambientais, sociais e de governança, incluindo sustentabilidade, impactos socioambientais e governança corporativa.
- **Financeiros** – Riscos decorrentes de exposição financeira, liquidez, variações de mercado, crédito, orçamento e demais fatores que possam afetar o desempenho econômico das Empresas Opy.
- **Integridade** – Riscos reputacionais ligados à conformidade, ética, conduta, anticorrupção, fraudes e cumprimento de leis, normas e princípios de integridade corporativa.
- **Operacionais** – Riscos provenientes de falhas, interrupções, ineficiências, incidentes ou desvios nos processos, atividades e serviços, no âmbito das operações das Empresas Opy.
- **Recursos Humanos** – Riscos relacionados à gestão de pessoas, engajamento, sucessão, desempenho, retenção, clima, saúde e segurança ocupacional.
- **Regulatórios** – Riscos associados a mudanças legislativas, regulatórias ou normativas, bem como ao cumprimento de contratos de concessão e de requisitos de autoridades competentes.
- **Tecnologia** – Riscos advindos de sistemas, infraestrutura tecnológica, segurança da informação, cibersegurança, indisponibilidade de serviços, falhas de TI ou ataques cibernéticos.



Política de Gestão de Riscos Corporativos

Elaborada por:	Área de Integridade Opy
Aprovada por:	Conselho de Administração Opy
Data da 1ª aprovação:	12/2025
Vigência:	Por tempo indeterminado
Versão:	1.0

A referida classificação serve como referência institucional para a Gestão de Riscos Corporativos, devendo ser observada na identificação, reporte e mitigação dos riscos.

7.3. Avaliação

Os Riscos Corporativos da Opy são avaliados de acordo com a probabilidade de ocorrência e o impacto causado à Companhia caso o risco se materialize. Essa avaliação é realizada tanto sob o ponto de vista inerente, isto é, antes da avaliação de qualquer aspecto de tratamento do risco, quanto na visão residual, ou seja, após a consideração dos aspectos de tratamento do risco.

A Área de Integridade é a responsável por assegurar a aplicação do método de avaliação para todos os riscos da matriz.

As métricas de probabilidade e impacto são revisadas em base anual pela Área de Integridade, com o apoio da Diretoria Executiva, e comunicadas ao Comitê de Auditoria, Riscos, Regulatório para avaliação. Sempre que houver alterações devem ser submetidas à avaliação do Comitê de Auditoria, Riscos, Regulatório.

Os Riscos Corporativos são classificados em quatro níveis:

- Críticos: estão além do apetite a riscos e precisam de ações imediatas.
- Altos: apesar de estarem dentro do apetite, estão próximos de ultrapassá-lo. Demandam ações.
- Médios: estão gerenciados e precisam ser monitorados periodicamente.
- Baixos: estão gerenciados e precisam ser monitorados com menor recorrência. Podem haver oportunidades de eficiência nas ações de tratamento.

Caso algum dono de risco ou qualquer outro colaborador da Opy identifique a necessidade de reavaliar um ou mais riscos, deve comunicar tempestivamente a Área de Integridade para que a tratativa adequada seja aplicada.

7.4. Tratamento

Os Riscos Corporativos que, em sua visão inerente, estejam além do apetite a risco (formalizado na Declaração de Apetite a Risco) devem possuir uma ou mais ações de tratamento para minimizar a sua probabilidade de ocorrência, a magnitude do impacto ou ambos.

Caso não sejam identificadas ações de tratamento suficientes para trazer o risco a um nível aceitável, planos de ação devem ser desenhados pelo Dono de Risco com apoio da Área de Integridade. A responsabilidade pelos planos de ação pode ser compartilhada pelos Donos de Riscos com outros colaboradores.

A Área de Integridade fará o monitoramento da implantação dos planos de ação dentro dos prazos estabelecidos.



Política de Gestão de Riscos Corporativos

Elaborada por:	Área de Integridade Opy
Aprovada por:	Conselho de Administração Opy
Data da 1ª aprovação:	12/2025
Vigência:	Por tempo indeterminado
Versão:	1.0

7.5. Reporte

Com periodicidade mínima semestral, a Área de Integridade reportará ao Comitê de Auditoria, Riscos, Regulatório os mapas de riscos, assim como os status dos planos de ação e outros temas que entender pertinente.

Com periodicidade mínima anual, a Área de Integridade reportará ao Conselho de Administração os mapas de riscos inerente e residual, e outros aspectos que entender pertinente.

Caso seja identificado uma piora repentina na avaliação de um ou mais riscos, fazendo com que passem a ser classificados como além do apetite a riscos, a Área de Integridade deverá fazer o reporte tempestivo à Diretoria Executiva, podendo o tema ser levado para o Comitê de Auditoria, Riscos, Regulatório.

8. REPORTE DE VIOLAÇÕES

O cumprimento das políticas da Opy, incluindo essa, é esperado de todos os colaboradores, conselheiros, membros de comitê e diretores quando atuando em nome das Empresas Opy. Cada colaborador, conselheiro, membros de comitê ou diretor será responsável por manter a conformidade com essas políticas dentro do seu respectivo setor.

Como consequência, colaboradores, conselheiros, membros de comitê e diretores são obrigados a denunciar qualquer conhecimento ou suspeita de violação desta Política, do Código de Ética da Opy ou da legislação aplicável.

No caso de dúvidas sobre o descumprimento dos instrumentos citados, entrar em contato com a Área de Integridade para mais orientações ou utilizar o Canal de Integridade da Opy, cujo link para acesso encontra-se disponível no site oficial da Companhia (<https://opyhealth.com.br/>).

9. EXCEÇÕES À POLÍTICA

Na excepcional hipótese em que o descumprimento desta Política for escusável por colaborador, conselheiro ou diretor, por motivo de ameaça à sua saúde, segurança e/ou liberdade, é indispensável que a Área de Integridade seja consultada com a devida antecedência, ao qual competirá avaliar as circunstâncias e analisar sobre a possibilidade de descumprimento da Política.

A opinião formalizada será então encaminhada para avaliação do Comitê de Auditoria, Riscos, Regulatório, que poderá decidir pela recomendação, ao Conselho de Administração, da aprovação do descumprimento da Política, de forma devidamente fundamentada e registrada em ata.

10. HISTÓRICO DE REVISÃO

A presente Política e outros documentos relacionados estão sujeitos a monitoramento



Política de Gestão de Riscos Corporativos

Elaborada por: Área de Integridade Opy
Aprovada por: Conselho de Administração Opy
Data da 1ª aprovação: 12/2025
Vigência: Por tempo indeterminado
Versão: 1.0

contínuo, passando por revisão anual da Área de Integridade, e, se alterações forem realizadas, aprovação por parte do Conselho de Administração.

Tipo de Alteração	Versão	Data da Alteração
1ª Aprovação e Publicação	1.0	12/2025

GLOSSÁRIO

Análise de Riscos: Processo de identificar, avaliar e priorizar riscos, seguido pela aplicação de recursos para minimizar, monitorar e controlar a probabilidade e/ou impacto de eventos adversos.

Apetite ao Risco: Nível de risco que uma organização está disposta a aceitar para alcançar seus objetivos.

Avaliação de Riscos: Processo de determinar a magnitude dos riscos identificados, geralmente combinando a probabilidade de ocorrência e o impacto potencial.

Conflito de Agência: Situação em que há divergência de interesses entre os gestores (agentes) e os acionistas (principais) de uma empresa.

Controles Internos: Políticas, procedimentos e práticas implementadas para garantir a integridade financeira e operacional, bem como a conformidade com leis e regulamentos.

Donos do Risco: Gestores designados pela organização para gerenciar diretamente riscos específicos sob sua responsabilidade.

Gestão de Riscos: Conjunto de atividades coordenadas para dirigir e controlar uma organização no que diz respeito a riscos.

Impacto: Consequência ou efeito de um risco se ele se materializar.

Identificação de Riscos: Processo de encontrar, reconhecer e descrever riscos que possam afetar a organização.

Aspectos de Tratamento de Riscos: Ações tomadas para reduzir a probabilidade e/ou impacto de um risco.

Monitoramento de Riscos: Processo contínuo de rastreamento e revisão dos níveis de risco e da eficácia das estratégias de mitigação.

Probabilidade: Chance de um evento de risco ocorrer.

Risco Residual: Risco que permanece após a implementação de medidas de tratamento.

Risco Corporativo: aqueles que na visão do acionista colocam em risco o retorno do investimento e a perenidade da organização, bem como aqueles que impedem a implementação do planejamento estratégico na visão da administração.

Stakeholders: Partes interessadas que podem ser afetadas pelas atividades da organização, incluindo acionistas, funcionários, clientes, fornecedores e a comunidade.