# Política de Gestão de Riscos

| Departamento | Data de atualização | Código |
|---|---|---|
| Compliance, Governança e Gestão de Riscos | 26/11/2025 | GRCPL3.1 |

## Sumário

## 1. Pontos Importantes

**O que fazer:**

- Preservar a reputação, ética, integridade e conformidade legal da Companhia em todas as decisões e relações.
- Conhecer e aplicar esta Política, disseminando a cultura de gestão de riscos em todos os níveis.
- Seguir os princípios e diretrizes desta Política.
- Observar as responsabilidades definidas nesta Política, reconhecendo que a estrutura de gestão de riscos é descentralizada e que cada área deve aproveitar seu conhecimento técnico e perfil profissional.

**O que não fazer:**

- Ignorar riscos identificados ou deixar de comunicar situações que possam impactar a Companhia.
- Descumprir planos de ação ou medidas definidas no processo de gestão de riscos.
- Adotar práticas que contrariem esta Política.

## 2. Objetivo

A Política de Gestão de Riscos Corporativa da Cyrela Brazil Realty S.A Empreendimentos e Participações ("Cyrela ou Companhia") tem como principal objetivo estabelecer as diretrizes necessárias e procedimentos claros para identificar, avaliar, tratar, monitorar e comunicar riscos, garantindo que os objetivos estratégicos da Companhia sejam atingidos com segurança e sustentabilidade.

Tem como propósito disseminar a cultura de gestão de riscos, integrar a gestão aos processos estratégicos e operacionais, assegurar recursos e suporte técnico para mitigação de riscos e alinhar as práticas às legislações, normas internas e melhores práticas do mercado, definindo as atribuições e responsabilidades de todos os administradores, incluindo o Conselho de Administração ("CA") e Comitê de Auditoria Estatutário ("CAE").

Esta Política tem carater majoritariamente orientador e metodológico, estabelecendo princípios, diretrizes e critérios gerais para a gestão do tema. As definições aqui apresentadas visam padronizar o entendimento institucional, garantindo coerência na aplicação dos conceitos. Os procedimentos operacionais, detalhamentos práticos e instruções de execução serão descritos em Manual Interno específico, que complementará esta Política e deverá ser seguido pelas áreas responsáveis na sua aplicação cotidiana.

## 3. Abrangência

Aplicável a todos os relacionamentos internos e externos da Companhia, o que inclui as pessoas físicas e jurídicas:

a) Colaboradores, independente de nível hierárquico e/ou posição de liderança;
b) Administradores;
c) Parceiros de negócios, prestadores de serviços, Fornecedores, clientes e qualquer Terceiro que possua relacionamento com a Companhia;
d) Os indivíduos que, de qualquer forma, representem os profissionais e colaboradores mencionados acima.

## 4. Escopo

O gerenciamento de riscos do Grupo Cyrela compreende, mas não se limita a:

- **Riscos operacionais:** Eventos que podem comprometer as atividades e processos internos relacionado a pessoas, infraestrutura, ex: gestão de pessoas, falha de procedimento.

- **Mercado e Financeiro:** Eventos que possam gerar perdas financeiras devido a fatores internos ou

externos, impactando a capacidade de pagamento, ex: taxa de juros, inflação, mudanças políticas.

- **Socioambiental:** Eventos que gerem impactos diretos sobre o meio ambiente e sobre as pessoas, ex: mudanças climáticas, gestão de residuos, responsabilidade social.
- **Reputação e Imagem:** Eventos que gerem impacto na reputação, credibilidade e valor de mercado, ex: noticiais midiáticas, comunicação com autoridades.
- **Tecnologia:** Eventos que podem causar consequências negativas nos sistemas, dados, operações e infraestrutura tecnológica de uma organização, ex: indisponibilidade de sistemas, invasões de sistemas;
- **Conformidade e Legal:** Eventos derivados de alteração ou descumprimento das legislações e/ou políticas institucionais, ex: LGPD, alterações da reforma tributária.

Os processos de gestão de riscos visam assegurar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo tanto às informações quanto aos riscos aos quais se está exposto, de forma a aumentar a probabilidade do alcance dos seus objetivos e reduzi-los aos níveis aceitáveis.

**A estrutura de gestão de riscos da Companhia é descentralizada,** para aproveitar e potencializar a gestão do conhecimento técnico e perfil dos profissionais de cada área. Os responsáveis pelos processos devem identificar e tratar os riscos que possam afetar os objetivos da Companhia.

A Área de Gestão Riscos visa:

i. Gerar valor de melhoria para tomada de decisões baseada em riscos e oportunidades;
ii. Adotar boas práticas de governança para manter transparencia, qualidade e gerar valor reputacional;
iii. Integrar analise de riscos nos processos de planejamento estratégico, tático e operacional;
iv. Apoiar na continuidade e liderança da marca e companhia.

## 5. Atribuições e Responsabilidades

A disseminação da cultura de gestão de riscos da Companhia é responsabilidade de todos os colaboradores, que têm o papel de contribuir para uma gestão eficiente.

Sendo assim, e sem prejuízo das atribuições legais, regulatórias e aquelas previstas no Estatuto Social e nas normas internas da Companhia, em especial nos respectivos regimentos internos, quando aplicável, a estrutura de gestão de riscos da empresa considera a atuação conjunta dos órgãos de governança

corporativa e de gestão que possuem as responsabilidades a seguir:

## 5.1. Compliance e Gestão de Riscos

a) Sugerir o Programa de Gestão de Riscos;
b) Aplicar metodologia de Gerenciamento de Riscos;
c) Monitorar o cumprimento do apetite ao risco no gerenciamento de riscos; dar suporte às áreas na identificação e tratamento de riscos;
d) Coordenar a atualização do mapa de risco e do plano de ação sempre que necessário;
e) Recomendar mecanismos de controle e planos de ação para mitigação dos riscos identificados e elaboração de planos de continuidade de negócios;
f) Consolidar informações e reportar riscos relevantes ao CAE e ao Conselho de Administração;
g) Promover treinamentos e disseminar cultura de gestão de riscos.

## 5.2. Conselho de Administração (CA)

a) Aprovar o nível de apetite a riscos com seus indicadores, alvos, tolerância e metodologia e acompanhar, com assessoria dos Comitês, as exposições resultantes das decisões tomadas na condução dos negócios da Companhia;
b) Deliberar sobre riscos estratégicos e de maior impacto;
c) Acompanhar o cumprimento dos parâmetros implementados para gestão dos riscos, com o apoio dos Comitês de assessoramento, do departamento de Compliance e o responsável pela auditoria interna;
d) Conscientizar e incentivar os gestores na busca de saídas econômicas para redução da probabilidade de eventos de risco ou para mitigar suas consequências;
e) Patrocinar a cultura de gestão de riscos com apoio da Diretoria Executiva e do CAE, que assumirá a liderança no acompanhamento do cumprimento dessa Política;
f) Garantir que o CAE tenha orçamento próprio para a contratação de consultores para assuntos contábeis, jurídicos ou outros temas, quando necessária a opinião de um especialista externo;
g) Avaliar anualmente, diretamente ou por meio do CAE, a estrutura e o orçamento da Auditoria Interna, que deverá ser suficiente ao desempenho de suas funções.

## 5.3. Comitê de Auditoria Estatutário (CAE)

Assessorar o CA para:

a) O monitoramento e operacionalização dos processos de auditoria interna e externa;

b) O monitoramento e controle dos mecanismos e controles internos relacionados à gestão de riscos;
c) O monitoramento da coerência das políticas, inclusive financeiras, da Companhia com as diretrizes estratégicas e o perfil de riscos do negócio.
d) Avaliar a Definição do Apetite a Riscos da companhia e recomendar alteração ou aprovação pelo CA.

## 5.4. Diretoria

a) Atuar diretamente na gestão dos riscos inerentes às suas atividades (identificar, avaliar e tratar);
b) Informar à área de *Compliance* sobre a identificação de novos riscos ou eventos que sejam relevantes e suas respectivas evoluções;
c) Suporte às decisões do Conselho de Administração no que tange a mitigação dos riscos;
d) Apoiar o subsídio de recursos (humanos, financeiros e tecnológicos) para a implementação de controles internos efetivos e estratégias de mitigação de riscos;
e) Acompanhar a implementação dessa Política, sugerir melhorias e assegurar a existência de plano de administração de crises que permita a Companhia ultrapassá-las de forma segura.

## 5.5. Auditoria Interna

As atividades de Auditoria Interna serão conduzidas por equipe interna independente ou, alternativamente, por empresa especializada, observado que, nesse caso, a empresa deverá ser auditora independente registrada na CVM.

A Auditoria Interna deve ter estrutura e orçamento considerados suficientes ao desempenho de suas funções, conforme avaliação anual realizada pelo Conselho ou pelo CAE. A Auditoria Interna será responsável por aferir a qualidade e a efetividade dos processos de gerenciamento de riscos, controles e governança da Companhia, conforme plano anual sugerido pela área de Compliance, avaliado pelo CAE e aprovado pelo Conselho.

Sem prejuízo do acima exposto e de outras atribuições que venham a ser avaliadas pelo CAE e aprovadas pelo Conselho, compete à Auditoria Interna:

a) Reportar periodicamente à Alta Administração os resultados das avaliações dos riscos e processos de gerenciamento de riscos;
b) Recomendar mecanismos de controle e planos de ação para mitigação dos riscos identificados e elaboração de planos de continuidade de negócios;

### 5.6. Auditoria Contábil - Externa

A auditoria contábil será conduzida por empresa especializada com apoio operacional da área financeira para emissão de opinião independente sobre as demonstrações financeiras da companhia.

### 5.7. Gestores e Donos do Risco

**a)** Assegurar a implementação dos planos de ação que visam mitigar os riscos;

**b)** Implementar controles internos recomendados pela área de riscos;

**c)** Aplicar as metodologias de gerenciamento de risco;

**d)** Identificar, documentar e comunicar às áreas responsáveis todas as perdas operacionais resultantes de falha, deficiência ou inadequação de processos e controles internos, pessoas e sistemas ou eventos externos; e,

**e)** Definir o Nível de Apetite a Risco com seus indicadores, alvos, tolerância e metodologia e submeter a aprovação do CA

### 5.8. Área de Qualidade

Riscos da dimensão operacional, e que são auditadas pela ISO 9001 do time de Qualidade serão acompanhados e monitorados por esta área.

A área de Qualidade é responsável por garantir que os riscos operacionais identificados nos processos certificados estejam mapeados, avaliados e tratados conforme o Sistema de Gestão da Qualidade.

Riscos estratégicos ou operacionais com alto impacto, identificados por meio de monitoramento feito pela área de Gestão de Riscos; comunicação formal das áreas ou outro meio, serão inseridos na matriz de riscos e auditados pela Auditoria Interna seguindo o fluxo estabelecido nos outros riscos.

## 6. Processo de Gestão de Riscos

A gestão de riscos da Cyrela segue o ciclo contínuo, integrado ao planejamento estratégico, aos controles internos e ao Programa de Integridade da Companhia, caracterizado pelas etapas descritas abaixo:

### 6.1. Identificação e Análise de Riscos

A Companhia a classificação de riscos corporativos estruturada de forma a proporcionar uma visão integrada e consistente dos eventos que possam impactar o alcance de seus objetivos estratégicos,

operacionais e de conformidade. A classificação considera três dimensões complementares: **origem**, **dimensão do efeito organizacional** e **macro categoria**.

- *Origem dos Riscos.*

**Interna:**

Fatores sob controle direto da Companhia, originados em seus processos, estruturas, sistemas, pessoas ou decisões internas.

**Externa:**

Fatores fora do controle direto da Companhia, decorrentes de mudanças no ambiente externo, como aspectos econômicos, regulatórios, sociais, ambientais ou tecnológicos.

- *Dimensão do Efeito Organizacional.*

**Estratégico:**

Compreende os riscos que podem comprometer a execução da estratégia corporativa, a sustentabilidade e a perenidade da Companhia. São, em geral, decorrentes de fatores externos ou de decisões de alto nível que influenciam o posicionamento competitivo, a reputação e a geração de valor no longo prazo.

**Operacional:**

Abrange os riscos relacionados à execução das atividades da Companhia, envolvendo processos internos, sistemas, pessoas e terceiros. Tais riscos podem afetar o alcance dos objetivos operacionais, a eficiência e a continuidade das operações.

- *Macro Categorias de Riscos.*

**Mercado e Financeiro:**

Riscos decorrentes de fatores internos ou externos que possam ocasionar perdas financeiras, comprometer a liquidez, o desempenho econômico ou a capacidade de pagamento da Companhia.

**Socioambiental:**

Riscos associados a eventos que possam gerar impactos adversos ao meio ambiente, às comunidades ou às pessoas, afetando a sustentabilidade das operações.

**Reputação e Imagem:**

Riscos relacionados a eventos que possam afetar negativamente a reputação, a credibilidade ou o valor de mercado da Companhia perante seus interessados.

**Tecnologia:**

Riscos que envolvem falhas, incidentes ou vulnerabilidades em sistemas, dados, infraestrutura

tecnológica ou segurança da informação, com potencial de comprometer a continuidade e a integridade das operações.

**Conformidade e Legal:**
Riscos decorrentes do descumprimento ou da inadequação a legislações, regulamentações, normas externas ou políticas e procedimentos internos da Companhia.
Riscos associados a falhas, ineficiências ou interrupções nos processos internos, envolvendo aspectos relacionados a pessoas, infraestrutura, sistemas e controles operacionais.

Os riscos corporativos relacionados à Companhia são identificados e analisados para assegurar que ameaças e oportunidades sejam reconhecidas tempestivamente e tratadas em nível aceitável.

Para identificar e descrever os riscos, a Companhia deve utilizar entrevistas, questionários, análise de evidências e de cenários, monitoramento de indicadores-chave de risco (KRIs), além da coleta de dados, documentos e validações junto às áreas técnicas envolvidas.

O resultado desse processo é a matriz de riscos corporativos, que relaciona os riscos conforme taxologia descrita acima, atribui responsáveis (donos de risco), materialização e suporta a avaliação, priorização e definição de planos de tratamento.

Avaliação e Priorização: Após a identificação dos Riscos, os mesmos serão analisados quanto a probabilidade X impacto que irá trazer em decorrência a sua materialização. O resultado será a sua criticidade.

## 6.2. Criticidade

A criticidade representa o grau de exposição da Companhia a determinado risco e é obtida pela combinação entre o Impacto e a Probabilidade de ocorrência do evento.

Essa análise permite classificar o risco quanto à sua relevância, orientar a priorização de tratamento e apoiar a tomada de decisão em todos os níveis da organização. A classificação é realizada conforme os níveis descritos a seguir: **Muito Baixo, Baixo, Médio, Alto e Crítico.**

### 6.2.1. Impacto

A Companhia adota a seguinte metodologia para avaliação do **impacto** dos riscos corporativos, considerando as principais dimensões afetadas por um evento de risco. O impacto representa a severidade das consequências caso o evento se materialize, sendo avaliado com base em parâmetros **financeiros, operacionais, ambientais, sociais, legais/conformidade e de reputação**.

Essa estrutura visa assegurar uma análise abrangente e consistente dos efeitos potenciais sobre o negócio, a sustentabilidade e a imagem institucional da Companhia. A classificação é realizada conforme os níveis descritos a seguir: **Muito Baixo, Baixo, Médio, Alto e Muito Alto.**

### 6.2.2. Probabilidade

A **probabilidade** representa a chance de ocorrência de um evento de risco, considerando fatores internos e externos que possam influenciar sua materialização.

A Companhia adota metodologia baseada em cinco níveis de classificação, que permitem mensurar de forma objetiva a frequência ou a possibilidade de um risco ocorrer, conforme percepção dos responsáveis pelos processos e histórico de eventos.

A avaliação é realizada em conjunto entre os **donos dos riscos** e a **área de Gestão de Riscos**, levando em consideração a natureza da atividade, controles existentes e o ambiente operacional em que o processo está inserido. A classificação é realizada conforme os níveis descritos a seguir: **Muito Baixo, Baixo, Médio, Alto e Muito Alto.**

## 7. Apetite a Riscos e Tolerância

A Gestão Administrativa sugere indicadores e suas métricas operacionais como alvo, metodologia e tolerancia, garantindo uma gestão de riscos proativa.

O Comitê de Auditoria Estatutário (CAE) avalia as propostas e recomenda a aprovação ao CA, o responsável final pela aprovação da Declaração de apetite ao Risco.

Os principais critérios de definição incluem:

- Níveis de perdas financeiras esperadas e não esperadas;
- Padrões de mercado e melhores práticas de governança;
- Preferências e expectativas das partes interessadas;
- Exposição a riscos socioambientais e de integridade corporativa;
- Retorno esperado sobre o capital;
- Volatilidade dos resultados;
- Quantidade de capital em risco;
- Cultura organizacional;
- Capacidade de resposta e resiliência da Companhia;
- Prioridades estratégicas de curto, médio e longo prazo.

## 8. Tratamento dos Riscos

O tratamento consiste na escolha da resposta mais adequada para modificar a probabilidade ou o impacto de cada risco. As alternativas são: **Aceitar**, **Transferir**, **Mitigar** ou **Evitar**.

Cada risco acima da criticidade "baixa" identificado deve ter um controle mitigatório implantado

- Para riscos críticos, deve-se criar planos de ação com reportes periódicos ao CAE e ao Conselho de Administração.
- Todas as ações devem ter um gestor para realizar o estudo técnico de viabilidade operacional e financeira da ação.
- Caso a opção seja aceitar o risco, devem ser estabelecidas pela Diretoria métricas de monitoramento específicas.

Além disso, riscos materializados devem ser classificados como elegíveis a ações corretivas e de melhoria contínua, visando reduzir a chance de reincidência.

A metodologia da Auditoria Interna será baseada em riscos (unicamente ou mesclando-se outras) para garantir a eficência dos controles implantados.

## 9. Comunicação e Monitoramento

A Companhia deve comunicar, de forma clara e tempestiva, os resultados das etapas de gestão de riscos, às partes interessadas internas e externas, quando aplicável.

A Diretoria, em conjunto com o departamento de *Compliance,* deve garantir, por meio de monitoramento contínuo, auditorias periódicas e indicadores-chave de risco (KRIs), a eficácia dos controles implementados.

Todas as etapas do processo devem ser registradas, documentadas e armazenadas pelo departamento de *Compliance,* de modo a permitir rastreabilidade e transparência.

Em casos de identificação de novos riscos, bem como de materialização de riscos já constantes na Matriz Corporativa de Riscos, o colaborador deverá comunicar imediatamente a área de Gestão de Riscos por meio do e-mail corporativo destinado a este fim a fim de que o evento seja avaliado e registrado.

O processo de gerenciamento de riscos é dinâmico, revisitado periodicamente, considerando alterações no ambiente interno, mudanças regulatórias e evolução dos negócios.

## 10. Disposições Gerais

Esta política passa a vigorar a partir da data de sua publicação, com a data de validade de 2 (dois) anos, podendo ser alterada a qualquer tempo e critério pela Área de Compliance que deverá submeter as alterações para análise do CAE e aprovação do Conselho de Administração.

Esta política deve ser lida e entendida em conjunto com as demais políticas que fazem parte do Programa de Integridade, disponíveis na intranet e no Portal de Integridade.

## 11. Referências

- Lei nº 12.846/2013 – Lei Anticorrupção Empresarial;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- ISO 31000 – Gestão de Riscos – Diretrizes;
- IBGC – Código das Melhores Práticas de Governança Corporativa;
- Código de Conduta do Grupo Cyrela;
- COSO ERM 2017;
- ISO 3100/2018;
- Lei nº 6.404/1976 – Lei das Sociedades por Ações.
- Resoluções e Instruções da Comissão de Valores Mobiliários (CVM), em especial no tocante à governança corporativa e controles internos.

## 12. Histórico de mudanças

| Revisão | Descrição | Data |
|---|---|---|
| 1.0 | - Elaboração da PLCOMP11-Política de Gestão de Riscos | 27/11/2020 |
| 2.0 | - Readequação geral da Política de Gestão de Riscos de acordo com modelo de negócio da Companhia;<br>- Alteração para novo modelo visual | 04/11/2021 |
| 3.0 | - Adequação para matriz 5x5<br>- Atualização das responsabilidades do CARF<br>- Nova classificação de natureza dos riscos<br>- Ajustes na estrutura e atribuições da Auditoria Interna | 09/03/2023 |
| 4.0 | - Alteração do prazo de revisão do documento<br>- Atualização das nomenclaturas do tratamento de risco<br>- Atualização das informações sobre o grau de exposição aos Riscos<br>- Atualização do Comitê - CAE | 14/12/2023 |
| 5.0 | - Revisão da Política;<br>- Alteração da Metodologia dos riscos | 26/11/2025 |

São Paulo, 26 de novembro de 2025.

CYRELA

*Aprovada em Reunião do Conselho de Administração da Cyrela Brazil Realty S.A.Empreendimentos e Participações realizada em 08 de dezembro de 2025.*