

1. OBJETIVO

Estabelecer princípios, conceitos, diretrizes e responsabilidades na Gestão de Riscos da Companhia Brasileira de Distribuição e das suas controladas que não sejam companhia aberta (em conjunto, “GPA”) no que tange a identificação, análise e avaliação dos Riscos (conforme abaixo definido) que possam afetar os seus objetivos estratégicos e a efetiva criação e proteção do valor do GPA.

Definir, a partir dos Riscos Inerentes (conforme abaixo definido), dispositivos de controles e de monitoramento das exposições, incorporando a visão de Riscos à tomada de decisões estratégicas e em conformidade com os requerimentos legais, com as melhores práticas e metodologias de mercado aplicáveis.

2. ABRANGÊNCIA

Aplicável para todos os macroprocessos e operações de negócio da Companhia Brasileira de Distribuição e suas controladas que não sejam companhia aberta.

3. DEFINIÇÕES

Apetite a Risco: É o nível de Risco que a Companhia está disposta a aceitar, de acordo com a relação risco/retorno, para atingir seus objetivos de acordo com os limites estabelecidos pela Alta Administração.

Capacidade: A disposição de recursos que a Companhia possui para atender o seu plano estratégico, como recursos de capital financeiro, tecnologias, processos e pessoas, entre outros.

COAUD: Comitê de Auditoria da Companhia.

COMEX: Comitê Executivo da Companhia.

Companhia: a Companhia Brasileira de Distribuição

Consequências do Risco: São fatores agravantes dos resultados e impactos de um Evento que possa afetar, positiva ou negativamente, a capacidade da Companhia em atingir seus objetivos.

DIREX: Diretoria Executiva da Companhia.

Evento: Uma ocorrência ou um conjunto de ocorrências, que podem gerar impactos ao GPA, afetando os seus resultados positiva ou negativamente.

Gestão de Riscos: Conjunto de atividades coordenadas e estruturadas a fim de alinhar o Apetite de Risco ao ciclo de tomada de decisão estratégica na busca de otimizar os resultados estabelecidos no planejamento estratégico e a efetiva criação e proteção do valor do GPA.

GPA: a Companhia Brasileira de Distribuição e suas controladas que não sejam companhias abertas.

Impacto: São fatores agravantes ou consequências no caso do Risco se materializar, pode ser classificado em Impacto Financeiro, e Reputacional.

Key Performance Indicator (KPI ou Indicadores-chave de Performance): Métricas utilizadas para medir e monitorar o desempenho e resultados dos processos, podendo ser utilizado para monitoramento de Riscos.

Probabilidade: É a possibilidade do Risco se materializar, podendo ser relatado de maneira qualitativa, quantitativa e por frequência.

Risco: Fatores e/ou Eventos que possam causar impactos negativos, comprometendo a capacidade da companhia de atingir seus objetivos estratégicos e a efetiva criação e proteção do valor do GPA.

Risco Inerente: Nível de Risco intrínseco à operação do negócio ou à atividade, sem considerar a execução de controles e ações diretas que reduzam as suas exposições, também chamado de risco bruto.

Riscos Priorizados: Lista de Riscos definida de forma deliberada pela administração da Companhia, que descreve níveis de exposições que possam potencializar impactos elevados para o negócio, cuja Gestão de Riscos deve ser priorizada de forma estruturada.

Risco Residual: Tipo de Risco em nível que já considera todos os controles e ações identificadas para redução da sua exposição.

Tolerância: Os limites da variação aceitável no desempenho em relação ao alcance dos objetivos de negócio.

4. ÁREAS RESPONSÁVEIS, PAPÉIS E RESPONSABILIDADES

Descrevemos todas as partes interessadas que estão dentro do contexto e do ciclo de vida do processo de Gestão de Riscos com as suas respectivas responsabilidades:

Função	Responsabilidades
Conselho de Administração	• Estabelecer as diretrizes gerais de Riscos alinhadas ao contexto de negócio e do ciclo de planejamento estratégico; • Estabelecer através da Capacidade e Tolerância do GPA os limites aceitáveis de Appetite a Risco; • Avaliar, deliberar e aprovar a matriz de Riscos estratégicos e Priorizados alinhados ao Appetite a Risco; • Influenciar e patrocinar dentro dos fóruns de gestão o monitoramento dos Riscos Priorizados; • Influenciar e patrocinar a cultura de riscos dentro do GPA; • Avaliar, anualmente, a suficiência da estrutura e do orçamento da área de Auditoria Interna para o desempenho das suas funções; • Revisar e aprovar as definições gerais das estratégias de Gestão de Riscos; • Aprovar a política de riscos, suas evoluções e revisões futuras.

COAUD	• Acompanhar as atividades da auditoria interna e da área de controles internos do GPA; • Avaliar e monitorar as exposições de Risco do GPA; • Propor aos fóruns elegíveis definições e diretrizes para compor o modelo de Gestão de Riscos dentro do GPA; • Acompanhar e apoiar o processo de Gestão de Riscos na definição dos Riscos Priorizados alinhados ao contexto de negócio e as diretrizes do Conselho de Administração; • Supervisionar as atividades de Gestão de Riscos seguindo o cumprimento das legislações legais, das políticas, normas e procedimentos internos do GPA; • Avaliar, monitorar e informar periodicamente o Conselho de Administração sobre os Riscos Priorizados identificados pelas revisões das áreas de Gestão de Riscos, auxiliando na avaliação dos planos de ação e recomendações; • Avaliar, aprovar e acompanhar a execução do tratamento e monitoramento dos Riscos Priorizados; • Avaliar, aprovar e recomendar à administração a correção ou aprimoramento das políticas internas do GPA; • Avaliar as informações trimestrais, demonstrações intermediárias e demonstrações financeiras da Companhia.
Comitê de Recursos Humanos e Governança Corporativa e Comitê de Sustentabilidade e Diversidade	• Elaborar o planejamento e assegurar a operacionalização da Gestão de Riscos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais do GPA; • Assessorar o Conselho de Administração na aplicação da metodologia de Gestão de Riscos no GPA; • Apoiar o Conselho de Administração na definição do Apetite a Risco e na definição dos Riscos Priorizados do GPA; • Apoiar o GPA na análise e aprovação da estratégia de Gestão de Riscos; • Assessorar o Comitê de Auditoria e o Conselho de Administração sobre os níveis de exposições dos Riscos; • Avaliar a eficácia do processo de Gestão de Riscos no GPA; • Identificar os Riscos decorrentes das mudanças estratégicas e diretivas do GPA sob decisão do Conselho de Administração.
COMEX / DIREX	• Promover a integração e a cultura de riscos no GPA e nos ciclos de gestão e planejamento estratégico; • Garantir a implantação de um modelo eficiente de Gestão de Riscos, alinhado aos objetivos de negócios e metas de negócio. Aplicar as diretrizes gerais estabelecidas pelo Conselho de Administração para atribuir o nível de Apetite a Risco aceitável para o GPA;

	• Acompanhar os Riscos gerenciados para garantir a efetividade das medidas de controle; • Participar dos rituais de validações e priorização dos Riscos do GPA. • Acompanhar os KPIs e as estratégias de mitigação dos Riscos Priorizados; • Avaliar e monitorar o tratamento dos Riscos de negócio alinhados à execução do planejamento estratégico; • Avaliar, tempestivamente, a eficácia a aplicabilidade das diretrizes da política de Riscos; • Avaliar e apoiar as adequações da estrutura destinada ao processo de gerenciamento, considerando recursos humanos, financeiros e tecnológicos.
Diretoria de Gestão de Riscos	• Definir e evoluir a metodologia de Gestão de Riscos alinhada à cadeia de valor e integrada dentro de todo o GPA; • Gerir o ciclo do processo de Gestão de Riscos no GPA cobrindo todas as unidades de negócio; • Garantir a gestão do fluxo de informações dentro de todas as unidades de negócio alinhada aos conceitos, a metodologia e aos prazos estabelecidos a cada ciclo de Gestão de Riscos; • Apoiar as unidades de negócio no ciclo de identificação, avaliação, tratamento e monitoramento dos Riscos para auxiliá-los na redução dos níveis de exposição dos Riscos; • Gerir a matriz de Riscos Priorizados, comunicando dentro dos principais fóruns de gestão seus status e níveis de exposições; • Suportar as áreas de negócio na identificação e avaliação do Impacto dos Riscos; e • Acompanhar a implementação dos planos de ação pela área responsável e reportar possíveis atrasos e/ou incremento dos Riscos para o negócio.
Dono do Risco	• Identificar, classificar e gerenciar os Riscos das respectivas áreas de acordo com as estratégias de mitigação, em conjunto com a Diretoria de Gestão de Riscos; • Indicar o profissional que responderá como facilitador na Gestão de Riscos junto a Diretoria de Gestão de Risco; • Assegurar a implementação dos planos de ação e acompanhamento dos KPIs; e • Prestar contas dos níveis de exposição, dos planos de ações e dos indicadores que descrevem o status do Risco Residual para os fóruns de governança e gestão.
Facilitador / Responsável	• Deter o conhecimento técnico dos processos no qual os Riscos estão inseridos;

	• Ser o responsável pela atualização das informações do mapeamento e tratamento dos Riscos da sua unidade de negócio; • Manter as informações atualizadas tempestivamente, respeitando o calendário de planejamento do ciclo de Gestão de Riscos; e • Monitorar o status dos planos de ação junto aos responsáveis pela implementação dos dispositivos de controles.
Auditoria Interna	• Aferir a qualidade e a efetividade dos processos de gerenciamento de Riscos, controle e governança do GPA; • Identificar e apontar oportunidades de melhorias nos processos de controle internos e de Gestão de Riscos; • Auditar as informações e controles relacionados aos KPIs desenvolvidos e monitorados pelas áreas funcionais; e • Reportar periodicamente ao COAUD e aos seus clientes auditados os resultados de avaliações independentes, imparciais e tempestivas sobre a efetividade da Gestão de Riscos no GPA.
Colaboradores	• Assegurar a operacionalização da Gestão de Riscos, fazendo parte do processo de identificação, avaliação e mensuração, implementando ações preventivas e corretivas; • Participar de treinamentos que permitam a disseminação de forma consciente da cultura de Gestão de Riscos.
Auditoria Externa	• Avaliar a qualidade dos controles internos voltados para o preparo de demonstrações financeiras, reportando à Companhia as fragilidades em tais controles, se encontrarem.

Tabela 1: Papéis e responsabilidades

5. DIRETRIZES ESPECÍFICAS

Temos como diretrizes gerais o compromisso com a proposta de valor do GPA, alinhados ao seu código de ética e conduta, para que possamos criar uma cultura de Gestão de Riscos que atinja a todos os seus colaboradores.

A Gestão de Riscos é parte do processo de Auditoria e Governança Corporativa do GPA, sendo parte integrante do processo decisório, contribuindo para a execução da sua estratégia. Os Riscos são identificados e tratados de forma a assegurar o cumprimento das metas estabelecidas no planejamento estratégico.

Para isso, a estrutura de Gestão de Riscos considera a atuação conjunta dos órgãos de governança corporativa e de gestão, de acordo com o conceito das 4 linhas de defesa, descrito na *tabela 2* abaixo:

1ª Linha	2ª Linha	3ª Linha	4ª Linha
- A Gestão Operacional, representado pelas diretorias, gerências e demais colaboradores das unidades de negócio que atuam nas operações e tarefas do dia-a-dia. - Devem gerenciar o desempenho e os Riscos assumidos de acordo com o estabelecido na política. - Implementam controles, planos de ação e prestam contas, tempestivamente, das informações relacionadas à Gestão de Riscos.	- As áreas de controles e funções de suporte, representados pela Diretoria de Gestão de Riscos, a qual por sua vez, pode requerer o assessoramento pelas áreas internas do GPA responsáveis por questões de <i>Compliance</i>, Controles Internos e Segurança da Informação. - Devem orientar, monitorar e avaliar a aderência aos padrões e políticas definidas e dar suporte à 1ª linha de defesa para atingir os objetivos do GPA. - Facilitar, comunicar e monitorar as práticas de Gestão de Riscos e auxiliar na identificação de Riscos segundo o Apetite a Risco estabelecido.	- As funções de garantia, representado pela Auditoria Interna, responsável por realizar auditorias ou revisões de práticas de Gerenciamento de Riscos e dos Controles Internos e eficácia da governança, identificando problemas e oportunidades de melhoria com independência, objetividade e autoridade para as recomendações.	- As funções de Auditoria Externa Independente, que tem por missão profissional avaliar a qualidade dos controles internos voltados para o preparo de demonstrações financeiras. Nesse papel, a Auditoria Externa Independente é também uma linha de defesa pois tem que reportar à Companhia as fragilidades em tais controles, se encontrarem.

Tabela 2: Linhas de defesa

5.1. PROCESSO DE GESTÃO DE RISCOS

O processo de Gestão de Riscos do GPA foi definido com base nas orientações do COSO – *Committee of Sponsoring Organizations of the Treadway Commission* e na norma ISO 31000: 2018 - Princípios e Diretrizes da Gestão de Riscos.

O ciclo de vida do processo é constituído de 7 etapas subsequentes e dependentes, as quais são executadas com frequência anual, conforme fluxo ilustrado na *figura 1*.



Figura 1: Etapas do processo de Gestão de Riscos GPA

5.2. ETAPAS DO PROCESSO

◆ Etapa 1 - Estabelecimento do Contexto:

Entender o cenário e contexto de negócio considerando fatores ligados ao planejamento estratégico de curto e longo prazo do GPA, alinhados ao ambiente em que esses objetivos são inseridos.

É uma etapa fundamental para garantir que o processo de Gestão de Riscos esteja alinhado aos ciclos de gestão e de planejamento estratégico do GPA para alinhar seus níveis aceitáveis de *Apetite a Risco*.

É constituída de um ciclo anual de alinhamentos executivos com os donos do processo e a Alta Administração para compor um mapa de referências que irá auxiliar nas próximas etapas, para identificar os Riscos que estão mais alinhados ao contexto do negócio.

Para estabelecer os cenários que devem apoiar essa etapa consideramos dois fatores influenciadores, são eles:

- **Fatores Externos:** Econômicos, Meio ambiente, Políticos e Sociais.
- **Fatores Internos:** Infraestrutura, Recursos Humanos, Processos e Tecnologias.

◆ Etapa 2 – Identificação dos Riscos:

A abordagem de identificação de Riscos é *top-down*, partindo de entrevistas com os principais executivos do GPA, tendo em vista os principais processos pelos quais são responsáveis.

O produto gerado nessa etapa é uma lista abrangente de Riscos baseada nos Eventos que possam identificar vulnerabilidades e ameaças que coloquem em risco a realização dos objetivos estratégicos do GPA.

Nesta etapa também deve ser definido o dono e o responsável por cada um dos Riscos identificados, assim como uma descrição que orientará as próximas etapas do mapeamento.

◆ Etapa 3 – Análise:

Realiza-se uma análise mais detalhada dos Riscos identificados, incluindo atributos importantes para dar clareza e respaldo qualitativo e quantitativo para gerar variáveis que possam classificar de forma holística o universo de Riscos para atuarmos de forma mais assertiva nas suas priorizações.

Define-se, entre outros, as suas causas ou fatores de risco e seus efeitos, classificando seus fatores agravantes para que possamos gerar uma lista de Riscos abrangente e relevante para prosseguir com o mapeamento.

Coletam-se informações para obter dados que possam descrever a Probabilidade e Impactos dos Riscos, gerando assim uma matriz qualitativa para descrever de forma executiva o universo de riscos com base nas suas classificações, como segue descrito na figura 2.

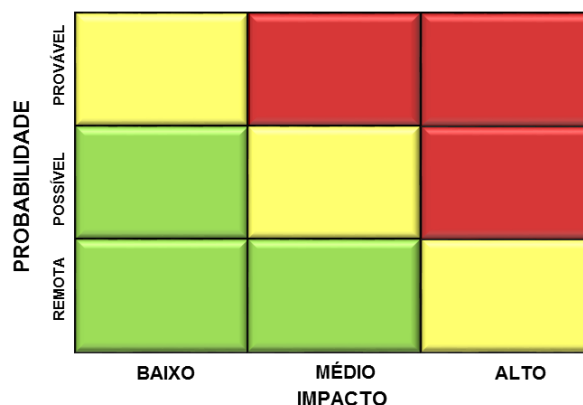


Figura 2: Matriz de Riscos Qualitativa

Os Riscos são classificados dentro dessa matriz qualitativa, seguindo os seguintes critérios:

- **Classificação Alta ou Risco Alto (Vermelho):** Representam uma ameaça potencial aos negócios do GPA e devem ser tomadas ações prioritárias para reduzir ou eliminar o componente de Risco.
- **Classificação Média ou Risco Médio (Amarelo):** Representam uma ameaça, podendo ser monitorados e gerenciados através de medidas de controles preventivas que possam manter o grau de exposição ou aceitação do Risco.
- **Classificação Baixa ou Risco Baixo (Verde):** Representam uma ameaça aceitável com Impactos menores, não havendo necessidade de monitoramento contínuo e podendo ser aceito.

◆ Etapa 4 – Avaliação:

Os Riscos Inerentes e seus potenciais Impactos de materialização para a realização dos objetivos do GPA são analisados.

Com o suporte da Alta Administração, dos executivos e dos líderes de processos avaliam-se os Eventos dentro das perspectivas de Probabilidade ou frequência e Impactos. Buscam-se variáveis para combinar métodos de avaliação qualitativos e quantitativos.

Considera-se, entre outras, variáveis para classificação de Impactos que auxiliam na melhor classificação dos Riscos, utilizando o gradiente de alto, médio e baixo para cada variável.

Por fim, combinando todas as variáveis de avaliação, define-se a criticidade dos Riscos identificados, o que nos permite construir um mapa de priorização, partindo dos Riscos de maior exposição para os de menor exposição.

Esse mapa auxilia o GPA a obter um maior grau de alinhamento do planejamento estratégico com o nível aceitável de Apetite a Risco do GPA.

◆ Etapa 5 – Tratamento:

A fase de tratamento de Riscos envolve identificar os dispositivos de controle existentes dentro do processo para classificação da sua efetividade como medida de prevenção e como fator redutor do grau de exposição (Fator Mitigatório) que irá auxiliar na atribuição do Risco Residual.

Para os processos que requerem maior grau de efetividade dos controles ou que não possuem fatores de mitigação efetivos, formaliza-se nessa etapa a implementação de um ou mais planos de ação para mitigar os fatores de risco.

Para cada plano de ação, são atribuídos responsáveis e cronogramas de implementação para garantir a eficácia e eficiência dos planos e assim reduzir o nível de Risco Residual.

Dentro desse processo, alternativas de respostas aos Riscos são aplicadas conforme *tabela 3*:

Eliminar	Reduzir ou Mitigar	Transferir	Aceitar
Adotar ações que alterem ou eliminem um processo ou um projeto, protegendo os objetivos do negócio dos Impactos deste Risco.	Adotar medidas de controle para reduzir a Probabilidade e/ou o Impacto de um Risco até um nível aceitável de acordo com o Apetite a Risco.	Adotar ações que reduzam a Probabilidade e/ou o Impacto do Risco pela transferência total ou pelo compartilhamento de uma parte do Risco.	Nenhuma medida é adotada para afetar a Probabilidade e/ou o Impacto do Risco, pois está dentro do nível aceitável de Apetite a Risco.

Tabela 3: Alternativas de resposta para os Riscos

◆ Etapa 6 – Monitoramento:

Constituída de um ciclo dinâmico e contínuo, sendo fundamental para garantir de forma tempestiva, preventiva e reativa ações que auxiliem em minimizar Impactos em caso de materialização dos Riscos.

Os colaboradores envolvidos em cada área devem ter a capacidade e competência para identificar, avaliar, priorizar, monitorar e gerir os seus Riscos, considerando todas as mudanças dentro do ambiente interno e externo, para que possam obter maior grau de controle dos seus processos para atingir os objetivos firmados no tratamento dos Riscos (*Ver tabela 3*).

O processo de monitoramento dos Riscos é constituído de duas frentes principais, são elas:

- **Planos de Ação:** Deve ser realizado pelas unidades de negócio de acordo com as responsabilidades definidas pelos donos dos Riscos, com periodicidade que pode variar de mensal, bimestral, trimestral, semestral, chegando até a anual, dependendo das necessidades de Gestão do Risco.
- **Medida de Controles:** Métricas e indicadores relacionados aos fatores de Risco e aos fatores de medidas de prevenção que são identificados durante a fase de tratamento dos Riscos, de acordo com os dispositivos de controle, definindo os limites aceitáveis que descrevam de forma indutiva se os indicadores apontam tendências ou desvios que possam materializar os Riscos para que atribuam gatilhos para as unidade de negócio realizar ações de reversão dos Eventos e consequentemente dos seus Impactos.

◆ Etapa 6 – Comunicação:

Cumpre-se um ritual frequente de alinhamentos que tem como objetivo desde a disseminação da cultura de Gestão de Riscos através de treinamentos e / ou de rituais de prestação de contas com os donos dos Riscos e com os principais fóruns de gestão do GPA, como COMEX / DIREX, Conselho de Administração e COAUD.

Para cumprir esse ritual de comunicação, define-se um plano com formatos de comunicação adequado ao público-alvo, com a descrição de frequência, envolvidos e a responsáveis.

5.3. CLASSIFICAÇÃO DOS RISCOS

Adotamos 4 classificações de Riscos dentro do processo, são eles:

- **Estratégicos:** Riscos que afetam a estratégia ou os objetivos estratégicos do GPA. Estão ligados a cenários de incertezas e/ou oportunidades e estão no foco prioritário da Alta Administração.
- **Operacionais:** Riscos decorrentes da inadequação ou falha na gestão de processos internos, de pessoas ou tecnologias que possam dificultar ou impedir o alcance dos objetivos.
- **Externos:** Riscos provenientes de fatores externos ao GPA, ou que não estão no controle do GPA.
- **Responsabilidade social corporativa (“CSR”):** Riscos relacionados ao tema de ESG, abordando aspectos ambientais, sociais e de governança que impactam o GPA.

6. PENALIDADES

O colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração ao Canal de Ouvidoria. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares baseadas na *Política de Gestão do Comitê de Ética*, *Código de Ética GPA* e na *Política de Consequências e Sanções Disciplinares*.