Política

Gestão de Riscos

ERM Oi

Diretrizes e Metodologia

Índice

Objetivo

Estabelecer diretrizes para o desenvolvimento e disseminação de uma cultura e modelo de gestão baseados em risco, e um conjunto de regras para implementação e manutenção de um processo estruturado e contínuo de gerenciamento de riscos corporativos.

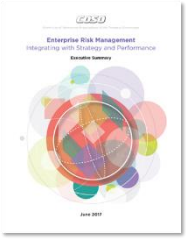
Abrangência

Esta Política é aplicável a todas as áreas da Oi e empresas do Grupo, mas poderão haver ajustes para adequar métricas (critérios de medição de impacto e probabilidade) mais apropriadas e proporcionais à realidade de cada área ou empresa e que atendam a requisitos específicos de dados processos, sempre respeitando os limites determinados nesta Política.

Referências

ISO 31000 2018 (*Risk Management Guidelines*):

Principal referência internacional para gestão de riscos, a última versão foi lançada em 2018 e determina a necessidade dos processos de gestão de riscos estarem mais próximos dos níveis estratégicos do ambiente de negócios.



COSO ERM (Gerenciamento de Riscos – Integrado com Estratégia e Performance):

Em sua última versão (2017) atualizou o *framework* para gestão de riscos corporativos, conectando esta aos processos relacionados a tomadas de decisão, desdobramento e execução da estratégia corporativa.

Caderno 19 de Governança Corporativa IBGC (Gestão de Riscos Corporativos):

Assim como as demais literaturas, passou por uma revisão, sugerindo papéis e responsabilidades aos processos de gestão de riscos considerando o âmbito estratégico e tático das organizações.

Disposições Gerais

A função de Gestão de Riscos é um processo cíclico e dinâmico que identifica, avalia, monitora e responde aos riscos que possam comprometer o atingimento dos objetivos estratégicos da Companhia ou causar impactos significativos ao seu negócio. Este processo permite que responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações suficientes relacionadas aos riscos aos quais estão expostos,

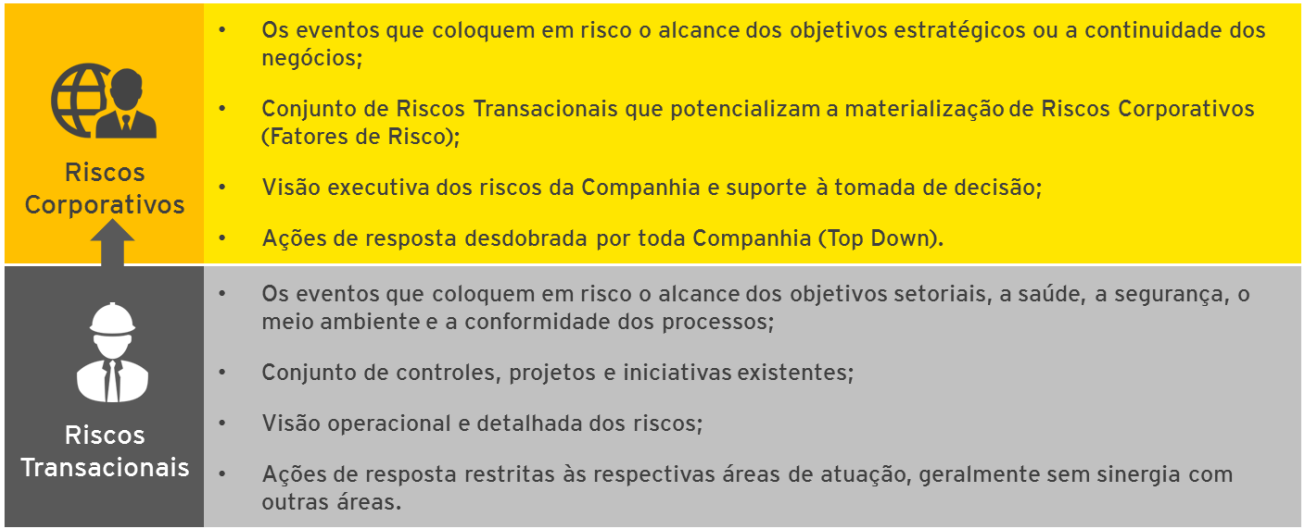
de forma a suportar decisões e definição de estratégias que aumentem a probabilidade de alcance dos objetivos e minimizem riscos a níveis aceitáveis.

Trata-se de uma abordagem preventiva que visa criar meios para gerenciar e manter os riscos sob controle (dentro do apetite estabelecido) de maneira a se antecipar a eventuais incidentes ou crises.

Há duas visões distintas e complementares de gestão de riscos: Visão Corporativa e Visão Transacional.

A **Visão Corporativa** gerencia riscos que afetam a companhia como um todo e estão diretamente relacionados aos objetivos estratégicos da Organização e a continuidade do negócio.

A **Visão Transacional** (camada operacional) gerencia riscos relacionados aos processos, sistemas, contratos e unidades de negócios da Companhia, considerando o impacto específico em cada área. Este tipo de risco detalha e complementa os riscos corporativos estando a eles associados como fatores de risco, conforme ilustrado abaixo:



Fonte: EY (Ernst Young)

Alinhamento Estratégico e Modelo Integrado

O gerenciamento de riscos é parte integrante do processo de elaboração dos objetivos estratégicos e está diretamente alinhado com estes objetivos, estabelecendo um ciclo integrado e virtuoso de retroalimentação entre as linhas de defesa da Companhia para uma cobertura mais ampla dos fatores de riscos internos e externos diante dos resultados esperados.

A estrutura de gestão de riscos apoia a integração da governança, em todos os níveis, atividades e funções significativas, englobando as mais diversas áreas e especialidades, atuando com sinergia para proteger o negócio e suportar a liderança no monitoramento e adequação tempestiva de sua estratégia frente as eventuais alterações no ambiente de riscos.

Fonte: The IIA (Modelo de Três Linhas de Defesa 2020)

Papéis e Responsabilidades

O gerenciamento de riscos não é um evento isolado de responsabilidade de uma única área, mas faz parte de um processo dentro da estrutura da Companhia e, por isso, requer o engajamento de áreas distintas, devendo ser realizado em todos os níveis (estratégico, tático e operacional). Abaixo listamos papéis e responsabilidades dos principais agentes do processo de gestão de riscos na Oi.

CONSELHO DE ADMINISTRAÇÃO (CA)

- Estabelecer valores, princípios e conduta requerida da Administração na Gestão de Riscos ("*Tone at the Top*");
- Aprovar a Política de Gestão de Riscos, definir o Apetite ao Risco da Companhia e as diretrizes estratégicas que devem ser seguidas;
- Avaliar periodicamente a exposição da Companhia a riscos e a eficácia dos sistemas de gerenciamento de riscos, dos controles internos e do sistema de integridade/conformidade.

COMITÊ DE AUDITORIA, RISCOS E CONTROLES (CARC)

- Supervisionar o sistema de gerenciamento de riscos, monitorar as exposições a risco da Companhia e, nesse âmbito, requerer as informações necessárias para subsidiar a avaliação dessa exposição e da efetividade das atividades mitigatórias relacionadas;
- Suportar o Conselho de Administração em assuntos relativos a avaliações de risco dos negócios e dos mecanismos internos de controle;
- Avaliar a efetividade e zelar pela independência e adequação dos recursos (humanos, tecnológicos e financeiros) alocados ao processo e sistema de gerenciamento de riscos;
- Avaliar em conjunto com a Diretoria, ao menos anualmente, as políticas e procedimentos com relação à avaliação e gerenciamento dos riscos.

CONSELHO FISCAL (CF)

- Conhecer os riscos da Companhia e definir/dialogar com os agentes integrantes do processo de gestão de riscos sobre os tipos, formatos e periodicidade da informação de que necessita para cumprir seu dever de fiscalização buscando reunir dados para subsidiar a formação de sua opinião sobre os atos de gestão;

DIRETOR PRESIDENTE (CEO)

- Responsável final pela Gestão dos Riscos, deve zelar pela governança e bom funcionamento da função de gestão de riscos da Companhia, provendo os recursos necessários para assegurar sua efetividade, fornecendo liderança e direcionamento estratégico, bem como apoiando sua execução e considerando seus insumos no processo decisório.

COMITÊ DE GESTÃO (CdG), COMITÊ DE COMPLIANCE E REDIR (REUNIÃO DE DIRETORIA)

Compostos pelos principais executivos da Alta Administração (Diretores N1), incluindo os diretores estatutários (REDIR), exercem a função de Comitês Executivos de Riscos. Suas principais atribuições são:

Validar e monitorar a execução das políticas e o cumprimento das normas de gestão de riscos, fazer o acompanhamento dos resultados de indicadores-chave e dos maiores riscos da Companhia, orientando quando houver a necessidade de tomada de decisão.

DIRETOR DE COMPLIANCE E RISCOS

Na atual estrutura organizacional da companhia, o Diretor de Compliance e Riscos exerce também a função de Diretor de Riscos (*CRO - Chief Risk Officer*) e Controles Internos, tendo reporte funcional ao Diretor Presidente (CEO) e independência é garantida pelo reporte ao CA, CARC e Conselho Fiscal. Entre suas principais atribuições estão:

- Disseminar a cultura e promover a integração da gestão de riscos na Companhia;
- Participar do planejamento estratégico sob a ótica do gerenciamento de riscos;
- Liderar a implantação de um modelo eficiente de gestão de riscos, incluindo metodologia, processos e sistemas de gerenciamento de riscos;
- Avaliar de forma o nível de exposição aos riscos e grau de maturidade e efetividade da Gestão de Riscos da Companhia, bem como colaborar na discussão sobre o Apetite ao Risco;

- Acompanhar as mudanças da criticidade dos Riscos Corporativos, bem como da efetividade dos planos de ação de mitigação de risco, remediações de gaps e tratamento de causa-raiz e efeitos;
- Efetuar reporte ao CdG, REDIR, CARC e CA acerca da Gestão dos Riscos Corporativos Prioritários.

GERÊNCIA DE GESTÃO DE RISCOS E CONTROLES

- Responsável pela gestão de riscos e controles, implementação e manutenção da política;
- Atuar como um integrador e facilitador das unidades de negócio nos assuntos de gestão de risco;
- Estabelecer e manter atualizada a documentação, informações e metodologia de Gestão de Riscos, assim como padrões e mecanismos de controle associados;
- Elaborar, revisar e manter atualizada a Régua de Probabilidade e Impacto;
- Acompanhar, analisar e reportar sobre mudanças na criticidade dos Riscos;
- Suportar e monitorar o processo de identificação e avaliação dos Riscos da Companhia;
- Apoiar o Risk Owner na gestão, controle e definição do plano de resposta aos Riscos;
- Criar e monitorar indicadores e níveis de exposição dos Riscos (KRI - *Key Risk Indicator*);
- Atualizar e revisar o mapeamento de Riscos junto aos executivos da Companhia sempre que houver atualizações no planejamento estratégico da Companhia ou sempre que fatos relevantes ocorrerem.

RISK OWNERS (DONOS DO RISCO)

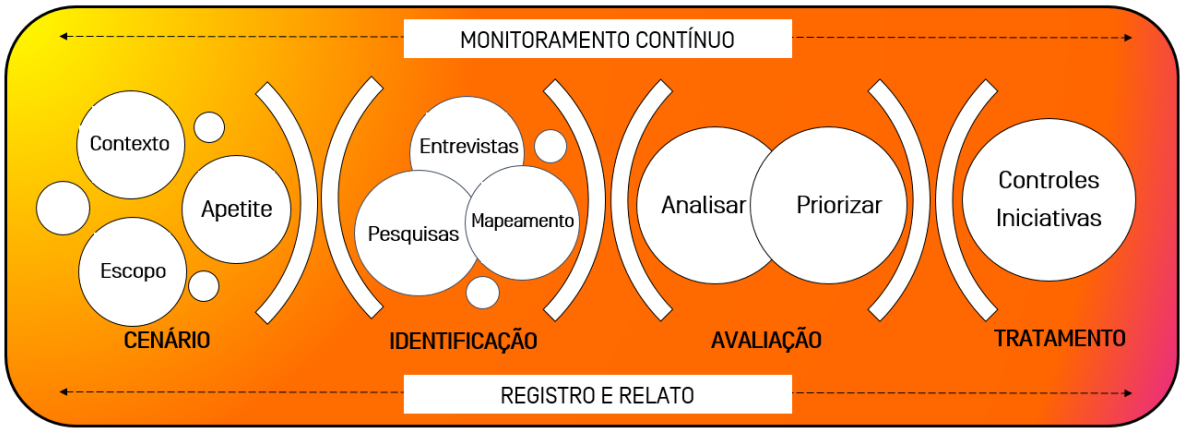
São os diretores e demais executivos responsáveis imediatos pelos riscos, entre suas principais responsabilidades estão:

- Avaliar e validar os Riscos Corporativos sob sua responsabilidade;
- Gerenciar estes riscos e acompanhar tempestivamente os resultados dos indicadores atrelados;
- Implantar ações necessárias para a mitigação dos riscos juntamente com as demais áreas envolvidas;
- Informar à área de Gestão de Riscos Corporativos as mudanças na Probabilidade e/ou Impacto do Risco ou sobre qualquer alteração na característica do mesmo;
- Informar à área de Gestão de Riscos Corporativos ao identificar Riscos não mapeados e tratados.
- Preencher e manter atualizados formulários e ferramentas de gestão de riscos.

Processo de Gestão de Riscos

A Gestão de Riscos é um processo estruturado e segue as etapas demonstradas a seguir:

Framework Oi de Gestão de Riscos

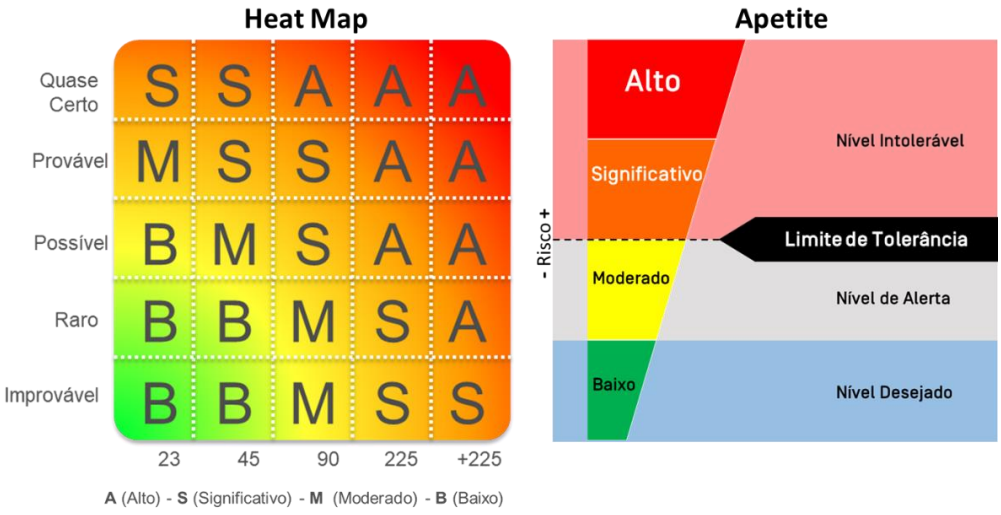


Cenário (Contexto e Escopo)

Nesta primeira etapa é realizado um levantamento de informações e estudo do **contexto externo** (ambiente financeiro, econômico, regulatório, socioambiental e relações com os *stakeholders*) e **contexto interno** (governança, estrutura organizacional, estratégia, processos, sistemas, contratos, relatórios de auditoria e outras avaliações disponíveis) para definição de **escopo**, isto é, atividades e temas críticos que serão objeto de mapeamento, chegando assim aos cenários de risco a serem melhor avaliados.

Apetite ao Risco

O Apetite ao Risco é uma declaração do mais alto nível da Organização (Conselho de Administração) sobre o quanto a companhia está disposta a aceitar de riscos para atingimento de seus objetivos. Composto pelos níveis de risco "Desejável, Alerta e Intolerável", ele estabelece os limites dentro dos quais o Conselho espera que a Administração opere, e determina parâmetros para análise dos riscos, bem como serve de base para priorização e decisão do tratamento (resposta) adequado.



O ***Heat Map*** acima estabelece a classificação do risco com base em uma análise (real ou estimada) de probabilidade (chance de materialização) e impacto (em R$MM) que será melhor detalhada no tópico a seguir. Ao lado dele o **Apetite** define o limite de tolerância aos riscos como sendo **inaceitáveis** casos com nível de exposição ao risco "**Alto**" e "**Significativo**".

Além dos aspectos quantitativos resultantes da análise de impacto e probabilidade, também são considerados no Apetite parâmetros qualitativos como julgamento profissional e as seguintes assertivas:

• A Oi não tolera a falta de conformidade e/ou má conduta de executivos, colaboradores ou terceiros com leis, regras e regulações aplicáveis;

• A Oi não tolera negligências operacionais que afetem os níveis de serviços dos seus clientes;

• A Oi não tolera desperdício de recursos e atos que possam causar dano ao seu patrimônio, de terceiros, ao patrimônio público ou ao meio ambiente;

• A Oi não tolera exposição negativa de sua marca que possa afetar sua imagem, reputação, atividades do negócio e partes interessadas.

Identificação de Riscos

Com base no resultado do cenário de risco são identificados, dentro do escopo determinado acima, quais riscos podem ajudar ou impedir a Oi no alcance de seus objetivos, bem como seus responsáveis (Risk Owners).

Para **encontrar**, **reconhecer** e **descrever** os riscos, a Oi utiliza entrevistas com executivos e conselheiros, coleta de dados, análise de evidências, documentos, pesquisas e validações junto as áreas técnicas envolvidas. Como resultado haverá uma lista de riscos associada ao escopo e ao cenário definido.

Categorização do Riscos

Para fins de categorização, os Riscos Corporativos na Oi devem ser divididos da seguinte forma:

Categoria	Descrição
Estratégico	Associados com as decisões estratégicas da Companhia para atingir os seus objetivos de negócios e/ou decorrentes da falta de capacidade ou habilidade da empresa para proteger-se ou adaptar-se a mudanças no ambiente. Exemplos: Riscos de perdas de participação de mercado ("Market share"), condições e preço de ações, compras e aquisições de empresas, etc.
Financeiro	Potencial impacto em receitas ou despesas podendo impactar o fluxo de caixa, indicadores econômicos e o resultado (lucro ou prejuízo), ocasionar em perdas ou causar distorções significativas nas demonstrações financeiras.
Compliance	Potencial impacto decorrente de descumprimento de normas internas, leis, regulamentos, compromissos voluntários ou processos movidos por partes interessadas. Dentre eles, destacamos riscos de corrupção, fraude, socioambientais, mudanças climáticas, legal, setorial, regulatório e derivados de desvios de conduta ética.
Operacional	Potencial impacto decorrente de problemas operacionais, como falhas em sistemas e procedimentos internos gerando consequências em produtos e serviços ao cliente.

Avaliação do Risco

Análise (Impacto e Probabilidade)

A análise de riscos deve determinar o **Nível de Exposição ao Risco** (Alto, Significativo, Moderado ou Baixo) já considerando controles e iniciativas implementadas (risco residual real).

Este Nível de Exposição ao Risco é apurado através da avaliação conjunta de critérios de **probabilidade** (histórico de ocorrência ou projeção estimada da possível materialização dos fatores de risco) e **impacto** (percepção sobre as consequências derivadas da ocorrência do risco).

Para **análise da probabilidade** de materialização do risco são utilizados dois critérios:

1. Frequência - risco com registro de materialização e histórico de ocorrências.

Escala	Frequência
Quase Certo (5)	< 1mês
Provável (4)	> 1mês ≤ 1ano
Possível (3)	> 1ano ≤ 3 anos
Raro (2)	> 3 anos ≤ 5 anos
Improvável (1)	> 5 anos

2. Projeções – risco sem registro de materialização e que devem ser estimados.

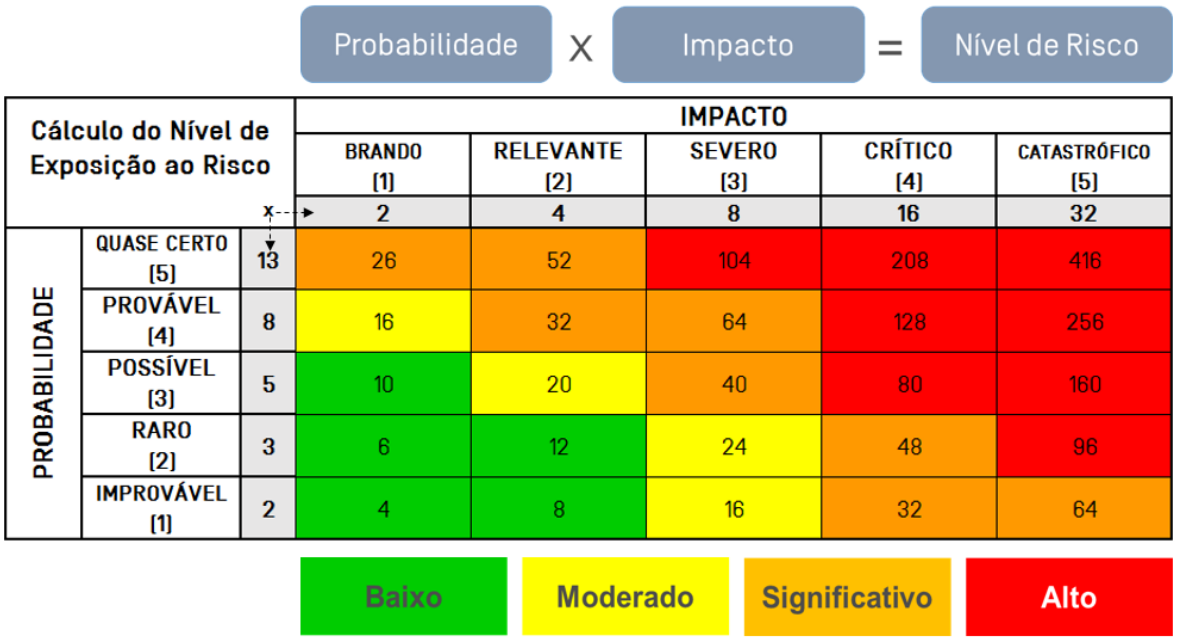
Escala	Projeção
Quase Certo (5)	> 80,01%
Provável (4)	> 50% ≤ 80%
Possível (3)	> 20% ≤ 50%
Raro (2)	> 5% ≤ 20%
Improvável (1)	< 5%

Vale ressaltar que os parâmetros de frequência e projeção acima são réguas iniciais que serão melhor analisadas em conjunto pelo *Risk Owner* e área de Compliance no momento da avaliação dos riscos, estando sujeitos a adequação para melhor enquadramento da probabilidade real ou estimada aplicável a cada caso.

Para **análise de impacto** leva-se em consideração os parâmetros detalhados abaixo, sendo o resultado final a maior pontuação obtida na análise dos vetores Financeiro, Compliance, Operações e Imagem.

ESCALA	VETOR PRINCIPAL	VETORES AUXILIARES		
	FINANCEIRO (EBITDA)	COMPLIANCE (Legal, Regulatório e Integridade)	OPERAÇÕES (Telecom e TI)	IMAGEM (Reputação e Credibilidade)
CATASTRÓFICO (5)	Maior que R$225MM (Acima de 5% do EBITDA)	• Decisões judiciais ou administrativas resultando em grandes penalizações, multas ou proibição da prestação de serviços; e elevada necessidade de provisionamento de despesas, garantias ou desembolso de caixa; • Perda de receita decorrente de restrições ou remoção de capacidade/licença para operar, intervenção regulatória significativa e impedimento de participação em licitações; • Redução de notas de crédito, perda de investimento, prisão de membros da Administração ou Conselho, corrupção, fraude, danos socioambientais; • Deficiências materiais nos controles internos.	• Paralisação da empresa como um todo e/ou perda crítica de capacidade de gerenciamento das operações, redes e sistemas da organização; • Redução nos níveis de serviço maiores que 10% das metas ou novos produtos/promoções atrasados por anos. • Comprovado vazamento em grande escala de informações próprias (financeiras, estratégicas, staff ou board) ou de terceiros (clientes, fornecedores e parceiros);	• Visibilidade negativa massiva em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional, nacional e/ou internacional (variação acima de 50% do volume de menções à companhia); • Mais de 96 horas (4 dias) de exposição negativa e massiva sem visibilidade para o posicionamento da companhia; • Potencial alto de mobilização massiva, envolvendo danos a vidas, denúncias com risco de sanções, falhas operacionais de larga escala e/ou outros temas críticos; • Aumento exponencial das reclamações (acima de 50%) e perda de clientes (acima de 5% da base) com possível movimento público de boicote à companhia.
CRÍTICO (4)	Até R$225MM (5% do EBITDA)	• Processos de larga abrangência que possam culminar na imposição de sanções e penalidades de órgãos fiscalizadores, regulatórios, organizações intergovernamentais, associações profissionais e institutos amplamente reconhecidos; • Restrições parciais sobre a capacidade de operar e algum nível de intervenção regulatória; • Pontos de atenção Legal/Regulatória com início de vigência no curto prazo, e necessidade de projetos estruturantes de elevado CAPEX; • Deficiências significativas nos controles internos.	• Interrupções significativas nas operações da empresa e/ou alta perda de capacidade de gerenciamento das operações, redes e sistemas da organização, • Redução nos níveis de serviço em até 10% das metas ou novos produtos/promoções atrasados por meses; • Vazamento parcial de informações próprias (financeiras, estratégicas, staff ou board) ou de terceiros (clientes, fornecedores e parceiros);	• Visibilidade negativa expressiva em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional, nacional e/ou internacional (variação de 25% a 50% do volume de menções à companhia); • Mais de 72 horas (3 dias) de exposição negativa e expressiva sem visibilidade para o posicionamento da companhia; • Potencial significativo de mobilização massiva, envolvendo danos a vidas, denúncias com risco de sanções, falhas operacionais de larga escala e/ou outros temas críticos; • Aumento significativo das reclamações (20% a 50%) e perdas de clientes (3% a 5%).
SEVERO (3)	Até R$90MM (2% do EBITDA)	• Não conformidades ou desvios de conduta aplicadas por órgãos externos, com necessidade de estabelecer provisão de multas/indenizações ou ajustamento de conduta, mas passível de remediação; • Pontos de atenção Legal/Regulatória de início de vigência no médio prazo, e necessidade de correções internas (com custos adicionais) para adequação; • Efetiva deficiência nos controles internos.	• Interrupções moderadas nas atividades da empresa e/ou perda moderada da capacidade de gerenciamento das operações, redes e sistemas da organização; • Redução nos níveis de serviço de até 5% das metas ou novos produtos/promoções atrasados por semanas; • Suspeita de vazamento de informações próprias (financeiras, estratégicas, staff ou board) ou de terceiros (clientes, fornecedores e parceiros);	• Visibilidade negativa de médio alcance em canais institucionais e/ou institucionais, mídia online e/ou offline, local e/ou regional, nacional e/ou internacional (variação de 10% a 25% do volume de menções à companhia); • Mais de 36 horas de exposição negativa sem visibilidade para o posicionamento da companhia; • Potencial moderado de mobilização massiva, envolvendo denúncias refutadas pela companhia, falhas operacionais e/ou outros temas críticos; • Aumento considerável das reclamações (5% a 20%) e perda de clientes (1% a 3% da base).
RELEVANTE (2)	Até R$45MM (1% do EBITDA)	• Não conformidades ou desvios de conduta em apuração por órgãos externos com potencial aplicação de multas/indenizações, mas sem necessidade de provisionamento. • Pontos de atenção Legal/Regulatória de início de vigência no longo prazo, e necessidade de pequenas correções internas (sem custos adicionais) para adequação; • Potencial conflito de interesses ou vulnerabilidades nos controles internos.	• Interrupções restritas nas atividades da empresa e/ou baixa perda de capacidade de gerenciamento das operações, redes e sistemas da organização; • Redução nos níveis de serviço menores que 5% das metas ou novos produtos/promoções atrasados por dias; • Potencial vazamento de informações próprias (financeiras, estratégicas, staff ou board) ou de terceiros (clientes, fornecedores e parceiros);	• Visibilidade negativa de pouco alcance em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional, nacional e/ou internacional (variação de 2% a 10% do volume de menções à companhia); • Mais de 12h de exposição negativa sem visibilidade para o posicionamento da companhia; • Potencial baixo de mobilização massiva; • Aumento das reclamações (até 5%) e perda de clientes (abaixo de 1% da base).
BRANDO (1)	Até R$23MM (0.5% do EBITDA)	• Não conformidades ou desvios de conduta de baixo impacto (remediáveis) aplicadas por áreas internas resultando em advertências, ações preventivas e implementação de pequenas melhorias.	• Interrupções limitadas em áreas ou departamentos específicos da empresa, sem comprometimento da continuidade das atividades; • Redução nos níveis de serviço menores que 2% das metas ou novos produtos/promoções atrasados por horas). • Vazamento interno (remediável) de informações próprias (financeiras, estratégicas, staff ou board) ou de terceiros (clientes, fornecedores e parceiros);	• Visibilidade negativa pontual em canais institucionais e/ou pessoais, mídia online e/ou offline, local e/ou regional, nacional e/ou internacional (variação de até 1% do volume de menções à companhia); • Exposição negativa sem recorrência significativa; • Sem potencial de mobilização massiva; • Sem variação no volume de reclamações ou perda de clientes.

O cálculo se dá pela atribuição de ratings de avaliação a serem preenchidos na Matriz de Riscos (de 1 a 5) que associados a fatores ponderados (pesos) são multiplicados e resultam em um coeficiente que posiciona o risco no *Heat Map*, conforme ilustrado abaixo.



Cálculo do Nível de Exposição ao Risco			IMPACTO				
			BRANDO [1]	RELEVANTE [2]	SEVERO [3]	CRÍTICO [4]	CATASTRÓFICO [5]
		x →	2	4	8	16	32
PROBABILIDADE	QUASE CERTO [5]	13	26	52	104	208	416
	PROVÁVEL [4]	8	16	32	64	128	256
	POSSÍVEL [3]	5	10	20	40	80	160
	RARO [2]	3	6	12	24	48	96
	IMPROVÁVEL [1]	2	4	8	16	32	64

Baixo | Moderado | Significativo | Alto

A utilização de pesos por escala visa assegurar destaque aos casos de maior probabilidade e impacto.

Priorização dos Riscos

Concluída a análise e obtida a classificação do risco, bem como verificado se o mesmo está ou não aderente ao Apetite estabelecido, ele é enquadrado em uma matriz de priorização através da qual é definida a estratégia de mitigação mais adequada (ações imediatas ou programadas a curto, médio e longo prazo) e as linhas de reporte para acompanhamento.

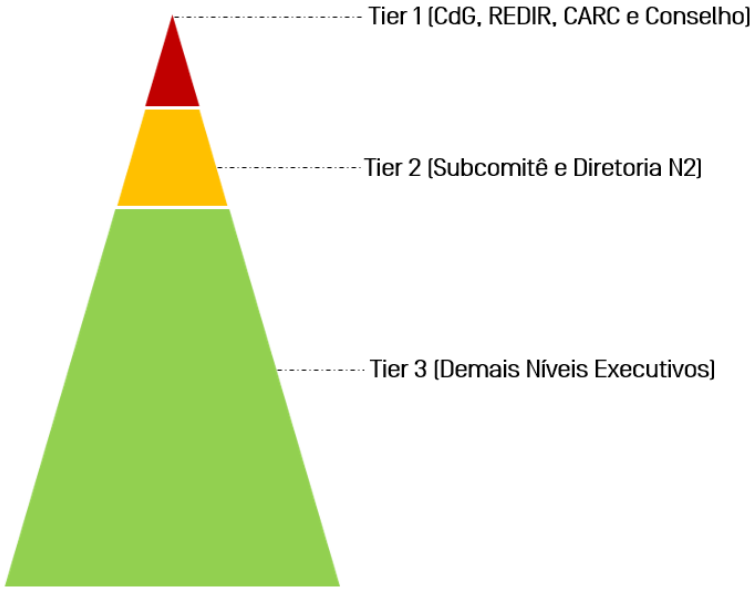
- **Riscos Altos e Significativos:** São riscos acima do Apetite ao Risco e demandam ação gerencial prioritária para eliminar a componente de risco ou reduzir seu impacto e/ou frequência. Devem ser quantificados e monitorados regularmente para direcionar continuamente as estratégias de mitigação. No caso de Riscos de baixa probabilidade e alto impacto ("Cisne Negro") devem ser estabelecidos planos de contingência;
- **Riscos Moderados:** São riscos de menor criticidade devido ao menor nível de impacto no valor do negócio, porém se caso seja de elevada frequência, requer atividades específicas e atenção da gerência na manutenção de respostas e controles para manter o impacto global em nível baixo, ou reduzi-lo sem custos adicionais. Demandam monitoramento para acompanhamento de seu nível. Caso subam, passam a estar acima do Apetite e demandar ação gerencial obrigatória.
- **Riscos Baixos:** Riscos de baixo impacto e frequência, gerenciados no curso das atividades das áreas de negócio, porém não havendo necessidade de monitoramento contínuo.

Linhas de Reporte

A Oi definiu também níveis de priorização para reporte de acordo com o resultado da análise dos riscos:

- **Riscos Corporativos "Tier 1" -** Compreendem os riscos mais estratégicos da Companhia. Trata-se de grupo de riscos com potencial impacto no resultado e continuidade dos negócios (requer atenção da Alta Administração e Conselho);
- **Riscos Corporativos "Tier 2" -** Derivados dos Riscos Corporativos de 1º nível ou com impacto significativo no resultado e continuidade dos negócios (requer a atenção da diretoria executiva);

  Riscos Corporativos "Tier 3" - Derivados dos Riscos Corporativos de 2º nível ou com impacto de baixo a moderado no resultado e continuidade dos negócios (requer a atenção dos gestores imediatos responsáveis pelos riscos).



É importante destacar que trata-se de uma classificação dinâmica, isto é, que pode se alterar conforme o resultado do monitoramento dos níveis de risco relacionados, e que quaisquer riscos que ameacem ultrapassar o Apetite estabelecido ou cujo acompanhamento seja requisitado pela Alta Administração e Conselho, serão objeto de reporte independente do *tier* a que estiver associado.

Tratamento e Resposta aos Riscos

As Áreas de Negócio devem desenvolver ações preventivas e corretivas para responder de forma apropriada, efetiva e mitigar os riscos da Companhia, para isso é necessário:

(A) Definir o tipo de resposta ao Risco - Uma estratégia de definição de resposta ao risco deve contemplar as respostas a seguir:

(B.1) Aceitar - Esta estratégia é adotada quando não é possível ou prático responder ao risco utilizando as outras estratégias. Quando a Alta Administração decide por aceitar o risco, significa que estão

concordando em enfrentar o risco, se e quando ele ocorrer. Um plano de contingência emergencial ou plano de solução paliativo devem ser desenvolvidos para essa eventualidade.

Via de regra são definidas ações para tratar todos os riscos identificados, ou cuja avaliação final ficou abaixo do risco residual esperado. Excepcionalmente, de forma fundamentada e conforme governança e alçada competente estabelecida no Regulamento de Riscos Corporativos (REG-881), é aprovado um **TAR (Termo de Aceitação ao Risco).** Trata-se de um "de acordo" dos diretores responsáveis (N1 e N2 envolvidos) formalizando que não haverá uma ação/iniciativa em função, por exemplo, de inviabilidade técnica ou financeira, custo x benefício da solução entre outros fatores.

Vale ressaltar que não se aplica TAR para casos com nível de exposição ao risco acima do Apetite ao Risco da Companhia ou apontados por Auditorias como *Material Weakness (MW) e Significant Deficiency (SD*). Além disto, todo TAR é reportado e submetido à apreciação do CARC.

(B.2) Compartilhar/Transferir - Envolve encontrar outra parte que esteja disposta a assumir a responsabilidade e arcar com os impactos do risco, caso ocorra (ex: seguros, títulos e garantias).

(B.3) Evitar - O risco pode ser evitado através da remoção da causa do risco ou ao executar a operação de uma forma diferente, porém ainda assim em linha com o alcance dos objetivos da empresa. Nem todos os riscos podem ser evitados/eliminados, e esta abordagem pode ser onerosa.

(B.4) Reduzir - A mitigação de riscos reduz a probabilidade e/ou o impacto de um evento de risco adverso para um limite aceitável (risco residual esperado) por meio da implantação de controles e iniciativas.

Nesta fase deve-se selecionar e implementar as melhores opções de resposta ao risco, avaliar a eficácia desta resposta, decidir se o risco remanescente é aceitável e, se for aplicável, realizar tratamentos adicionais. Deve-se balancear benefícios, custos, esforços, vantagens e desvantagens da implementação. Sendo possível:

- Realizar análises adicionais para melhor compreensão do risco;
- Aprimorar os controles e iniciativas existentes, e avaliar a necessidade de novas implementações;
- Contratação de seguro para compartilhamento do riscos e retenção monitorada;

Para maior detalhamento dos mecanismos de resposta ao risco (controles e iniciativas) vide o Regulamento de Controles Internos (REG-895).

Monitoramento Contínuo

A Oi realiza monitoramento e análise crítica permanente do seu ambiente de riscos e controles associados, incluindo testes e acompanhamento de indicadores (KRI - *Key Risk Indicator*) para medir a eficácia da mitigação e aderência ao Apetite e tolerância estabelecidos. O monitoramento pode ser realizado por meio de atividades contínuas, avaliações independentes (auditorias internas e externas) e auto avaliações.

Registro e Relato

Todas as etapas do processo de gestão de riscos devem ser registradas e ter sua documentação suporte e evidências armazenadas no sistema iBPMS, resultando em uma Matriz de Riscos e Controles por área, com

informações disponíveis a qualquer tempo para suportar a tomada decisão, melhorar as atividades de gestão e auxiliar na interação necessária para efetiva prevenção e mitigação dos riscos.

Apesar de haver um ciclo periódico de revisão dos riscos ativos e da identificação de novos riscos ou reavaliação dos existentes poder ocorrer tempestivamente (por evento), em regra eles serão reportados mensalmente para o Diretor Presidente, bimestralmente para o CARC, e semestralmente para o CA, podendo haver reporte em menor frequência caso necessário, incluindo outros fóruns (CdG e REDIR) em reuniões ordinárias/extras.

Este reporte será realizado através de um *dashboard* com a relação dos principais riscos e suas interdependências, status da implementação e efetividade de controles para mitigação, bem como eventuais alterações de cenário e atualização dos níveis de exposição.

Obs. Imagem meramente ilustrativa do modelo utilizado

Responsabilização (Accountability)

As sanções pelo descumprimento desta Política, incluindo a não observância ao Apetite estabelecido, seguirão o regime disciplinar da Diretoria de Gente, podendo ser executadas por meio de advertência verbal, escrita, suspensão ou rescisão do contrato de trabalho, sem prejuízo de eventual abertura do processo judicial. Também poderão ser impactadas notas individuais (metas) do programa de bônus, na avaliação discricionária dos executivos envolvidos em eventual descumprimento ou negligência no gerenciamento de riscos.

As infrações, quando identificadas, serão registradas e reportadas aos órgãos de governança competentes pelas Diretorias de Compliance ou Auditoria Interna, conforme aplicável.

Aprovação e Vigência

Este documento foi aprovado pelo Conselho de Administração em sua reunião ordinária de 28 de Outubro de 2020 , revoga versões anteriores e tem vigência de 18 meses, devendo ser revisado após este período.