GESTÃO DE RISCOS CORPORATIVOS

O presente documento foi redigido de acordo com o Código de Ética e Conduta, Programa de Anticorrupção, Política de Conflito de Interesses e os Princípios Gerais do Controle Interno do Grupo Telecom Itália.

QUADRO DE FORMALIZAÇÃO

	Nome	Função
ELABORADO POR:	Paulo Vinícius Beliene Duarte	Risk & Compliance – Enterprise Risk Management
	Mayara da Rocha Pinheiro	Risk & Compliance – Enterprise Risk Management
	Ana Carolina Ferreira Conde	Risk & Compliance – Enterprise Risk Management
VERIFICADO POR:	Marcia Regina Cavalcante	Risk & Compliance - Governance & Operational Compliance
	Gustavo Brantes	Risk & Compliance - Processes & Financial Compliance
	Rodrigo Ferreira Abdon	PC&O - Organizational Development – Processes Design & Improvement Programs
	Fabiane Ferreira Caldeira	PC&O - Organizational Development –Organizational Architecture
	Luiz Guilherme Almaraz	Risk & Compliance – Enterprise Risk Management
	Simone Paulino de Barros	Legal & Corporate Affairs - Corporate Affairs & Staff Legal Partner
APROVADO POR:	Claudio Creo	Risk & Compliance
	Gustavo Barrese	PC&O - Organizational Development
COMUNICADO:	Maria Antonietta Russo	People, Culture & Organization
	Mario Girasole	Regulatory Institut. and Press Relations
	Anna Carolina Meireles de Oliveira	Regulatory Institut. and Press Relations - Envir., Social & Governance
	Luca Fadda	Audit

Todos os direitos reservados

A cópia deste documento não é válida em meio impresso.

INFOGRÁFICO – RESUMO

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.

HISTÓRICO DAS REVISÕES

N° Versão	Descrição	Data
00	Emissão Inicial.	26/06/2012
01	Adequações do Documento.	28/06/2013
02	Novo processo ERM – Enterprise Risk Management.	25/09/2014
03	Adequações do Documento.	25/11/2016
04	Adequação à nova metodologia de processos.	06/12/2018
05	Adequações do Documento.	02/06/2020
06	Revisão Geral do processo de Gestão de Riscos Corporativos	05/05/2025

Todos os direitos reservados

A cópia deste documento não é válida em meio impresso.

ÍNDICE

QUADRO DE FORMALIZAÇÃO 2
1. DESTINATÁRIOS 6
2. OBJETIVO E CAMPO DE APLICAÇÃO 6
3. DIVULGAÇÃO 7
4. REFERÊNCIAS 7
5. DESCRIÇÃO GERAL DO PROCESSO E DAS RESPONSABILIDADES 8
6. GLOSSÁRIO 11
7. ANEXOS 13

PREMISSAS

O processo de Gestão de Riscos Corporativos está estruturado com base nos seguintes princípios fundamentais:

- **Objetivo Geral do Processo:** O processo de Gestão de Riscos Corporativos tem como finalidade fornecer suporte às decisões estratégicas da alta administração, por meio da identificação, priorização, classificação, resposta e monitoramento dos principais riscos da companhia, alinhando-se aos objetivos estratégicos estabelecidos no Plano Industrial.
- **Metodologia:** A avaliação e mensuração de riscos é conduzida utilizando uma abordagem integrada que combina critérios qualitativos e quantitativos, assegurando uma análise robusta e objetiva dos riscos, que permita o entendimento dos principais riscos enfrentados pela companhia.
- **Sinergia:** A Gestão de Riscos Corporativos fomenta a colaboração e a integração entre todos os níveis da organização, combinando conhecimentos técnicos e de negócios. Além disso, fortalece continuamente a interação entre as partes interessadas, promovendo uma gestão de riscos mais eficaz e identificando oportunidades por meio de uma abordagem integrada e colaborativa.
- **Melhoria Contínua e Excelência:** O processo de Gestão de Riscos Corporativos segue as melhores práticas nacionais e internacionais, baseadas em normas e diretrizes de referência para a gestão de riscos. Trata-se de um processo dinâmico e evolutivo, focado na melhoria contínua, adaptando-se às mudanças no ambiente interno e externo, incorporando aprendizados adquiridos e atendendo às necessidades da organização e de seus stakeholders.

1. DESTINATÁRIOS

Todas as funções do grupo TIM no Brasil.

2. OBJETIVO E CAMPO DE APLICAÇÃO

Este documento tem como objetivo formalizar:

- Os princípios gerais do processo de Gestão de Riscos Corporativos;
- As funções do processo e suas responsabilidades.

A Gestão de Riscos é uma ferramenta estratégica essencial para a proteção e criação de valor para a Empresa. Neste contexto, a TIM S.A, adotou um modelo que permite identificar e gerenciar os riscos corporativos de forma homogênea, destacando potenciais sinergias entre as funções envolvidas no Sistema de Controles Internos da companhia, e considerando as particularidades de cada cenário de risco.

Portanto, o processo de Gestão de Riscos Corporativos tem como objetivo a gestão eficaz dos riscos, a fim de:

- Estabelecer uma base sólida de avaliação dos principais riscos corporativos, a fim de apoiar a tomada de decisões e os processos de planejamento da companhia;

- Auxiliar a empresa no gerenciamento dos riscos corporativos, possibilitando maior eficácia no atingimento dos objetivos estratégicos;
- Incentivar uma abordagem proativa na gestão de riscos corporativos;
- Aumentar o nível de conscientização da companhia em relação ao gerenciamento de riscos corporativos;
- Aprimorar a identificação e o monitoramento de ameaças e oportunidades;
- Melhorar a governança e fortalecer a confiança das partes interessadas;
- Evitar ou reduzir prejuízos para a companhia;
- Prevenir ou minimizar a materialização e possíveis impactos dos riscos corporativos.

3. DIVULGAÇÃO

O conteúdo deste documento será divulgado através de disponibilização de infográfico (Simplifica TIM) nos canais internos da Cia. para todos(as) os(as) colaboradores(as), além de e-mail para os responsáveis pelas funções de nível 1.

4. REFERÊNCIAS

- Gestão por Processos – PL.001;
- Gestão e Mapeamento de Processos – POP.002;
- Aprovar Processos Empresariais – IO.003;
- Mapa de Macroprocessos TIM;
- Classificação e Gestão das Informações – PL.051;
- Modelo Organizacional da TIM S.A;
- Manual Sistema de Gestão Antissuborno e Anticorrupção;
- Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018;
- Código de Defesa do Consumidor;
- RGC - Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações;
- Código de Ética e Conduta da TIM S.A.;
- POP.370 – Ciclo de Avaliação dos Riscos Corporativos
- Regulamento do Novo Mercado da B3;
- Resolução CVM n° 53 – 15.10.2021;
- IBGC – Gerenciamento de Riscos Corporativos_2017;

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.

- Referências Internacionais:
  - Internal Control –Integrated Framework -COSO 2013;
  - COSO ERM-Integrating with Strategy and Performance, 2017;
  - Lei Sarbanes Oxley Act;
  - ISO 31000 - Gestão de riscos – Diretrizes.

5. DESCRIÇÃO GERAL DO PROCESSO E DAS RESPONSABILIDADES

5.1. Conceito de Riscos e Oportunidades:

Eventos podem gerar impactos negativos, positivos, ou, até mesmo, ambos. Os eventos com impactos negativos são considerados **riscos**, que exigem avaliação e resposta da administração para garantir que não prejudiquem o alcance dos objetivos da Companhia. Já os eventos com impactos positivos são classificados como **oportunidades**, com o potencial de contribuir favoravelmente para o atingimento dos objetivos e apoiar a criação de valor para a Companhia.

5.2. Descrição Geral do Processo:

O processo de Gestão de Riscos Corporativos é realizado, no mínimo, anualmente, com objetivo de avaliar o perfil de risco da Companhia e monitorar sua evolução ao longo do tempo. Trata-se de um processo cíclico, que deve estar em linha ao Plano Industrial, contemplando as seguintes etapas:

- **Identificação e Priorização:** consiste na identificação de eventos e fatores internos e externos que possam representar riscos reais ou potenciais, com capacidade de impactar negativamente as estratégias e os objetivos da companhia. Esta etapa inclui a revisão do Dicionário de Riscos Corporativos, e a priorização dos riscos que serão avaliados no ciclo atual. As principais técnicas utilizadas incluem:
  - Captura de riscos e tendências de mercado por meio de pesquisa de informações públicas e externas à TIM;
  - Captura de riscos e sensibilidades para o negócio através de entrevistas com stakeholders chaves da empresa (ex: executivos, membros dos Comitês e Conselho, Auditoria Interna, Compliance, entre outros);

Adicionalmente, caso possível, podem ser utilizadas outras ferramentas para identificação e priorização dos riscos, como pesquisas a concorrentes e empresas de estruturas similares, bem como a análise de dados históricos e indicadores de risco para identificar tendências. Por fim, cabe ressaltar que o Dicionário de Riscos Corporativos pode ser revisado a qualquer momento, caso necessário.

- **Classificação:** consiste na avaliação do nível de exposição dos riscos identificados e priorizados, levando em consideração critérios de impacto e vulnerabilidade. O modelo de avaliação desses critérios segue parâmetros qualitativos e quantitativos definidos na metodologia vigente, sendo aplicados conforme as particularidades de cada risco. Os resultados são compilados e compartilhados

com as partes interessadas, com o suporte da equipe de Enterprise Risk Management (ERM), juntamente com os Risk Owners e outros agentes de risco. Os riscos são então posicionados no Mapa de Riscos.

- **Plano de Resposta:** consiste na avaliação e definição de respostas para mitigar os riscos identificados e priorizados. Durante esta fase, o Risk Owner, com o apoio da área de Risk & Compliance - Enterprise Risk Management, elabora estratégias para reduzir a exposição do risco. As possíveis respostas aos riscos incluem: aceitar, reduzir/mitigar, transferir ou evitar.
- **Monitoramento:** consiste no acompanhamento contínuo da evolução dos riscos e dos planos de resposta. Esta etapa inclui a supervisão das ações em andamento para mitigação dos riscos, a avaliação da eficácia das respostas e a revisão da exposição ao risco após a execução das medidas definidas. Ao longo de todo o ciclo, a área de Risk & Compliance - Enterprise Risk Management realiza reportes das atividades ao Comitê Executivo de Riscos, Conselho de Administração, CAE e CCR.

5.3. Papéis e Responsabilidades:

A Gestão de Riscos Corporativos envolve diversas funções dentro da estrutura organizacional da empresa.

Abaixo, apresentamos o fluxo de comunicação e as responsabilidades das principais partes envolvidas:

- Conselho de Administração:
  - Aprovar as diretrizes estratégicas e as políticas de gestão de riscos corporativos;
  - Orientar de forma estratégica e garantir o fortalecimento das atividades de gestão de riscos corporativos;
  - Acompanhar os resultados da identificação, priorização, classificação e resposta dos riscos corporativos;
  - Avaliar se a Governança de Riscos Corporativos da empresa é adequada e possui recursos suficientes.

- Presidente
  - Fornecer liderança e direcionamento aos altos executivos, estabelecendo os valores, os princípios e as principais políticas (aprovadas pelo Conselho de Administração) que constituem o alicerce do modelo de riscos e do sistema de controles internos;
  - Estar ciente dos riscos inerentes às operações, das respostas a esses riscos e das melhorias de controles necessárias, além do status das iniciativas em andamento;
  - Estabelecer e colocar em prática o tom e nível de maturidade esperados pelo Conselho de Administração em relação ao modelo de gestão de riscos corporativos;
  - Promover uma cultura de gestão de riscos corporativos na companhia;

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.

- Reunir periodicamente a diretoria executiva para revisar suas responsabilidades quanto à gestão dos riscos corporativos;
- Garantir a adequação da estrutura (recursos humanos, financeiros e sistemas) destinada ao processo de gestão de riscos corporativos.

- Comitê Executivo de Riscos
  - Garantir que os riscos sejam adequadamente considerados no estabelecimento da estratégia e dos objetivos da companhia;
  - Analisar e aprovar a metodologia de gestão de riscos corporativos, e suas posteriores atualizações;
  - Acompanhar e supervisionar o processo de gestão de riscos corporativos;
  - Acompanhar as revisões do Dicionário de Riscos Corporativos, de acordo com os ciclos de gestão de riscos corporativos;
  - Acompanhar a definição da lista de riscos a serem priorizados para avaliação em cada ciclo de gestão de riscos corporativos;
  - Acompanhar os resultados de classificação dos riscos corporativos;
  - Acompanhar a definição das estratégias de mitigação dos Planos de Resposta;
  - Acompanhar a implementação das ações mitigatórias assim como a evolução do nível de exposição dos riscos.

- Área de Enterprise Risk Management
  - Propor a metodologia corporativa de gestão de riscos, fundamentada em uma visão integrada e sistêmica das atividades da companhia;
  - Desenvolver, testar e implantar os modelos e metodologias para avaliação e gestão de riscos corporativos;
  - Elaborar o planejamento e assegurar a operacionalização da gestão de riscos corporativos, considerando todas as dimensões da estrutura definida, englobando atividades estratégicas, táticas e operacionais;
  - Identificar e alertar à Administração para questões emergentes e para as mudanças no cenário de riscos;
  - Elaborar, treinar e disseminar a cultura de gestão de riscos corporativos na companhia;
  - Recomendar os processos e procedimentos para a gestão dos riscos prioritários;

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.

- Atuar como verificador da correta gestão de riscos da companhia e informar ao Comitê Executivo de Riscos e ao Conselho de Administração os resultados de suas avaliações através de relatórios periódicos;
- Assessorar as áreas funcionais e de negócios na identificação e na avaliação do impacto e vulnerabilidade dos diversos tipos de riscos;
- Propor, junto aos Risk Owners, os riscos prioritários da companhia para avaliação no ciclo;
- Realizar avaliação dos riscos com base nos critérios de classificação de impacto e vulnerabilidade, e consolidar os resultados para posicionamento no Mapa de Riscos.
- Analisar, em conjunto com os Risk Owners, as estratégias de mitigação dos riscos
- Suportar as áreas na definição dos planos de resposta;
- Executar as tarefas para um adequado monitoramento dos riscos prioritários, informar e discutir com o Comitê Executivo de Riscos os resultados de suas avaliações através de relatórios periódicos;
- Reportar formalmente ao Comitê Executivo de Riscos, Conselho de Administração, CAE e CCR o progresso e os resultados dos ciclos de gestão de riscos.

- Risk Owners
  - Participar ativamente na identificação e avaliação dos riscos da companhia com apoio da área de Enterprise Risk Management;
  - Definir, com auxílio da área de Enterprise Risk Management, plano de resposta para os riscos priorizados;
  - Implementar e dar visibilidade do desenvolvimento das ações estabelecidas no plano de resposta aprovado;
  - Comunicar prontamente à área de Enterprise Risk Management quaisquer desvios ou necessidades de ajustes nos planos;
  - Definir, monitorar e dar visibilidade de indicadores para os riscos priorizados.

6. GLOSSÁRIO

- **Agentes de risco:** São colaboradores designados pelo Risk Owner para apoiar na execução das atividades de gestão de riscos. Suas responsabilidades incluem a coleta de informações, monitoramento dos riscos, implementação de ações de mitigação e comunicação contínua sobre a evolução dos riscos, conforme as diretrizes estabelecidas pelo Risk Owner.

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.

- **CdA:** Conselho de Administração, órgão de deliberação colegiada, exerce a administração superior da Companhia.
- **CAE:** Comitê de Auditoria Estatutário, órgão colegiado de assessoramento, vinculado diretamente ao Conselho de Administração.
- **CCR:** Comitê de Controle e Risco, órgão colegiado de assessoramento, vinculado diretamente ao Conselho de Administração.
- **Comitê Executivo de Riscos**: Comitê formado pelo Presidente e Vice-Presidentes para supervisão das definições metodológicas e execução do processo de Gestão dos Riscos Corporativos, mediante agendamento de pauta no Staff do CEO.
- **CoSO – The Committee of Sponsoring Organization of the Treadway Commission**: em português: Comitê das Organizações Patrocinadoras da Comissão Treadway. O CoSO é uma organização sem fins lucrativos, dedicada a melhoria dos relatórios financeiros, sobretudo pela aplicação da ética e efetividade na aplicação e cumprimento dos controles internos e é patrocinado pelas cinco das principais associações de classe de profissionais ligados à área financeira nos EUA.
- **CoSO - Enterprise Risk Management - Integrating with Strategy and Performance**: em português: CoSO - Gerenciamento de Riscos Corporativos - Integrado com a Estratégia e Performance. Framework de gerenciamento de riscos corporativos, organizado em cinco componentes de fácil compreensão que harmonizam diferentes pontos de vista e estruturas operacionais, melhorando a estratégia e tomada de decisões.
- **Indicador de Risco (KRI -** Key Risk Indicator**):** São os principais indicadores de riscos da companhia que sinalizam as causas das mudanças no nível de risco dos objetivos de negócio. Quando monitorados de forma eficiente, os KRIs ajudam a Companhia a tomar ações preventivas, reduzir perdas e identificar oportunidades de crescimento, proteção e criação de valor.
- **Monitoramento:** atividades contínuas, integradas nas operações de negócios, avaliações ou combinação de ambas, a fim de acompanhar e modificar, quando necessário, o processo de Gestão de Riscos Corporativos em função das mudanças que ocorrem no ambiente operacional do negócio.
- **Nível de Risco:** avaliação qualitativa / quantitativa do nível de risco (impacto x vulnerabilidade).
- **Nível de Impacto:** mensuração/identificação de impactos econômicos e/ou impactos estratégicos, legal e regulatório, imagem e reputação, satisfação do cliente, continuidade do negócio, socioambiental que um risco pode gerar à Companhia.
- **Nível de Vulnerabilidade:** identificação do nível de vulnerabilidade, através dos seguintes critérios: governança dos controles internos, registro de ocorrência e velocidade de resposta.
- **Oportunidade:** possibilidade de que um evento ocorra (externo ou interno à empresa), capaz de afetar positivamente a realização dos objetivos de negócio/corporativo.
- **Risco:** possível evento com capacidade de impactar negativamente o atingimento dos objetivos estratégicos. Os eventos podem estar relacionados a fatores internos, que refletem decisões de

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.

negócios (aspectos como infraestrutura, pessoal, processos e tecnologia) e fatores externos (aspectos econômicos, tecnológicos e de natureza ambiental e/ou sócio-políticos).

- **Risk Owner:** Responsável por identificar, avaliar, monitorar e gerenciar os riscos em sua área ou processo específico, assegurando a implementação das ações de mitigação e o acompanhamento contínuo dos riscos sob sua responsabilidade. O Risk Owner é sugerido pelo time ERM levando em consideração o escopo do risco/tema com posterior formalização ao Comitê Executivo de Riscos. Atualmente estão definidos como Risk Owners os responsáveis pelas funções de Nível 1 da Companhia.

7. ANEXOS

- ANEXO 1 – Código(s) do(s) Controle(s) Associado(s)

Todos os direitos reservados
A cópia deste documento não é válida em meio impresso.