Política de Gestão de Riscos

POLÍTICA CORPORATIVA

v3.0 - 2023

SUMÁRIO

DOCUMENTO PÚBLICO

As informações contidas neste documento podem ser divulgadas publicamente – incluindo clientes, fornecedores, prestadores de serviço, público em geral e mídias sociais – sem que causem algum dano à RTM.

SIGLAS, ABREVIAÇÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
Ação de mudança	Ações que envolvam definir os responsáveis por implementar mudanças para os departamentos, para garantir as condições impostas pelo programa de *compliance* a fim de que sejam bem compreendidas por todos.
Instâncias Externas de apoio à Governança	São as instituições encarregadas pela avaliação, auditoria e monitoramento independente e, nos casos em que disfunções são identificadas, encarregadas também pela comunicação dos fatos às instâncias superiores de governança
Organização	Grupo de pessoas e instalações com uma série de responsabilidades, autoridades e relacionamentos. Exemplo: Companhia, corporação, firma, empresa, instituição de caridade, profissional liberal ou associação, ou partes ou combinações destas
Partes Interessadas	Aqueles que possuem algum interesse nos resultados de uma organização Pessoa ou organização que pode afetar, ser afetada ou se perceber afetada por uma decisão ou atividade.
Processo	Atividade ou conjunto de atividades executados por uma organização, que produzam ou suportem um ou mais produtos ou serviços, inter-relacionadas ou interativas, que usam ou transformam entradas para entregar um resultado.
Risco	Efeito da incerteza nos objetivos. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças. Normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.
Risco Positivo	É a oportunidade que, se acontecer, irá trazer impacto positivo, gerando ganhos e melhorias.
Risco de Segurança	Risco associado ao ambiente digital de operações e suas vulnerabilidades: sistemas e dados que processam, transferem ou armazenam. Os mais comuns são: acesso não autorizado, ataques de negação de serviços, cibe espionagem, difusão de vírus/malware, destruição de recursos, violação de dados.
Risco de Conformidade	O risco de conformidade é a possibilidade de ocorrência de perdas resultantes de penalidades legais por não observância de regulamentos e legislações externas, bem como internas, ao qual a RTM se submete
Risco Estratégico	O risco estratégico é qualquer evento, seja ele interno ou externo, que possa impactar, de forma direta ou indireta, os objetivos estratégicos da RTM e suas estratégias
Risco Operacional	O risco operacional é a possibilidade de ocorrência de perdas resultantes de processos internos, pessoas, sistemas inadequados ou falhos, ou de eventos externos
Risco Financeiro	O risco financeiro é a possibilidade de ocorrência de perdas em decorrência de transações financeiras

1. INTRODUÇÃO

1.1. RESUMO

O documento Política de Gestão de Riscos visa descrever as diretrizes necessárias para o controle e monitoramento dos riscos inerentes ao negócio, buscando minimizá-los com o objetivo de proteger o patrimônio da instituição e, consequentemente, o patrimônio das partes interessadas.

1.2. APLICAÇÃO

Às empresas RTM:

- RTM Rede de Telecomunicações do Mercado Ltda; e
- RTM Infraestrutura em Tecnologia da informação Ltda.

1.3. REQUISITOS ESTATUTÁRIOS E REGULAMENTARES

- ABNT NBR **ISO 22.301** (Sistema de gestão da continuidade de negócios)
- ABNT NBR **ISO 27.001** (Requisitos para sistemas de gestão da segurança da informação)
- ABNT NBR **ISO 27.005** (Gestão de riscos de segurança da informação)
- ABNT NBR **ISO 31.000** (Diretrizes para gestão de riscos)
- BACEN **Resolução 4893** (Política de segurança cibernética para instituições autorizadas pelo Banco Central)
- **COBIT 2019** (Objetivos de controle de informação e tecnologia relacionada)
- **RISK IT** (framework complementar ao COBIT com diretrizes e práticas para auxiliar no gerenciamento de riscos
- relacionados a I&T)
- **LEI 13.709/18** (Lei Geral de Proteção de dados – LGPD)
- **NIST SP 800-37** (Estrutura de gestão de riscos para sistemas de informação e organização)
- **NIST SP 800-39** (Gerenciamento de riscos de segurança da informação)
- **NIST SP 800-53** (Controles de segurança e privacidade para sistemas de informação)
- **PCI DSS v3.2.1** (Padrão de segurança de dados da indústria de cartões de pagamento)
- **SWIFT SIP v3** (Programa de segurança do cliente da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais)

1.4. DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA

A Política de Gestão de Riscos está alinhada às demais políticas da RTM, dentre as quais destacamos:

2. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política de Gestão de Riscos descrevem as funções exercidas pelos colaboradores da RTM que atuam diretamente neste processo, além das devidas ações que são executadas para as demais áreas de negócio da RTM.

2.1. Alta Direção

Compete à alta direção as seguintes atribuições:

- Ser comprometida com a gestão de riscos, alocando os recursos necessários ao processo;
- Divulgar e apoiar internamente a área de Riscos;
- Deliberar sobre decisões estratégicas se comprometendo em desenvolver as análises dos riscos relativos a essas decisões;
- Estabelecer contextos externo e interno para Gestão de Riscos.

2.2. Comitê Estratégico de Governança, Riscos e *Compliance*

Compete ao comitê Estratégico de Governança, Riscos e *Compliance* a função de **direcionador estratégico e comunicador**, além das seguintes atribuições:

- Estabelecer as diretrizes para a Gestão de Riscos;
- Aprovar e revisar periodicamente a Estrutura de Gestão de Riscos e a política de Gestão de Riscos;
- Atribuir papéis, responsabilidades e alçadas;
- Acompanhar os resultados das atividades de gestão de riscos, incluindo as ações de monitoramento;
- Definir a estratégia de gestão de riscos;
- Revisar e aprovar a matriz de riscos da RTM;
- Realizar reuniões periódicas para avaliação dos pontos da Política de Gestão de Riscos e para as alterações necessárias;
- Aprovação do plano de tratamento de riscos;
- Avaliar a eficácia da estrutura de gestão de riscos.

2.3. DICOR – Diretoria Corporativa

- Aprovar a metodologia de Gestão de Riscos;
- Aprovar normas específicas para o cumprimento das diretrizes e do processo de gestão de riscos.

2.4. DIROP – Diretoria de Operações

- Aprovar a metodologia de Gestão de Riscos;
- Aprovar normas específicas para o cumprimento das diretrizes e do processo de gestão de riscos.

2.5. Gerência de Governança, Riscos e *Compliance*

Compete a área de GRC – Governança, Riscos e *Compliance*, as funções **de proprietária e gestora do processo** de Gestão de Riscos, além das seguintes atribuições:

- Participar da formulação e atualização da política de Gestão de Riscos;
- Monitorar o cumprimento dos papéis e responsabilidades de cada área integrante da estrutura de gerenciamento de riscos;
- Definir ferramentas para a Gestão de Riscos, em conjunto com a Gerência de Governança de TIC;
- Definir a metodologia para a Gestão de Riscos, em conjunto com a Gerência de Governança de TIC;
- Manutenir o processo de Gestão de Riscos;
- Monitorar os processos, riscos e controles mapeados e registrados na matriz de riscos;
- Elaborar as políticas e normas referentes à Gestão de Riscos;
- Revisar, atualizar e coordenar os planos referentes à Gestão de Riscos;
- Participar efetivamente na disseminação da cultura de riscos e na integração da Gestão de Riscos em todos os níveis hierárquicos da RTM.

2.6. Gerência de Governança de TIC

Compete a área de Governança de TIC a função de **co-gestora de riscos de TI & Riscos de Segurança,** além das seguintes atribuições:

- Participar da formulação e atualização da política de Gestão de Riscos, assim como das demais atividades e decisões de gestão de riscos, em conjunto com a Gerência de GRC.

2.7. Áreas de Negócio

Compete às áreas de negócios as seguintes atribuições:

- Identificar, reportar, analisar e avaliar os riscos de suas respectivas áreas de negócio;
- Responder aos riscos de acordo com os critérios estabelecidos pela RTM;
- Elaborar o plano de ação para mitigar os riscos;
- Implantar o plano de tratamento de riscos.

3. OBJETIVOS

A Política de Gestão de Riscos tem como principal objetivo fornecer as diretrizes gerais para minimizar os impactos negativos causados por quaisquer eventos que ofereçam riscos aos negócios da RTM.

4. METODOLOGIA

A metodologia de Gestão de Riscos implantada na RTM baseia-se nos princípios apresentados no item 1.3 – requisitos estatutários e regulamentares e traz opções de abordagem de riscos.

Figura 1 - Ciclo de vida da gestão de riscos

5. ESCOPO

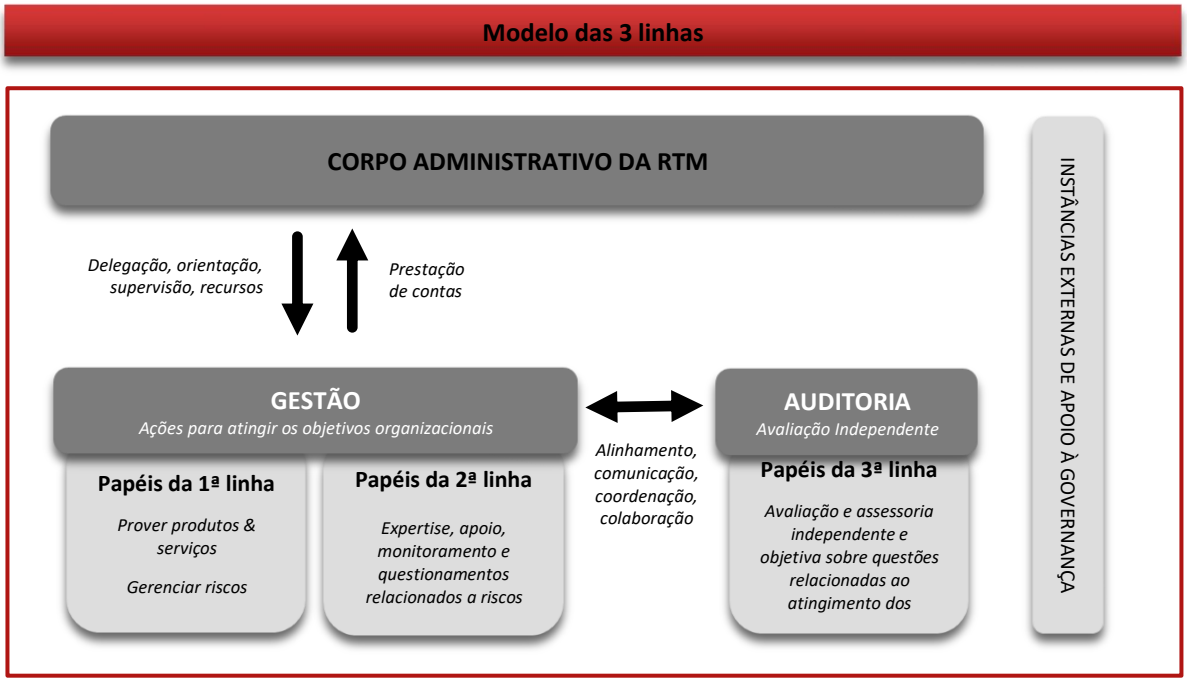
Buscando uma Gestão de Riscos baseada nas melhores ferramentas e boas práticas do mercado, a RTM adota, para a gestão de seus riscos, conforme a sua maturidade, as seguintes naturezas: estratégico, operacional, financeiro, segurança e de conformidade.

6. DIRETRIZES GERAIS

6.1. Estrutura de Gestão de Riscos

A estrutura de Gestão de Riscos definida pela RTM, baseada no modelo de 3 linhas do IIA, visa estabelecer, implementar, manter e aprimorar continuamente o processo de gestão de riscos, e se baseia nas seguintes diretrizes:

- A Gerência de Governança, Riscos e Compliance é designada como proprietária e responsável direta pela gestão do processo de Gestão de Riscos;
- São alocados recursos humanos com habilidade, experiência e competência em gestão de riscos;
- São realizadas ações de busca em legislações e guias de melhores práticas que assegurem a identificação dos requisitos a serem atendidos que se relacionem à Gestão de Riscos;
- Papéis e responsabilidades, além da atribuição de alçadas, são formalmente definidos, documentados e comunicados.



6.2. Conscientização, Educação e Treinamento

- Todos os colaboradores da RTM devem estar cientes da relevância e importância de suas atividades no escopo da Gestão de Riscos;
- O tema Gestão de Riscos deve ser incluído nas reuniões de equipe.

6.3. Melhoria Contínua

- O processo de Gestão de Riscos deve ser continuamente e sistematicamente monitorado e atualizado;
- As lacunas ou os riscos positivos identificados devem ser analisados criticamente e registrados, caso relevantes e adequados às circunstâncias;
- As ações de mudanças devem ser planejadas, analisadas e executadas;
- Uma vez implementadas, as melhorias devem contribuir para o aprimoramento da gestão de riscos.

7. DIRETRIZES ESPECÍFICAS

- Adoção das boas práticas de Governança Corporativa e dos princípios da Gestão de Riscos:
    - Gestão de Riscos como parte da cultura da organização;
    - Integração da gestão de riscos realizada conforme a maturidade da RTM frente à governança de seus processos;
    - Processo de Gestão de Riscos na RTM como de responsabilidade primária de todas as áreas de negócio, que constituem a primeira linha;
    - O exercício contínuo de identificação, avaliação e adoção de ações de mitigação de risco;

7.1. Processo de Gestão de Riscos

O Processo para Gestão de Riscos definido pela RTM se baseia no (a):

- Definição da metodologia para gestão de riscos, contendo os critérios definidos para classificação, análise, avaliação e aceitação dos riscos, que será detalhada no normativo interno específico;
- Definição da estratégia de monitoramento contínuo de riscos;
- Definição de um portifólio de ações e de gerenciamento de riscos;
- Estabelecimento e documentação do processo de tratamento dos riscos;
- Estabelecimento e documentação do processo de comunicação de riscos;
- Integração da Gestão de Riscos com o processo de Planejamento Estratégico da RTM, antecipando-se às ameaças que podem afetar os objetivos estratégicos, financeiros, operacionais, de segurança ou de conformidade;

7.2. Tratamento e Resposta aos Riscos

O processo definido pela RTM deve abranger as seguintes fases e atividades:

- Registro formal e aprovação dos riscos;
- Documentação dos resultados do tratamento dos riscos por meio da Matriz de Riscos;
- Avaliação da eficácia do tratamento de riscos;
- Especificação de requisitos para projetos e programas de implementação das ações de respostas aos riscos selecionados;
- Elaboração de um plano de tratamento de riscos, contendo as ações de respostas aos riscos;
- Priorização dos riscos para tratamento;
- Implementação das ações voltadas à resposta ao risco.

7.2.1. Identificação de Riscos

- Os riscos serão identificados, documentados e priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes para a RTM;
- A responsabilidade pela identificação dos riscos será da primeira linha, proprietários de processos.

7.2.2. Análise de Riscos

- Após identificados, os riscos serão analisados para que se possa compreender a sua natureza, características, impactos, consequências, probabilidade de ocorrência e dependências;
- Cenários de riscos serão elaborados e utilizados, e os cenários mais graves e de maior probabilidade de ocorrência deverão ser comunicados ao Comitê Estratégico de Governança, Riscos e Compliance.

7.2.3. Avaliação de Riscos

- A avaliação de riscos também incluirá as avaliações baseadas em cenários de indisponibilidade;
- O resultado da avaliação de riscos será documentado e comunicado.

7.2.4. Resposta aos Riscos

- Estabelecer controles para aceitar, evitar, compartilhar ou mitigar os riscos;
- Responder ao risco com base nos resultados das atividades de monitoramento contínuo, avaliações de risco e itens pendentes nos planos de tratamento de riscos.

8. PENALIDADES

Violações a este normativo estão sujeitas a sanções disciplinares estabelecidas pela RTM e Legislações Vigentes, e serão decididas caso a caso pelo Comitê Estratégico de Governança, Riscos e Compliance.

Para realizar uma denúncia de violação deste normativo deve-se utilizar o Canal de Denúncias da RTM (https://canal.ouvidordigital.com.br/rtm ou WhatsApp 31 8947-7889).

ANEXOS

I. Matriz de papéis e responsabilidades (RACI)

MATRIZ RACI

Nome do processo:	Gerenciar Riscos
Responsável pelo processo:	DICOR / Gerência de Governança, Riscos e Compliance
Responsável pela atualização do documento:	DICOR / Gerência G.R.C / Controles Internos
Última atualização:	24/04/2023

➤ **Papéis e Responsabilidades**

Quem foi designado para a execução, conclusão e entrega da atividade	R	Responsável
Quem tem autoridade para tomar decisões e validar formalmente uma entrega	A	Responsabilizado
Quem deve ser consultado e/ou participar da decisão no momento da execução da atividade	C	Consultado
Quem deve receber as informações sobre o início da atividade e/ou sobre os resultados	I	Informado

Gestão de Riscos Atividades ↓	DGER - Diretoria Geral	Conselho de Acionistas	DICOR - Diretoria Corporativa	DIROP - Diretoria de Operações	DNEG - Diretoria de Negócios	Comitê Estrat. Gov., Riscos e Compliance	Comitê Executivo de TI	Ger. de Governanç, Riscos e Compliance	Gerência de Governança de TIC	Área de Negócio
Estabelecer as diretrizes para a Gestão de Riscos (Listar o conjunto de orientações para estabelecimento de ações e prioridades relacionadas à Gestão de Riscos)	C		A			R		I		
Definir papéis e responsabilidades (Definir formalmente papéis e responsabilidades dentro do Processo de Gestão de Riscos)			A	A		R		I	I	I
Definir alçadas de aprovação (Definir formalmente alçadas de aprovação para tomada de decisões dentro do Processo de Gestão de Riscos)						R		I	I	I
Definir escopo e limites (Definir o escopo e os limites das atividades dentro do Processo de Gestão de Riscos)	I		A			C		R	C	
Identificar e documentar os requisitos legais e regulatórios (Realizar busca ativa dos requisitos legais e regulatórios e documentar)			A					R	C	
Assegurar a alocação de pessoal capacitado (Assegurar o envolvimento de pessoal capacitado nas atividades do Processo de Gestão de Riscos)			A	A				R	R	
Aprovar estrutura de Gestão de Riscos (Aprovar a estrutura de Gestão de Riscos com a sua Política)	I					R		I	I	
Definir metodologia de Gestão de Riscos (Definir um método de Gestão de Riscos adequado, incluindo critérios de: taxonomia, coleta, classificação, análise, avaliação, critérios de impacto, aceitação e significância do risco)			A			I		R	I	I
Definir portfólio de ações de resposta aos riscos (Definir e manter um inventário de atividades de controle para responder/mitigar o risco)			A			I		R		
Definir estratégias de monitoramento (Definir as estratégias de monitoramento do ambiente organizacional, interno e externo, e operacional)			A			I		R		I
Elaborar e documentar processos e procedimentos (Elaborar e documentar a Norma de Tratamento de Riscos)			A					R	C	I
Planejar, elaborar e documentar o Plano de Comunicação de Riscos (Processo de Comunicação de Riscos)			A			I		R		I
Definir ferramentas de Gestão de Riscos (Definir e assegurar a alocação de ferramentas à serem usadas na Gestão do Risco)			A			I		R	C	I
Identificar os riscos (Identificar os riscos na unidade organizacional respeitando o escopo e os seus limites)								A/C	A/C	R
Analisar os riscos (Analisar de forma criteriosa os riscos identificados)								A/C	A/C	R
Avaliar os riscos (Avaliar os riscos, identificados e analisados, os comparado com os critérios de aceitação e os priorizando)			A					R	R	I
Responder os riscos (Responder os riscos, podendo: aceitar, evitar, compartilhar, mitigar e remover a fonte do risco)			C	C				A	A	R
Avaliar a eficácia do tratamento de risco (Avaliar a eficácia do tratamento de riscos)						R		C	C	I
Priorizar os riscos (Priorizar os riscos de acordo com sua criticidade)						R		I		I
Realizar a elaboração do inventário de riscos (Processo de Perfil de Risco (Inventário))			A	A		I		R	C	I
Especificar requisitos para o Plano de Tratamento de Riscos (Especificar os requisitos para os riscos)			A					R	C	I
Elaborar o Plano de Tratamento de Riscos (Elaborar e documentar o plano de ação para mitigar os riscos)						A		C	C	R
Aprovar o Plano de Tratamento de Riscos de TI (Analisar e aprovar o Plano de Tratamento de Riscos de TI)	A	I		I		R	I	I	I	
Aprovar o Plano de Tratamento de Riscos (Analisar e aprovar formalmente o Plano de Tratamento de Riscos)	A/R		R		R	I		I		
Implementar o Plano de Tratamento de Riscos (Implantar as ações do Plano de Tratamento de Riscos)	A		A	A	A	I		I		R
Monitorar e atualizar o Plano de Tratamento de Riscos (Monitorar e atualizar os planos de acordo com os resultados de avaliação, de auditoria e/ou do monitoramento contínuo)			A			I		R		I
Coordenar os planos relacionados (Coordenar os planos relacionados a Gestão de Riscos)			A			I		R	C	
Gerir a Matriz de Riscos (Elaborar, revisar e atualizar a Matriz de Riscos)			A			I		R	C	I
Prover conscientização e treinamento em gestão de riscos Processo de Conscientização e Treinamento em Riscos)			A			I		R	C	I
Revisar e atualizar os mecanismos de acompanhamento e controle do processo (Revisar e atualizar os mecanismos de acompanhamento e controle avaliando as práticas e os processos existentes, para encontrar lacunas à serem preenchidas)			A			I		R	C	