DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

rtm

Política de Gestão de *Compliance*

POLÍTICA CORPORATIVA

v2.0 - 2023

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

SUMÁRIO

SIGLAS, ABREVIAÇÕES E DEFINIÇÕES 3
1. INTRODUÇÃO 5
2. PAPÉIS E RESPONSABILIDADES 6
3. OBJETIVOS 8
4. METODOLOGIA 8
5. ESCOPO 8
6. DIRETRIZES GERAIS 9
6.1. Estrutura de Gestão de Compliance 9
6.2. Conscientização, Educação e Treinamento 9
6.3. Melhoria Contínua 9
7. DIRETRIZES ESPECÍFICAS 10
7.1. Processo de Gestão de Compliance 10
7.2. Programa de Compliance 10
7.3. Programa de Integridade 11
7.3.1. Prevenção 11
7.3.2. Detecção 12
7.3.2.1. Auditoria e monitoramento 12
7.3.2.2. Denúncias 12
7.3.2.3. Investigação 12
7.3.3. Resposta 13
7.3.3.1. Sanções 13
8. PENALIDADES 13
ANEXOS 14
CONTROLES DO DOCUMENTO 15

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.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

SIGLAS, ABREVIAÇÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
Ação corretiva	Ação para eliminar a causa de uma não-conformidade em curso (real) e para evitar sua recorrência.
Ação preventiva	Ação para mitigar a causa de uma não conformidade iminente (potencial) e para evitar sua recorrência.
Ação de monitoramento	Consiste no acompanhamento contínuo, por parte de gestores e colaboradores, no desenvolvimento dos programas e políticas em relação a seus objetivos e metas.
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.
Compliance	Conjunto de mecanismos para atendimento a todas as obrigações de Compliance da organização Origina do verbo "comply", que significa Cumprir. Na tradução livre: Conformidade. É o conjunto de disciplinas a fim de cumprir e se fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da empresa.
Conduta	Comportamento e práticas esperados dos Colaboradores e Terceiros, que impactam os resultados para os clientes, fornecedores, mercados e comunidade.
Conformidade	Atendimento a um requisito.
Corrupção	Ato ou efeito de corromper; decomposição, suborno, adulteração, vício.
Cultura de integridade e *Compliance*	Valores, éticas, crenças e conduta que existem por toda a organização e interagem com as estruturas e os sistemas de controle da organização para produzir normas comportamentais que contribuem para o *Compliance.*
Não-conformidade	Não atendimento a um requisito, implicitamente ou explicitamente após sua identificação. Pode ser detectada internamente, por auditoria interna ou externa.
Objetivos de *Compliance*	Resultado a ser alcançado para atender todos os requisitos.
Obrigações de *Compliance*	Requisitos que uma organização mandatoriamente tem que cumprir, como também os que uma organização voluntariamente escolhe cumprir.
Oportunidade de melhoria	Ação objetivando o aumento da capacidade do atendimento aos requisitos.
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.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

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.
Programa de Integridade	Conjunto de mecanismos e ações de integridade com objetivo de estimular um comportamento íntegro na RTM, além de sanar desvios, fraudes, irregularidades e atos ilícitos praticados na organização.
Requisito	Necessidade ou expectativa que é declarada, geralmente obrigatória ou implícita.
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 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.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

1. INTRODUÇÃO

1.1. RESUMO

Esta política estabelece as diretrizes e funções do Programa de Compliance e Integridade da RTM.

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 37.301** (Sistema de Gestão de *Compliance*)
- ABNT NBR **ISO 27.001** (Requisitos para Sistemas de Gestão da Segurança da Informação)
- BACEN **Resolução 4893** (Política de Segurança Cibernética para instituições autorizadas pelo Banco Central)
- **COBIT 2019** (Objetivos de Controle de Informação e Tecnologia relacionada)
- **Lei 12.846/13** (Lei Anticorrupção ou Lei da Empresa Limpa)
- **Lei 13.709/18** (Lei Geral de Proteção de dados – LGPD)
- **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

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

2. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política de Gestão de Compliance descrevem as funções exercidas pelos colaboradores da RTM que atuam diretamente neste processo.

2.1. Alta Direção

Compete a Alta Direção a função de **apoiador**, além das seguintes atribuições:

- Demonstrar ativamente liderança e comprometimento para estabelecer, desenvolver, implementar, avaliar, manter e melhorar a Gestão de Compliance, com resultados por meio das suas ações e decisões;
- Assegurar que a presente política e os objetivos de Compliance estão estabelecidos e são compatíveis com a direção estratégica da organização;
- Encorajar um comportamento que crie e apoie o Compliance, de forma a prevenir e não tolerar comportamentos que o comprometam;
- Assegurar que os recursos necessários para o sistema de Gestão de Compliance estejam disponíveis.

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:

- Assegurar que o sistema de Gestão de *Compliance* seja analisado criticamente a intervalos planejados;
- Aprovar e revisar periodicamente a estrutura e a política e os planos de Gestão de *Compliance*;
- Definir escopo e limites para Gestão de *Compliance*;
- Aprovar normas específicas para o cumprimento das diretrizes e do processo de Gestão de *Compliance*;
- Atribuir papéis, responsabilidades e alçadas;
- Analisar resultados de auditorias e recomendações;
- Atuar como órgão disciplinar, analisando as supostas violações de regras e políticas praticadas pelos colaboradores.

2.3. DICOR – Diretoria Corporativa

Acompanhar os resultados das atividades de Gestão de *Compliance* nos processos corporativos.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

2.4. DIROP – Diretoria de Operações

Acompanhar os resultados das atividades de Gestão de *Compliance* em processos de TIC.

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 *Compliance*, além das seguintes atribuições:

- Definir metodologia e ferramentas para a Gestão de *Compliance*;
- Definir a estratégia de gestão e monitoramento contínuo de *Compliance*;
- Manutenir o macroprocesso de Gestão de *Compliance*;
- Elaborar as políticas, normas e planos referentes à Gestão de *Compliance*;
- Compilar as informações relacionadas à Gestão de *Compliance.*

2.6. Gerência de Governança de TIC

Compete a área de Governança de TIC a função de **gestora do processo** de Gestão de *Compliance* em Tecnologia da Informação e Comunicação, além das seguintes atribuições:

- Manutenir o processo de Gestão de *Compliance* em TIC;
- Elaborar as políticas, normas e planos referentes à Gestão de *Compliance* em TIC.

2.7. Áreas de negócio

A Compete as áreas de negócio a responsabilidade pelo *Compliance* dentro de seus processos, além das seguintes atribuições:

- Identificar, comunicar e executar as obrigações de *Compliance* relativas às suas operações;
- Assegurar que todos os seus processos estejam em conformidade com todas as regras de *compliance* estabelecidas;
- Analisar registros, designar responsáveis, planejar e executar as ações do Plano de Ação definido para tratamento das não-conformidades e oportunidades de melhoria, que poderão ser de responsabilidade de um ou mais líderes;
- Acompanhar a evolução do cumprimento da ação por intermédio de evidências objetivas até a respectiva avaliação de eficácia.

2.8. Colaboradores

- Qualquer Colaborador poderá identificar uma não-conformidade na sua área de atuação cabendo ao mesmo, obrigatoriamente, acionar seu gestor para oficializar a ocorrência, solicitar o registro e acompanhar a ocorrência no sistema.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

3. OBJETIVOS

A Política de Gestão de *Compliance* tem como objetivos:

- Apoiar os princípios de governança de *Compliance;*
- Estabelecer as principais diretrizes e responsabilidades relacionadas à Gestão de *Compliance*;
- Prevenir e/ou tratar quaisquer desvios ou inconformidades dentro do negócio.

4. METODOLOGIA

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

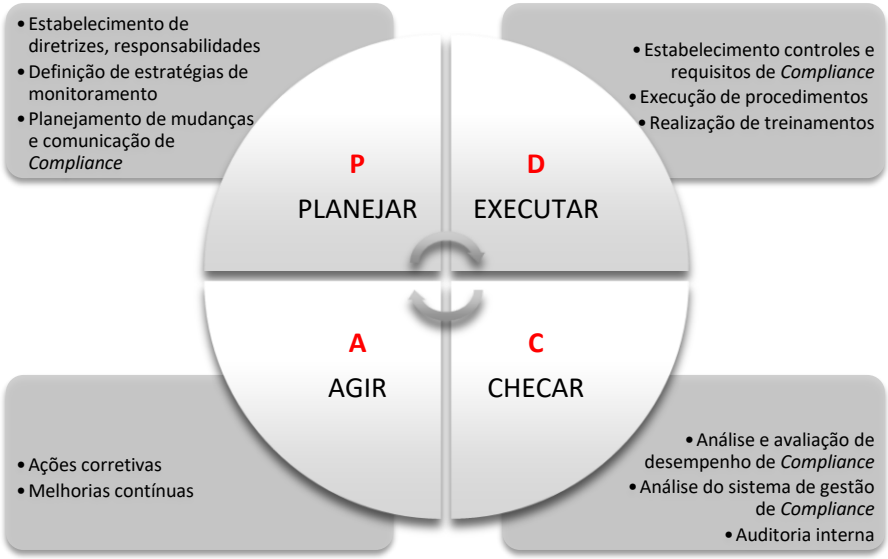

Figura 1 - Ciclo de vida da Gestão de Compliance

5. ESCOPO

O escopo abrange:

- Medidas de *Compliance* para o bom cumprimento dos requisitos legais, regulatórios e contratuais;
- Medidas de integridade para prevenir, detectar e remediar a ocorrência de atos indesejados.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

6. DIRETRIZES GERAIS

6.1. Estrutura de Gestão de Compliance

A estrutura de Gestão de *Compliance* definida pela RTM visa estabelecer, implementar, manter e aprimorar continuamente a Gestão de *Compliance*, de acordo com a sua maturidade, 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 Compliance;
- A Gerência de Governança de TIC é designada como responsável direta pelo gerenciamento do Compliance em Tecnologia da Informação e Comunicação;
- São alocados recursos humanos com habilidade, experiência e competência em Gestão de Compliance;
- Os objetivos de Compliance são especificados para as funções e níveis pertinentes;
- Papéis e responsabilidades são formalmente definidos, documentados e comunicados.

6.2. Conscientização, Educação e Treinamento

- Os programas de Conscientização, Educação e Treinamento devem seguir as diretrizes específicas estabelecidas para os temas;
- A RTM deve prover anualmente atividades de conscientização e/ou treinamento de compliance para os colaboradores que desempenham essas atividades, para as partes interessadas pertinentes e para as terceiras partes que atuam em seu nome e que possam causar um risco de compliance para a empresa.

6.3. Melhoria Contínua

- O processo de gestão de compliance deve ser continuamente e sistematicamente atualizado;
- As ações corretivas devem ser planejadas, analisadas e executadas.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

7. DIRETRIZES ESPECÍFICAS

7.1. Processo de Gestão de Compliance

O *Compliance* definido pela RTM se baseia no gerenciamento de:

- auditorias
- denúncias e investigações
- não-conformidades com os requisitos internos (processos organizacionais: políticas, normas, procedimentos, códigos), externos (leis, regulamentos, normas técnicas, padrões) e contratuais
- obrigações de *Compliance*

7.2. Programa de Compliance

- A gestão dos requisitos estatutários, regulamentares e contratuais é realizada pela Gerência de Governança, Riscos e Compliance e pela Gerência de Governança de TIC, por meio das áreas de Controles Internos;
- São realizadas ações de busca em legislações e guias de melhores práticas que assegurem a identificação dos requisitos externos;
- A integração dos requisitos estatutários, regulamentares e contratuais, com os processos de negócio da RTM, deve ser assegurada;
- Os sistemas de gestão da RTM, abaixo mencionados, devem ser analisados periodicamente para garantir sua adequação, suficiência e eficácia, no contexto dos objetivos estratégicos estabelecidos:
  - ✓ SGSI – Sistema de Gestão da Segurança da Informação
  - ✓ SGPI – Sistema de Gestão da Privacidade da Informação
  - ✓ SGQ – Sistema de Gestão da Qualidade
- Reuniões periódicas entre os gestores e a Alta Direção devem ser realizadas para manter o alinhamento das equipes e avaliar as não-conformidades, as oportunidades de melhoria e necessidades de mudanças nesses sistemas de gestão;
- Controles para gerenciar as obrigações de Compliance e riscos de conformidade associados devem ser documentados, mantidos, analisados criticamente de forma periódica e testados para assegurar a sua eficácia contínua;
- As não-conformidades devem ser registradas e tratadas a fim de identificar, monitorar e mitigar riscos internamente;
- As oportunidades de melhoria devem ser registradas e, caso implementadas, acompanhadas conforme detalhamento desse procedimento;
- Um plano deve ser formalizado, contendo as ações para tratamento das não-conformidades e oportunidades de melhorias identificadas;
- O planejamento das comunicações internas e externas, pertinentes ao sistema de Gestão de Compliance, deve ser realizado incluindo: o que comunicar, quando comunicar, com quem se comunicar e como se comunicar.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

7.3. Programa de Integridade

O Programa de Integridade da RTM será estruturado em observância aos pilares da Gestão de *Compliance* (prevenção, detecção e resposta) visando estimular um comportamento íntegro na organização.

7.3.1. Prevenção

Diretrizes para auxiliar na identificação de não conformidades, na análise de riscos de conformidade e na estruturação de regras que eliminem essas ameaças.

7.3.1.1. Liderança

- A alta direção deve ter participação ativa e pessoal na implementação do programa, além de assegurar que a cultura de integridade e *Compliance* seja entendida como um compromisso da organização e não somente dos gestores de governança;
- Todos os gestores devem conduzir e disseminar práticas de governança corporativa no ambiente corporativo, em todos os seus relacionamentos e processos, de maneira a evitar o risco de envolvimento em atos indesejados e escândalos que os levem a responder civil, penal e administrativamente.

7.3.1.2. Comunicação

- Um processo de comunicação eficaz, abrangendo todas as partes interessadas – órgãos reguladores, clientes, parceiros de negócio, fornecedores, serviços de emergência, entre outras – deve ser adotado;
- Os instrumentos normativos e demais documentações que tratam sobre integridade devem estar disponíveis em locais de fácil acesso a todos, interna e externamente a RTM.

7.3.1.3. Treinamento e conscientização

- Todos os colaboradores da RTM devem estar cientes da relevância e importância de suas atividades no escopo da Gestão de Compliance;
- A RTM deve organizar, periodicamente, treinamentos e eventos que promovam a conscientização sobre condutas éticas e de integridade.

7.3.1.4. Combate a atos ilícitos

- Regras de ética e de conduta devem ser estruturadas em documento próprio para explicitar o comportamento esperado de colaboradores e terceiros;
- Ações para detecção de atos ilícitos – corrupção, fraude, suborno, lavagem de dinheiro, conflito de interesses, brindes, terrorismo, entre outros – devem ser planejadas e implementadas;

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

- Políticas e demais instrumentos normativos, para mitigar os riscos de conformidade com fornecedores e terceiros, devem ser documentados e comunicados;
- Diligência apropriada deve ser estabelecida para contratação e supervisão de serviços terceirizados.

7.3.2. Detecção

Diretrizes para auxiliar no monitoramento das medidas e ações propostas.

7.3.2.1. Auditoria e monitoramento

- As estratégias de monitoramento contínuo do Sistema de Gestão de Compliance devem ser definidas;
- Deve ser realizado um levantamento prévio dos riscos relacionados às obrigações de compliance de RTM;
- Os riscos de conformidade devem ser identificados, analisados e avaliados baseado em um processo de gestão de riscos;
- O mapeamento e a identificação de atividades suspeitas, incluindo as de terceiros, devem ser realizados para evitar riscos de responsabilidade.

7.3.2.2. Denúncias

- Canais de denúncia, abertos e amplamente divulgados a colaboradores e terceiros, devem ser estabelecidos para comunicação de atos indesejados e desvios cometidos, além do aumento das possibilidades de ciência sobre as inconformidades. Esses canais devem contar com:
    - Os devidos mecanismos de proteção dos denunciantes de boa-fé e a proibição de retaliação;
    - Orientações de como, quando e onde fazer uma denúncia, além da possibilidade de realizá-la de maneira anônima;
    - Meios para que o denunciante acompanhe o andamento de denúncia;
    - Normas e procedimentos transparentes para se administrar uma denúncia, delimitando com exatidão as etapas e as responsabilidades de cada agente envolvido.

7.3.2.3. Investigação

- A detecção de indícios da ocorrência de atos indesejados e desvios cometidos deve levar a RTM a iniciar uma investigação interna, que servirá como base para que sejam tomadas as providências cabíveis;
- Confirmada a ocorrência do ato indesejado envolvendo a RTM, providências para assegurar a imediata interrupção das irregularidades devem ser tomadas e as ações de resposta ao ato devem ser executadas.

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

7.3.3. Resposta

Diretrizes para auxiliar na aplicação de sanções com o objetivo de educar, prevenir ou reprimir condutas irregulares.

7.3.3.1. Sanções

- A aplicação das sanções se fará necessária para a manutenção da legitimidade do sistema de Compliance. Portanto, os tipos de sanções e suas regras devem ser claras, formalizadas e amplamente divulgadas;
- Violação de regras de integridade serão analisadas e sujeitas as sanções administrativas, penais e civis;
- Medidas disciplinares devem ser aplicadas aos colaboradores como consequências da inobservância ou observância inadequada a um comportamento descrito nas políticas ou demais normativos corporativos;
- Medidas administrativas devem ser aplicadas à terceiros – clientes, fornecedores, prestadores de serviços e parceiros – como consequência de infrações ou irregularidades no cumprimento do contrato de prestação de serviços;
- O Comitê Estratégico de Governança, Riscos e Compliance atuará como órgão disciplinador, analisando as supostas violações de regras e descumprimento de normativos.

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/rtmou WhatsApp 31 8947-7889).

DocuSign Envelope ID: 9921ECF5-1ED0-4C71-9B09-64AE07D7E263

ANEXOS

Não há.