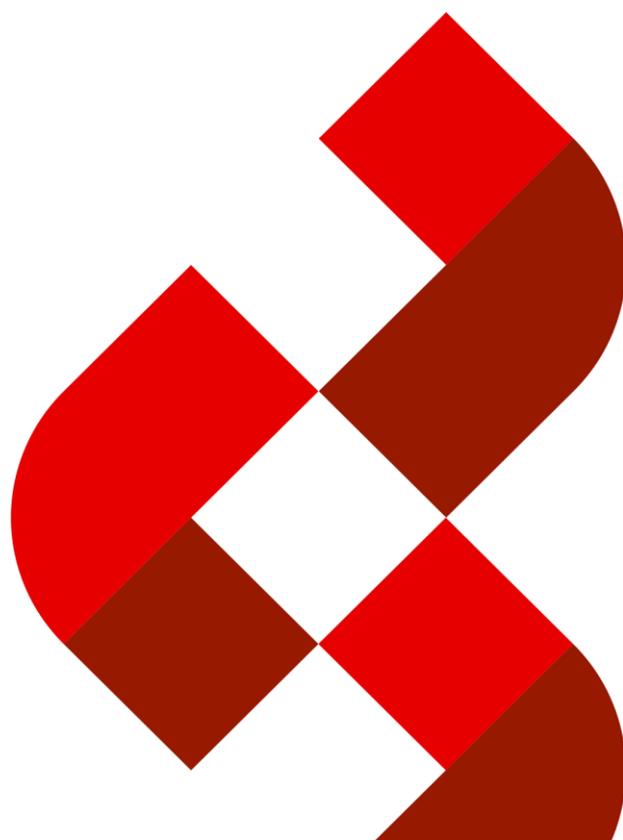




# Política de Gestão de Continuidade de Negócios

POLÍTICA CORPORATIVA

V2.1 - 2024





O *hub integrador* do  
mercado financeiro

## SUMÁRIO

SIGLAS, ABREVIACÕES E DEFINIÇÕES .....	3
1. INTRODUÇÃO .....	5
2. PAPÉIS E RESPONSABILIDADES .....	7
3. OBJETIVOS.....	12
4. METODOLOGIA.....	12
5. ESCOPO .....	13
6. MAPA DE PROCESSO DE NEGÓCIOS .....	14
7. DIRETRIZES GERAIS .....	15
<b>7.1. Estrutura de Gestão de Continuidade de Negócios</b> .....	15
<b>7.2. Conscientização, Educação e Treinamento</b> .....	15
<b>7.3. Melhoria Contínua</b> .....	15
8. DIRETRIZES ESPECÍFICAS .....	16
<b>8.1. Requisitos de Continuidade</b> .....	16
<b>8.2. Requisitos de Segurança da Informação</b> .....	16
<b>8.3. Ambientes de Redundância</b> .....	17
<b>8.4. Estratégias de Continuidade</b> .....	17
<b>8.5. Plano de Continuidade de Negócios - PCN</b> .....	18
<b>8.6. Testes</b> .....	19
9. PENALIDADES .....	19
CONTROLES DO DOCUMENTO.....	21

### DOCUMENTO PÚBLICO

As informações contidas neste documento podem ser divulgadas publicamente, incluindo clientes, fornecedores, prestadores de serviço, público em geral e mídias sociais



## SIGLAS, ABREVIACÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
<b>Análise de Impacto nos Negócios (BIA)</b>	Processo de analisar as funções de negócios e os efeitos que uma interrupção possa causar nelas
<b>Alta direção</b>	Pessoa ou grupo de pessoas que dirige e controla uma organização em seu nível mais alto
<b>Atividades críticas</b>	Atividades que devem ser executadas de forma a entregar os produtos e serviços fundamentais da organização que a permitam atingir seus objetivos mais importantes e sensíveis a tempo
<b>Ciclo de vida da gestão de continuidade de negócios</b>	Série de atividades que, coletivamente, abordam todos os aspectos e fases do programa de gestão de continuidade de negócios
<b>Contingência</b>	Planejamento e tratamento de situações indesejadas (eventos ou ocorrências que possam afetar a operação)
<b>Continuidade de Negócios</b>	Capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios, para conseguir continuar suas operações em um nível aceitável previamente definido
<b>Estratégia de continuidade de negócios</b>	Abordagem de uma organização que garante a sua recuperação e continuidade, ao se defrontar com um desastre, outro incidente maior ou interrupção de negócios
<b>Gestão de Continuidade de Negócios (GCN)</b>	Processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado
<b>Gestão de Riscos</b>	Desenvolvimento estruturado e aplicação de uma cultura de gestão, políticas, procedimentos e práticas às tarefas de identificação, análise e controle dos riscos
<b>Grupo RTM</b>	RTM Rede de Telecomunicações para o Mercado Ltda e RTM Infraestrutura em Tecnologia da Informação Ltda
<b>Impacto</b>	Consequência avaliada de um evento em particular
<b>Incidente</b>	Situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises
<b>Interrupção</b>	Evento, seja previsto (por exemplo, uma greve ou furacão) ou não (por exemplo, um blecaute ou terremoto), que cause um desvio negativo, imprevisto na entrega e execução de produtos ou serviços da organização, de acordo com seus objetivos
<b>Organização</b>	Grupo de pessoas e instalações com uma série de responsabilidades, autoridades e relacionamentos. Exemplo: <i>Companhia, corporação, firma, empresa, instituição de caridade, profissional liberal ou associação, ou partes ou combinações destas</i>



O *hub integrador* do  
mercado financeiro

<b>Partes interessadas</b>	Aqueles que possuem algum interesse nos resultados de uma organização
<b>Perda</b>	Consequência negativa
<b>Período máximo de interrupção tolerável</b>	Duração a partir da qual a viabilidade de uma organização será ameaçada de forma inevitável, caso a entrega de produtos e serviços não possa ser reiniciada
<b>Planejamento de contingência</b>	Desenvolvimento e manutenção de procedimentos acordados de forma prevenir, reduzir, controlar, mitigar e escolher ações a serem tomadas no caso de uma emergência
<b>Plano de Continuidade de Negócios (PCN)</b>	Documentação de procedimentos e informações desenvolvida, consolidada e mantida de forma que esteja pronta para uso caso ocorra um incidente, de forma a permitir que a organização mantenha suas atividades críticas em um nível aceitável previamente definido
<b>Produtos e serviços</b>	Resultados benéficos que uma organização fornece a seus clientes e partes interessadas, como produtos manufaturados, seguros automobilísticos, conformidade com regulamentações e benefícios comunitários
<b>Programa de gestão de continuidade de negócios</b>	Processos contínuos de gestão e governança que são suportados pela alta direção e que recebem os recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por meio de treinamentos, testes, manutenção e análises críticas
<b>Processo</b>	Atividade ou conjunto de atividades executados por uma organização que produzem ou suportem um ou mais produtos ou serviços
<b>Recursos</b>	Todos os ativos, pessoas, experiências, informação, tecnologia (incluindo o edifício e equipamento), premissas, suprimentos e informação (eletrônica ou não) que uma organização deve ter disponível para uso, quando necessário, a fim de operar e atingir seus objetivos
<b>Risco</b>	Algo que pode ocorrer e seus efeitos nos objetivos da organização
<b>Sistema de Gestão</b>	Sistema que estabelece e atinge políticas e objetivos
<b>SGCN</b>	Sistema que estabelece e atinge políticas e objetivos para a continuidade do negócio
<b>Tempo objetivado de recuperação (RTO – Recovery Time Objective)</b>	Tempo alvo para retomada da entrega de produtos ou serviços ou atividades após um incidente
<b>Testes</b>	Atividade no qual os planos de continuidade de negócios são exercitados parcial ou integralmente de forma a garantir que os planos contenham as informações apropriadas e produzam o resultado desejado quando postos em prática



## 1. INTRODUÇÃO

A RTM entende que deve estar preparada para minimizar os impactos financeiros, operacionais, legais e regulatórios ocasionados pela interrupção total ou parcial dos seus processos críticos de negócio, bem como a indisponibilidade de acesso físico ou lógico e de seus recursos humanos e tecnológicos críticos, de forma a garantir a confiabilidade, integridade e disponibilidade dos seus produtos e serviços aos seus clientes e ao mercado financeiro.

Ressaltamos que todos os procedimentos e documentos relacionados na Política de Continuidade de Negócios são alinhados com o comprometimento de melhoria contínua e estão aderentes as obrigações internas e externas, a missão, visão estratégica e valores da RTM.

### 1.1. RESUMO

O documento Gestão de Continuidade de Negócios visa descrever as diretrizes necessárias para prover a continuidade das operações da organização, após situações de indisponibilidade total ou parcial das suas funções vitais de negócio.

### 1.2. APLICAÇÃO

Em todo Grupo RTM:

- RTM Rede de Telecomunicações do Mercado Ltda
- RTM Infraestrutura em Tecnologia da Informação Ltda

### 1.3. REQUISITOS ESTATUTÁRIOS E REGULAMENTARES

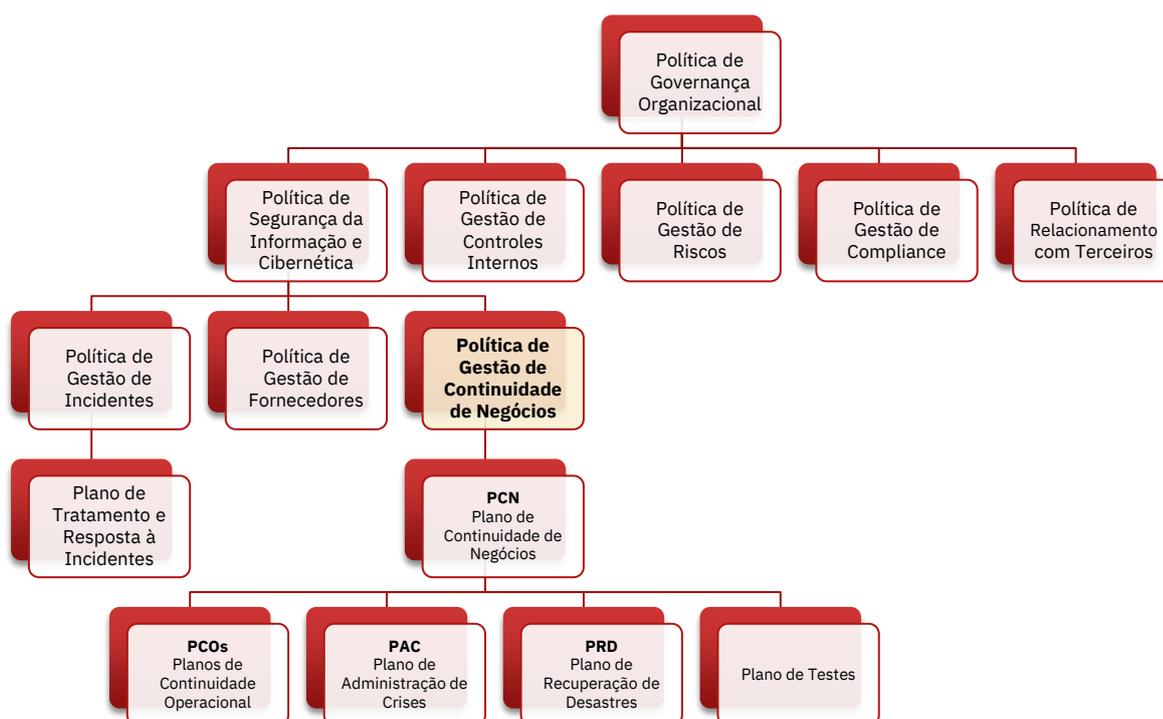
- ABNT NBR **ISO 22.301** (Sistema de gestão de continuidade de negócios)
- ABNT NBR **ISO/IEC 27.002** (Código de prática para controles de segurança da informação)
- BACEN **Resolução 4893** (Política de segurança cibernética para instituições autorizadas pelo Banco Central)
- BACEN **Resolução 304** (disciplina, no âmbito do Sistema de Pagamentos Brasileiro, o funcionamento dos sistemas de liquidação, entre outros)
- **COBIT 2019** (Objetivos de controle de informação e tecnologia relacionada)
- **NIST SP 800-34** (Guia de planejamento de contingência para sistemas de informação)
- **NIST SP 800-53** (Controles de segurança e privacidade para sistemas de informação)
- **PCI DSS v4.0** (Padrão de segurança de dados da indústria de cartões de pagamento)
- **SWIFT PSCF v2023** (Programa de segurança do cliente da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais)

## 1.4. DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA

A Política de Gestão de Continuidade de Negócios está alinhada as demais políticas da organização, dentre as quais destacamos as seguintes:

- Política de Governança Organizacional
- Política de Gestão da Controles Internos
- Política de Gestão da Riscos
- Política de Gestão da Compliance
- Política de Relacionamento com Terceiros (clientes, fornecedores, prestadores de serviço e órgãos públicos)
- Política de Segurança da Informação e Cibernética
- Política de Gestão da Incidentes

A Política de Gestão de Continuidade de Negócios irá reger os demais planos específicos, os quais deverão estar alinhados com a estratégia de continuidade de negócios definida para a RTM. Abaixo a relação entre a ela e as demais políticas e procedimentos internos associados.

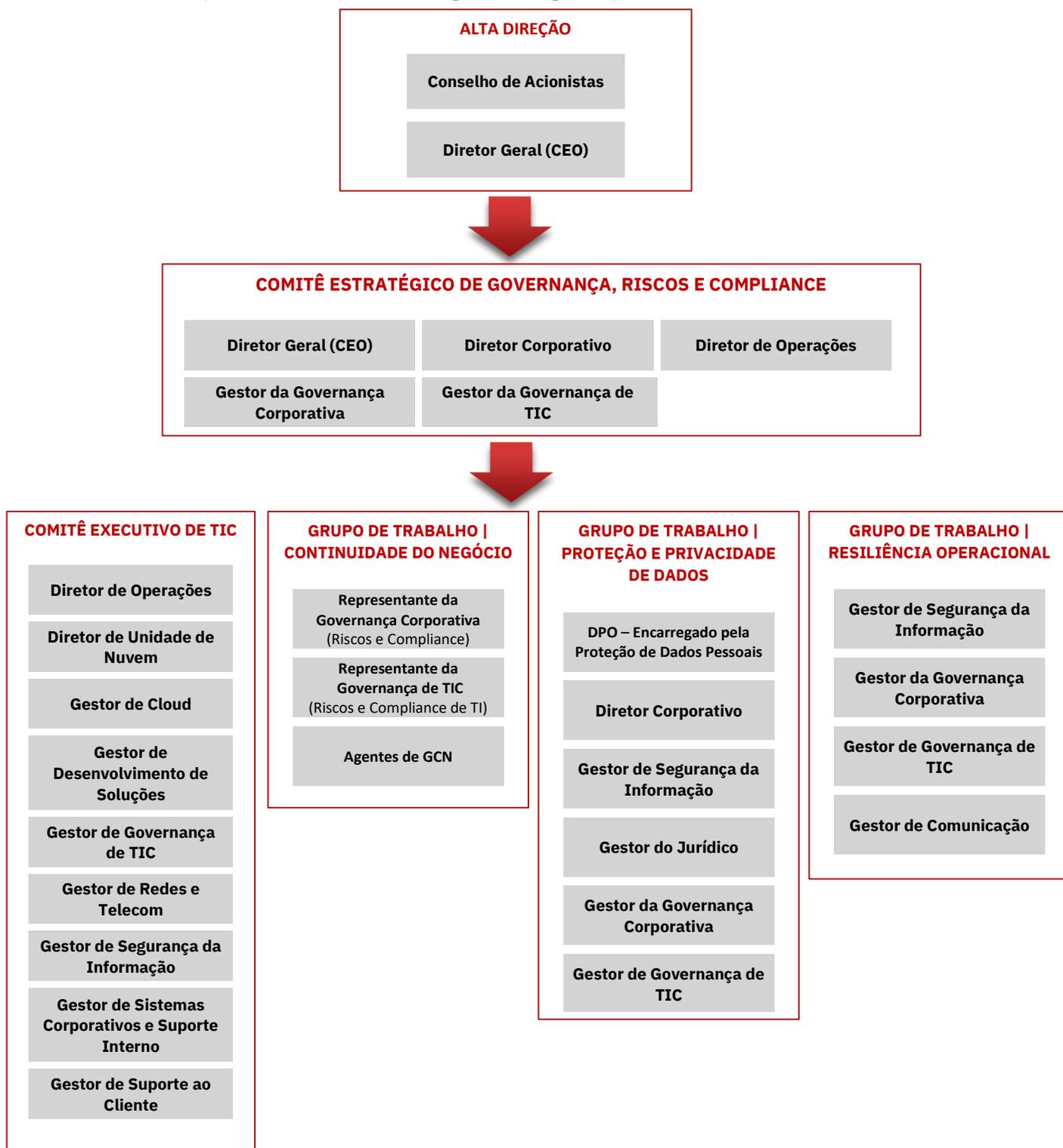




O *hub integrador* do mercado financeiro

## 2. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política de Gestão de Continuidade de Negócios descrevem as funções exercidas pelos colaboradores da RTM que atuam diretamente neste processo e que avaliam os danos ocasionados pelos eventos disruptivos, além das devidas ações que serão executadas para as demais áreas de negócio da organização.





## 2.1. Alta Direção

Compete à Alta Direção a função de **apoiador** e as seguintes atribuições:

- Demonstrar liderança e comprometimento;
- Prover os recursos (infraestrutura, recursos humanos, recursos materiais, entre outros), inclusive de contingência, para implementar e suportar os Planos de Continuidade de Negócios;
- Atribuir alçadas e responsabilidades;
- Comunicar a importância da Gestão de Continuidade de Negócios;
- Acompanhar os resultados das atividades de 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** e as seguintes atribuições:

- Assegurar que os requisitos de continuidade de negócios sejam considerados na implementação e manutenção do Sistema de Gestão de Continuidade de Negócios (SGCN);
- Aprovar a estratégia de continuidade de negócios, inclusive em relação a segurança da informação e prontidão de TIC;
- Avaliar as notificações de “ALERTA DE CRISE” (interrupção parcial) e de “ALERTA DE DESASTRE” (interrupção total) do evento disruptivo, além de comunicar e formalizar o status atualizado junto aos principais envolvidos;
- Declarar, após a análise da notificação e procedência dos fatos, “SITUAÇÃO DE CRISE” ou “SITUAÇÃO DE DESASTRE”;
- Ativar a contingência de pessoal;
- Realizar reuniões periódicas para validação dos pontos da Política de Continuidade de Negócios e para as alterações necessárias;
- Comunicar institucionalmente os colaboradores, clientes, fornecedores, autoridades reguladoras e veículos de comunicação do segmento de atuação, quando necessário, sobre a entrada, o estado e o encerramento da contingência.

## 2.3. Comitê Executivo de TIC

Compete ao Comitê Executivo de TIC a função de **Comitê de Contingência Tecnológica** e as seguintes atribuições:

- Definir as estratégias de contingência, de segurança da informação durante a interrupção e a prontidão de TIC para atender aos objetivos da continuidade de negócios;
- Garantir a continuidade das operações e serviços de TIC;
- Avaliar as perdas de TI e, no menor tempo possível, verificar os sistemas afetados;



- Avaliar a notificação de “ALERTA DE EMERGÊNCIA” (interrupção parcial) do evento disruptivo e formalizar o status atualizado junto aos principais envolvidos;
- Declarar, após a análise da notificação e procedência dos fatos, “SITUAÇÃO DE EMERGÊNCIA”
- Acionar os procedimentos preliminares de resposta a emergências e comunicar o responsável pelo site alternativo sobre a necessidade de uso das instalações contratadas;
- Coordenar as atividades de contingência da infraestrutura tecnológica, infraestrutura física e a contingência de serviços externos, incluindo a ativação dos Planos de Continuidade Operacionais (PCOs);
- Coordenar as atividades de recuperação, em caso de acionamento da contingência em uma situação de interrupção, incluindo a ativação dos Planos de Recuperação de Desastres (PRDs);
- Apontar as possíveis ameaças cibernéticas que a organização está vulnerável, bem como as ações que deverão ser tomadas caso se realizem;
- Tentar recuperar ativos que ainda estejam disponíveis no site afetado;
- Administrar contratos de serviços de TIC, tanto os relacionados diretamente ao site alternativo quanto aos demais ligados aos Planos de Continuidade de Negócios;
- Atender todas as ocorrências e incidentes de segurança da informação e de disponibilidade de produtos e serviços reportadas.

## 2.4. GT | Proteção e Privacidade de Dados Pessoais

Compete ao GT | Proteção e Privacidade de Dados Pessoais as seguintes atribuições:

- Avaliar os mecanismos de tratamento e proteção dos dados existentes e propor ações voltadas ao seu aperfeiçoamento, considerando o estado de normalidade ou na ocorrência de eventos disruptivos (emergências, crises e desastres);
- Estabelecer os objetivos de privacidade de dados;
- Assegurar o cumprimento das políticas de privacidade de dados pessoais, inclusive em situações de eventos disruptivos (emergências, crises e desastres);
- Revisar normativos de proteção e privacidade de dados pessoais;
- Aprovar critérios para a privacidade por padrão e desde a concepção;
- Atuar como facilitador na promoção das ações necessárias para a adequação de projetos e atividades que envolvam dados pessoais;
- Atuar nos eventos disruptivos (emergências, crises e desastres) que envolvem dados pessoais.

## 2.5. GT | Resiliência Operacional

Compete ao GT | Resiliência Operacional as seguintes atribuições:

- Receber as notificações dos eventos disruptivos (crises e desastres);
- Atuar como comitê de crise na ocorrência de eventos adversos que possam comprometer a imagem da RTM e/ou a continuidade do negócio.



## 2.6. GT | Continuidade do Negócio

Compete ao Grupo de Trabalho, denominado Continuidade do Negócio, a função de **facilitador** em todo o processo e as seguintes atribuições:

- Certificar-se de que os recursos foram mapeados e analisados criticamente a fim de estabelecer a menor exposição ao risco operacional;
- Apontar as possíveis ameaças que a organização está vulnerável e as ações que deverão ser tomadas caso se realizem;
- Acionar os procedimentos detalhados nos Planos de Continuidade de cada área da organização e convocar os demais colaboradores;
- Realizar as comunicações formais, de maneira clara e coesa, com os colaboradores;
- Providenciar atendimento adequado aos colaboradores com problemas;
- Realizar a primeira avaliação dos danos com os técnicos responsáveis;
- Posicionar a Gerência de Governança, Riscos e Compliance sobre o andamento da recuperação;
- Apoiar os colaboradores durante a operação em contingência;
- Acompanhar todas as atividades definidas no Plano de Testes do PCN, bem como manter sua área ciente dos procedimentos de testes e elaborar o relatório de realização dos testes;
- Tentar recuperar ativos que estejam ainda disponíveis no site afetado.

## 2.7. Gerência de Governança, Riscos e Compliance

Compete a Gerência de Governança, Riscos e Compliance as funções de **proprietária e gestora do processo de Continuidade de Negócios** e as seguintes atribuições:

- Estabelecer um Sistema de Gestão de Continuidade de Negócios (SGCN);
- Identificar e analisar os requisitos internos, legais e regulatórios;
- Definir os princípios, guias e políticas que necessitam ser incluídos ou é recomendável ser utilizados como referência;
- Encaminhar para a Alta Direção todas as medidas adotadas para a prevenção ou mitigação dos riscos à Continuidade dos Negócios identificados e garantir a confiabilidade dessas informações encaminhadas;
- Assegurar que a Política de GCN e seus planos relacionados sejam formalmente aprovados, publicados e comunicados, além da sua execução e revisão periódica;
- Assegurar a existência da Política de GCN e seus planos relacionados e o atendimento às necessidades da RTM, baseados nas análises de risco e de impactos nos negócios;
- Assegurar o treinamento dos Planos de Continuidade de Negócios;
- Definir os cenários de riscos disruptivos, assim como o planejamento e auditoria de seus testes;
- Assegurar que as alterações relacionadas aos processos de negócio sejam refletidas nos Planos de Continuidade de Negócios.



## 2.8. Gerência de Governança de TIC

- Identificar e analisar os requisitos internos, legais e regulatórios sobre a segurança da informação na disrupção e a prontidão de TIC na continuidade do negócio.

## 2.9. Gerência Financeira e Administrativa

- Administrar contratos de ativos de serviços, tanto os relacionados diretamente ao site alternativo quanto aos demais ligados aos Planos de Continuidade de Negócios.

## 2.10. Agentes de GCN

Compete ao Agente de Gestão de Continuidade de Negócios a função de **representante da sua área de negócio** e as seguintes atribuições:

- Identificar ameaças e impactos, garantindo que os recursos foram mapeados e analisados criticamente a fim de estabelecer a menor exposição ao risco operacional;
- Identificar e/ou sugerir controles que reduzam a possibilidade de ocorrência das ameaças identificadas;
- Apoiar na elaboração e na manutenção do Plano de Continuidade Operacional (PCO) e do Plano de Recuperação de Desastres (PRD);
- Informar apropriadamente a Gerência de Governança, Riscos e Compliance sobre riscos não mapeados de sua área, sejam eles novos ou não identificados anteriormente;
- Participar ativamente dos processos de teste, planejamento e treinamento;
- Apoiar os colaboradores de sua área durante a operação em contingência.

## 2.11. Áreas de Negócio

Compete às áreas de negócio as seguintes atribuições:

- Nomear colaboradores como Agentes de GCN, titulares e suplentes;
- Atualizar as documentações relacionadas aos seus processos;
- Apoiar na elaboração e aprovar os planos e procedimentos operacionais relacionados às suas áreas;
- Executar os testes de conformidade;
- Permanecer alinhada a esta Política de Gestão de Continuidade de Negócios e a todos os Planos de Continuidade de suas respectivas áreas.

### 3. OBJETIVOS

Com o comprometimento em alcançar a excelência na segurança, continuidade e na recuperação de seus serviços, produtos e processos críticos, a RTM assegura aos seus clientes, fornecedores e parceiros de negócios, que suas atividades fundamentais possam continuar, em casos de desastres e/ou indisponibilidade total ou parcial de suas operações.

Essa Política de Gestão de Continuidade de Negócios tem, portanto, como principal objetivo fornecer as diretrizes para minimizar os impactos negativos causados por quaisquer eventos que ofereçam riscos à continuidade de negócios da RTM.

A Política de Continuidade de Negócios tem ainda por objetivo:

- Conscientizar os colaboradores da RTM, sobre a importância do tema, aumentando sua capacidade de lidar com eventos inesperados;
- Definir responsabilidades para todos os profissionais que por força de suas funções estão envolvidos com as atividades de gestão, elaboração e manutenção dos Planos de Continuidade de Negócios;
- Assegurar condições de continuidade dos processos de negócios a fim de limitar graves perdas decorrentes de riscos externos;
- Implementar as diretrizes necessárias para o cumprimento das melhores práticas relacionadas a Gestão de Continuidade de Negócios.

### 4. METODOLOGIA

A metodologia de Gestão de Continuidade dos Negócios implantada na RTM baseia-se nos princípios apresentados no item 1.3 – requisitos estatutários e regulamentares – e tem como objetivo buscar a continuidade dos processos, sistemas e atividades críticas das áreas por meio da implantação de procedimentos alternativos e de contingências operacionais formalizados.

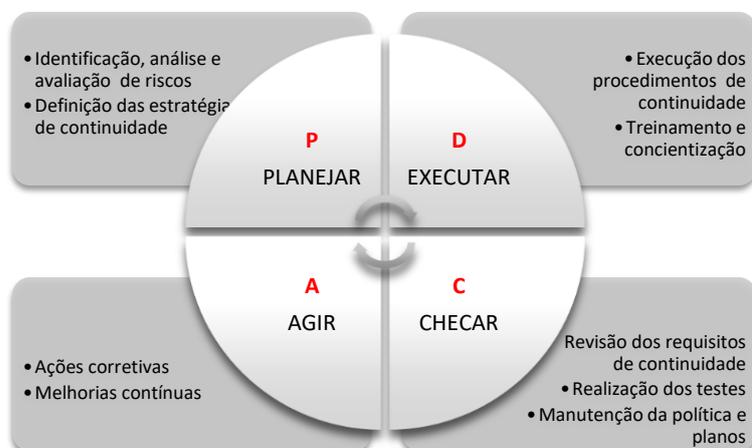


Figura 1 - Ciclo de vida da gestão de continuidade de negócios



O *hub integrador* do  
mercado financeiro

## 5. ESCOPO

Esta Política de Gestão de Continuidade de Negócios suporta todas as áreas de negócios e áreas de suporte ao negócio, localizadas no complexo de prédios da matriz, após a ocorrência ou durante a suspeita de uma crise que afete os processos críticos de negócios da RTM.

Entende-se por “complexo de prédios da RTM” o conjunto de prédios, que hospedam as operações da RTM, e estão localizados nos seguintes endereços:

Endereço: Rua Libero Badaró, 377- 22º, 26º e 27º andares – Centro – São Paulo – SP CEP: 010009-000

Endereço: Av. República do Chile, 230 – 7º andar - Centro – Rio de Janeiro – RJ CEP: 20031-170



O *hub integrador* do mercado financeiro

## 6. MAPA DE PROCESSO DE NEGÓCIOS

O mapa de processos de negócios deverá nortear toda Análise de Impacto, Estratégia e Planos de Continuidade de Negócios:

PRODUTOS	CONECTIVIDADE	CONTINGÊNCIA	DATA CENTER	NEGÓCIOS	SEGURANÇA	VOZ
	<b>CLOUD LINK</b> Conectividade dedicada e segura às principais nuvens públicas	<b>SITE DE CONTINGÊNCIA</b> Ambiente no padrão de escritório para emergências, manutenção e outras ocorrências	<b>CLOUD SERVER</b> Ambiente de servidores virtualizados com infraestrutura flexível e robusta	<b>HUB FUNDOS</b> Plataforma desenvolvida para comunicação dos players do mercado de fundos de investimentos	<b>GESTÃO DE VULNERABILIDADES</b> Analisa vulnerabilidades em ativos, sejam internos, externos ou aplicações a fim de identificar possíveis ameaças que comprometam o ativo e ambiente.	<b>RTM COMMUNITY</b> Plataforma de comunicação crítica de voz hospedada na nuvem RTM (RCS) com facilidades de busca e conexão entre usuários da solução.
	<b>CNET - REDE CORPORATIVA</b> Dados, voz e imagem entre matriz, filiais e parceiros das instituições financeiras		<b>RCS - CLOUD SERVICES</b> Ambiente de servidores virtualizados com infraestrutura flexível e robusta	<b>HUB REGISTRADORAS</b> Plataforma para atender a Circular nº 3.952 integrando instituições a CIP e B3 Registradora	<b>HSM AS A SERVICE</b> Solução completa de HSM como serviço, que tem como principal função o suporte a operações de criptografia e a gestão e proteção das chaves criptográficas, de modo a garantir a segurança e o sigilo dos dados.	<b>HOTLINE</b> Solução de comunicação de voz através de uma linha direta, privada e segura entre Instituições Financeiras
	<b>FNET - REDE FINANCEIRA</b> Rede privada para o mercado Financeiro		<b>COLOCATION</b> Estrutura física e racks para hospedar servidores	<b>HUB SLC</b> Plataforma para atender às Circulares de nº 3.765 e 3.952 do Banco Central		<b>TELEFONIA COMO SERVIÇO</b> Plataforma colaborativa de Telefonia IP em nuvem
SERVIÇOS	<b>INTERNET</b> Acesso a internet a partir dos ambientes tecnológicos da RTM (Datacenter, RCS, rede, etc)		<b>HOSTING</b> Serviço de hosting dedicado	<b>SWIFT</b> Solução desenvolvida para instituições que desejam acesso à rede SWIFT		<b>TRADE SOLUTION</b> Plataforma de comunicação para ambientes críticos
	<b>VENDORS</b> Solução de acesso às plataformas de negociação de ultra baixa latência RoboTrader da BLK Sistemas Financeiros, solução FIS VALDI Trader ou ao NYFIX (itiviti).		<b>BACKUP AS A SERVICE</b> Solução de proteção de dados / backup ofertada a partir da nuvem RTM.	<b>SANDBOX DREX</b> Serviço de Atendimento e Suporte de Primeiro Nível para os clientes da Solução Sandbox Drex. Estes clientes utilizam o produto para entender, experimentar e criar novos projetos baseados na tecnologia Blockchain na com base nas oportunidades do projeto Piloto Real Digital do Banco do Brasil.		
	<b>RSFN</b> Finalidade amparar o tráfego de informações no âmbito do SFN para serviços					



## 7. DIRETRIZES GERAIS

### 7.1. Estrutura de Gestão de Continuidade de Negócios

- A Gerência de Governança, Riscos e Compliance foi designada como responsável pelo processo de Gerenciamento da Continuidade de Negócios;
- Os demais papéis, responsabilidades e autoridades na gestão de continuidade de negócios devem estar definidos formalmente;
- Devem ser realizadas ações de busca ativa em legislações e guias de melhores práticas que assegurem a identificação dos requisitos a serem atendidos que estejam relacionados à gestão de continuidade de negócio;
- Devem ser alocados recursos humanos com habilidade, experiência e competência em continuidade de negócios.

### 7.2. Conscientização, Educação e Treinamento

- Todos os colaboradores da RTM devem estar cientes da relevância e importância de suas atividades no escopo de continuidade de negócios;
- O tema GCN deverá ser incluído nas reuniões dos gestores com suas equipes.

### 7.3. Melhoria Contínua

- A gestão do processo de Continuidade de Negócios (GCN) deverá ser contínua e sistematicamente atualizada;
- As revisões deverão ocorrer, no mínimo, anualmente ou sempre que ocorrerem mudanças significativas;
- Os recursos e as documentações do SGCN devem ser mantidos para garantir que permaneçam eficazes e alinhados com as prioridades do negócio, além de garantir a geração das evidências necessárias;
- Avaliação da documentação e capacidade da continuidade de negócio:
  - Deve-se avaliar a adequação e eficácia da BIA - análises de impacto de negócios, avaliação de risco, estratégias e documentações pertinentes;
  - Avaliar o compliance com os requisitos legais e regulamentares e com os objetivos de continuidade de negócios;
  - Os fornecedores e parceiros, pertinentes a continuidade de negócio, devem ser avaliados em relação a sua capacidade de atender aos requisitos definidos;
  - As avaliações e melhorias devem ser aplicadas conforme, minimamente, os resultados dos testes, exercícios e relatórios pós incidentes.

## 8. DIRETRIZES ESPECÍFICAS

### 8.1. Requisitos de Continuidade

- Serão realizadas ações de busca ativa em legislações e guias de melhores práticas que assegurem a identificação dos requisitos a serem atendidos que estejam relacionados à continuidade dos processos de negócio da RTM;
- Os requisitos estatutários e regulamentares serão mapeados, avaliados e documentados pela Gerência de Governança, Riscos e Compliance e a pela Gerência de Governança de TIC, por meio das áreas de Controles Internos;
- Os requisitos relacionados aos controles preventivos de riscos serão aplicados pela Gerência de Governança, Riscos e Compliance e a pela Gerência de Governança de TIC, por meio das áreas de Processos e Controles Internos.

### 8.2. Requisitos de Segurança da Informação

- Deve-se planejar e definir os requisitos de segurança da informação em eventos adversos (emergência, crise, desastres);
- Os requisitos de disponibilidade dos recursos de processamento da informação serão garantidos pela Diretoria de Unidade de Nuvem, por meio de implementação de redundância suficiente para atendê-los;
- Os requisitos de verificação, análise crítica e avaliação da continuidade da segurança da informação serão verificados pelas Gerências de Governança, Riscos e Compliance e de Governança de TIC em intervalos regulares, garantido que são válidos e eficazes em situações adversas;
- Os requisitos de controle e proteção, implementados pelas Diretorias de Operações e Unidade de Nuvem, assegurarão que os registros serão protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio;
- Os requisitos de controles de criptografia serão utilizados pelas Diretorias de Operações e Unidade de Nuvem, em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes;
- Os requisitos de privacidade e proteção das informações de identificação pessoal serão assegurados de acordo com o requerido por legislação e regulamentação pertinente.



### 8.3. Ambientes de Redundância

- Todos os processos automatizados e a geração de informações são suportados direta ou indiretamente pela estrutura de dois Data Center, localizados nos estados de São Paulo (site 1), e Rio de Janeiro (site 2) e sendo ambos com Alta Disponibilidade;
- Em relação aos locais de armazenamentos, os sites da RTM são distantes bastantes para garantir a segurança dos dados e em caso de desastres e catástrofes naturais ou interrupção de serviços externos essenciais. Mesmo que o site de São Paulo seja devastado por uma inundação ou incêndio, os dados serão preservados no site do Rio de Janeiro, por estarem geograficamente afastados;
- Está implementado o fornecimento de serviços redundantes de infraestrutura para os data centers, tais como energia e telecomunicações.

### 8.4. Estratégias de Continuidade

A estratégia de continuidade de negócios definida pela RTM para garantir a continuidade dos seus processos críticos de negócio aborda todas as etapas, pessoas e recursos necessários para recuperar um processo crítico e está baseada nas seguintes diretrizes:

- Manutenção de uma área funcional dentro da estrutura organizacional da empresa denominada Gerência de Governança, Riscos e Compliance, a qual será proprietária e responsável direta pela gestão do processo de Gestão de Continuidade do Negócio;
- Manutenção de um grupo de trabalho, denominado GT | Continuidade do Negócio, para manter o processo de GCN na RTM, composto pelas áreas de riscos corporativo, riscos de TI, bem como pelos agentes de gestão de continuidade que forem designados;
- Manutenção do papel do Agente de Gestão de Continuidade de Negócios, o qual atuará como corresponsável pelo programa de Continuidade de Negócio em cada área de negócio, buscando promover a cultura de continuidade e manter atualizados todos os planos da sua respectiva área;
- Identificação dos processos críticos e tratamento de acordo com a sua complexidade e risco, visando se antecipar às situações de crise;
- Identificação e formalização de estratégias que atendam os requisitos de continuidade e recuperação das atividades priorizadas, conforme prazo definido e capacidade aceitável, e que limitam o impacto da disrupção nos produtos e serviços da RTM;
- Planejamento da contingência (emergência) com o objetivo de definir as necessidades e ações mais imediatas, assegurando a diminuição do impacto da disrupção e, se acontecer, o período dela;
- Definição dos recursos (pessoas, informações e dados, infraestrutura física, equipamentos e consumíveis, sistemas de TIC, logística, financeiro e terceiros) e seus requisitos necessários e adequados para a implantação e manutenção das estratégias de continuidade;
- Implantação gradativa dos Planos de Continuidade de Negócios em cada área da RTM, definindo “ondas” para planejamento, implantação, teste e auditoria dos planos e soluções de



continuidade. A implantação do Plano de Continuidade de Negócios será iniciada pelos processos mais críticos da organização e seguirá continuamente até que todos sejam reestabelecidos;

- Utilização da infraestrutura física e tecnológica da RTM, localizadas em São Paulo e Rio de Janeiro, para prover posições de contingência para as áreas de negócio;
- Não utilização dos espaços destinados aos clientes para fins de contingência, de modo a preservar as atividades destes intactas.

## 8.5. Plano de Continuidade de Negócios - PCN

- **Estrutura:** o Plano de Continuidade de Negócios da RTM será constituído pelos seguintes documentos:
  - **Planos de Continuidade Operacional (PCOs)** que são voltados aos processos operacionais e são os primeiros a serem acionados. Objetiva reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente;
  - **Plano de Administração da Crise (PAC)** que é acionado na Crise e tem seu término quando se volta à normalidade.
  - **Plano de Recuperação de Desastres (PRD)** que é acionado junto com o PCO e é focado na recuperação/restauração de ativos dos componentes que suportam o PCN. Objetiva definir o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação;
  - **Plano de Testes** para confirmar a eficiência do PCN.

Os planos devem ser interligados com o intuito de coletivamente ser possível atingir os objetivos de continuidade e recuperação das atividades priorizadas. Detalhando as ações necessárias, os limites existentes e o gerenciamento das consequências imediatas decorrente da interrupção.

- **Desenvolvimento:**
  - O desenvolvimento do Plano de Continuidade de Negócios será baseado na avaliação dos processos críticos estabelecidos, compreendendo as principais etapas:
    - Análise de Riscos;
    - Análise de Impacto nos Negócios (BIA); e
    - Planejamento (estratégias de continuidade e recuperação).
  - Os gestores e os agentes de GCN designados devem conhecer as fases do desenvolvimento do PCN e contribuir para a identificação das ameaças e das vulnerabilidades que podem afetar o negócio, mas que não constam do Plano;
  - O PCN deve ser desenvolvido inicialmente considerando somente as situações de risco com maior impacto e se ampliará conforme a maturidade da RTM frente à governança de seus processos.



## 8.6. Testes

- Deverá ser implementado e mantido um programa de exercícios e testes, consolidado por meio do Plano de Testes, para acompanhamento da eficiência e da validade das estratégias e soluções de continuidade de negócios da RTM;
- O programa de exercícios e testes deve ser alinhado e consistente com os objetivos de continuidade de negócios e baseado nos cenários apropriados;
- O Plano de Testes deverá abranger os seguintes tópicos:
  - Objetivos específicos;
  - Periodicidade de realização;
  - Tipos de testes que serão realizados;
  - Responsabilidades pela gestão, condução e acompanhamento;
  - Aspectos técnicos, logísticos, administrativos da execução dos testes.

## 9. 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).



O *hub integrador* do mercado financeiro

## ANEXOS

- I. Matriz de papéis e responsabilidades (RACI);
- II. Plano de Continuidade de Negócios (PCN)

