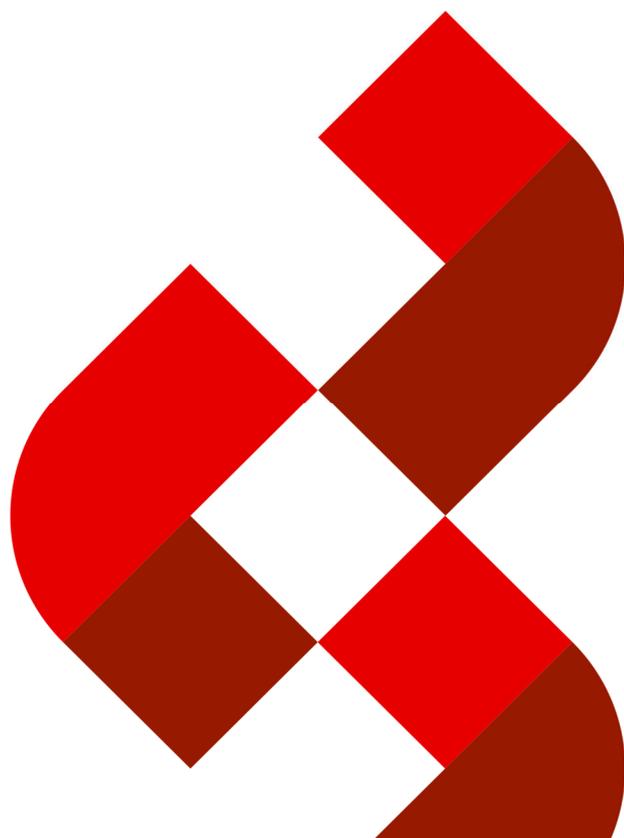




# Política de Segurança da Informação e Cibernética

POLÍTICA CORPORATIVA

V4.1 - 2024





O *hub integrador* do  
mercado financeiro

## SUMÁRIO

SIGLAS, ABREVIACÕES E DEFINIÇÕES .....	4
1. INTRODUÇÃO .....	6
2. PAPÉIS E RESPONSABILIDADES .....	7
3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO .....	12
4. OBJETIVOS.....	13
5. METODOLOGIA.....	14
6. ESCOPO .....	14
7. DIRETRIZES GERAIS .....	15
<b>7.1. Estrutura de Gestão da Segurança da Informação</b> .....	15
<b>7.2. Governança da Segurança da Informação</b> .....	15
<b>7.3. Conscientização, Educação e Treinamento</b> .....	16
<b>7.4. Melhoria contínua</b> .....	16
8. DIRETRIZES DE S.I. E CIBERNÉTICAS .....	17
<b>8.1. Acessos</b> .....	17
<b>8.2. Ativos</b> .....	17
<b>8.3. Backup</b> .....	18
<b>8.4. Continuidade de Negócios</b> .....	18
<b>8.5. Criptografia e Chaves</b> .....	18
<b>8.6. Eventos</b> .....	18
<b>8.7. Fornecedores</b> .....	19
<b>8.8. Incidentes de TIC e Segurança da Informação</b> .....	19
<b>8.9. Mudanças</b> .....	20
<b>8.10. Orientações aos Usuários Finais</b> .....	20
<b>8.11. Propriedade Intelectual</b> .....	20
<b>8.12. Proteção contra <i>Malware</i></b> .....	21
<b>8.13. Prevenção e Detecção de Intrusão</b> .....	21



O *hub integrador* do mercado financeiro

<b>8.14.</b>	<b>Proteção e Privacidade de Dados</b>	21
<b>8.15.</b>	<b>Redes</b>	22
<b>8.16.</b>	<b>Riscos</b>	22
<b>8.17.</b>	<b>Segurança Física e do Ambiente</b>	22
<b>8.18.</b>	<b>Segurança em Nuvem</b>	23
<b>8.19.</b>	<b>Sistemas e Aplicações</b>	23
<b>8.20.</b>	<b>Testes de Segurança</b>	23
<b>8.21.</b>	<b>Tratamento de Desvios e Exceções</b>	23
<b>8.22.</b>	<b>Vulnerabilidades Técnicas</b>	24
<b>9.</b>	<b>PENALIDADES</b>	24
	<b>ANEXOS</b>	25
	<b>CONTROLES DO DOCUMENTO</b>	26

## DOCUMENTO PÚBLICO

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



O *hub integrador* do  
mercado financeiro

## SIGLAS, ABREVIACÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
<b>Alta direção</b>	Pessoa ou grupo de pessoas que dirige e controla uma organização em seu nível mais alto
<b>Apetite ao risco</b>	Quantidade e tipo de risco que uma organização está disposta a buscar, manter ou assumir
<b>Autenticação</b>	Valida a autorização do usuário para acessar, transmitir e receber determinadas informações, confirmando a identidade dos colaboradores antes de liberar o acesso aos sistemas e recursos, garantindo que não se passem por pessoas não autorizadas
<b>Autenticidade</b>	Garantia da veracidade da autoria da informação, entretanto, não visa garantir a veracidade do conteúdo da informação. A autenticidade garante a veracidade do autor, de quem de fato produziu aquela informação, não entrando no mérito se o conteúdo produzido é verdadeiro ou falso
<b>Backup</b>	Cópia de segurança
<b>Compliance</b>	Conjunto de mecanismos para atendimento a todas as obrigações de <i>Compliance</i> da organização
<b>Confidencialidade</b>	Garantia de que as informações não sejam disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados
<b>Conformidade</b>	Atendimento a um requisito
<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>Controles internos</b>	É um conjunto de atividades, planos, métodos, indicadores, e procedimentos interligados, utilizados para assegurar a conformidade dos atos de gestão
<b>Criptografia</b>	Técnica utilizada para codificar os dados, sendo apenas decifráveis para aqueles que possuem sua decodificação. Evitando o livre acesso aos dados
<b>Disponibilidade</b>	Garantia de que a informação esteja acessível e utilizável sempre que necessário para as pessoas autorizadas
<b>Erradicação</b>	Eliminação de vetores causadores do incidente de segurança da informação
<b>GT   Denúncias e Investigações</b>	Grupo de pessoas autorizadas a recepcionar as denúncias, investigar e encaminhar para a aplicação das consequências
<b>Grupo RTM</b>	RTM Rede de Telecomunicações Para o Mercado LTDA RTM Infraestrutura em Tecnologia da Informação LTDA



O *hub integrador* do  
mercado financeiro

<b>Impacto</b>	Consequência avaliada de um evento em particular
<b>Incidentes de segurança da informação</b>	Um simples evento ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação
<b>Integridade</b>	Garantia de que a informação seja mantida em seu estado original, visando protegê-la, no processo, transporte e armazenamento, contra alterações indevidas, seja ela intencional ou acidental
<b>Malware</b>	Definição genérica para qualquer software de computador com intenção maliciosa
<b>Não repúdio</b>	Ou irretratabilidade. Garante que uma pessoa ou entidade não possa negar a autoria da informação fornecida, como no caso do uso de certificados digitais para transações online e assinatura de documentos eletrônicos. Ou seja, o não repúdio é a incapacidade da negação da autoria da informação
<b>Organização</b>	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
<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>Requisito</b>	Necessidade ou expectativa que é declarada, geralmente obrigatória ou implícita
<b>Risco</b>	Efeito da incerteza nos objetivos organizacionais, em outras palavras, riscos são “possíveis acontecimentos que podem ou não ocorrer (incerteza), e que se ocorrerem podem impedir ou atrapalhar o alcance dos objetivos de uma organização ou de um processo de negócio específico.”
<b>SGSI</b>	Sistema de Gestão de Segurança da Informação
<b>Segurança da Informação</b>	Conjunto de ações e boas práticas com o objetivo de proteger os ativos da organização
<b>TIC</b>	Tecnologia da informação e comunicação
<b>Vulnerabilidades técnicas</b>	Fraqueza de um ativo ou grupo de ativos que pode ser explorada



O *hub integrador* do  
mercado financeiro

## 1. INTRODUÇÃO

### 1.1. RESUMO

O documento Política de Segurança da Informação e Cibernética visa descrever as diretrizes necessárias para prover a gestão da segurança da informação e cibernética, norteando para a elaboração de processos, normas e procedimentos.

### 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/IEC 27.001** (Sistemas de gestão da segurança da informação – Requisitos)
- ABNT NBR **ISO/IEC 27.002** (Código de prática para controles de segurança da informação)
- ABNT NBR **ISO/IEC 27.014** (Governança de segurança da informação)
- ABNT NBR **16167** (Diretrizes para classificação, rotulação, tratamento e gestão da informação)
- **COBIT 2019** (Objetivos de controle de informação e tecnologia relacionada)
- BACEN **Resolução 4893** (Política de segurança cibernética para instituições autorizadas pelo Banco Central)
- **LEI 13.709/18** (Lei geral de proteção de dados - LGPD)
- **NIST SP 800-12** (Uma introdução à segurança da informação)
- **NIST SP 800-53** (Controles de segurança e privacidade para sistemas de informação)
- **NIST SP 800-61** (Guia de tratamento de incidentes de segurança)
- **NIST SP 800-100** (Manual de segurança da informação - Um guia para gerentes)
- **NIST SP 800-209** (Diretrizes de segurança para infraestrutura de armazenamento)
- **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 Segurança da Informação e Cibernética está alinhada às demais políticas da organização, dentre as quais destacamos as seguintes:





## 2. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política de Segurança da Informação e Cibernética descrevem as funções exercidas pelos componentes da estrutura de governança da RTM e a sua organização.

### 2.1. Alta Direção

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

- Demonstrar liderança;
- Prover os recursos necessários para o SGSI - Sistema de Gestão de Segurança da Informação;
- Apoiar o Comitê Estratégico de Governança, Riscos e *Compliance* quanto a qualquer decisão relacionada ao SGSI, bem como a estratégia e ações para redução de riscos;
- Apoiar as políticas o SGSI da RTM;
- Receber relatórios de violações das políticas e diretrizes o SGSI.

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

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

- Identificar e atribuir responsabilidades com relação à segurança da informação e cibernética;
- Direcionar a segurança da informação e cibernética;
- Aprovar a Política de Segurança da Informação e Cibernética da RTM;
- Receber ocorrências que possam impactar na segurança e, se necessário, aprovar iniciativas que melhorem o nível de segurança;
- Receber, analisar e deliberar sobre casos de violação das políticas de segurança da informação e cibernética da RTM e, se necessário, notificar as lideranças;
- Propor ajustes, aprimoramentos e modificações na estrutura normativa e organizacional, submetendo à avaliação da Alta Direção da RTM;
- Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação e cibernética;
- Deliberar sobre a estratégia de proteção e mitigação dos riscos relacionados à segurança da informação e cibernética;
- Direcionar quanto ao apetite de riscos de segurança da informação;
- Viabilizar e promover o planejamento, manutenção e melhoria contínua do SGSI – Sistema de Gestão de Segurança da Informação;
- Realizar a análise crítica do SGSI e contribuir para a melhoria contínua.



O *hub integrador* do  
mercado financeiro

## 2.3. Comitê Executivo de TIC

- Avaliar a Política de Segurança da Informação e Cibernética da RTM;
- Aprovar as políticas complementares de segurança da informação da RTM.

## 2.4. DIROP – Diretoria de Operações

- Aprovar mecanismos de registro e controle de eventos de TIC e SI;
- Aprovar mecanismos de registro e controle de incidentes de TIC, bem como, de não conformidades.

## 2.5. DIRUN – Diretoria de Unidade de Nuvem

- Aprovar mecanismos de registro e controle de incidentes de segurança da informação, bem como, de não conformidades.

## 2.6. Gerência de Segurança da Informação

- Consolidar, manter e coordenar a elaboração, o acompanhamento, a evolução e a avaliação, do SGSI – Sistema de Gestão de Segurança da Informação, bem como realizar rondas, vistorias, auditorias e análise crítica, visando a melhoria contínua;
- Em conjunto com a Gerência de Governança de TIC, elaborar e manter as políticas e normas de segurança da informação e cibernética;
- Elaborar e manter os procedimentos de segurança da informação e cibernética;
- Implementar os controles técnicos para atender as políticas de segurança da informação e cibernética, no que tange as suas responsabilidades técnicas;
- Coordenar projetos e iniciativas para assegurar que os objetivos de segurança da informação e cibernética sejam atingidos;
- Elaborar e executar o programa de conscientização, educação e treinamento em segurança da informação;
- Monitorar ocorrências que possam impactar na segurança e, se necessário, propor iniciativas que melhorem o nível de segurança;
- Identificar e analisar riscos de segurança da informação e riscos cibernéticos;
- Gerenciar incidentes de segurança da informação;
- Gerenciar acessos de colaboradores, clientes e terceiros;
- Gerenciar vulnerabilidades técnicas;
- Gerenciar controles criptográficos;
- Gerenciar atualizações e correções;
- Implementar mecanismos de proteção contra malware;
- Implementar mecanismos para prevenção e detecção de intrusão no ambiente operacional da RTM;
- Acompanhar e analisar alertas de segurança junto aos devidos responsáveis.



O *hub integrador* do  
mercado financeiro

## 2.7. Gerência de Governança, Riscos e Compliance

- Realizar a gestão de riscos;
- Realizar a gestão de continuidade de negócios;
- Realizar o monitoramento e avaliação de riscos de fornecedores;
- Gerenciar as não-conformidades.

## 2.8. Gerência de Governança de TIC

- Manter as áreas da RTM informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo segurança da informação;
- Realizar a gestão dos ativos de TIC;
- Em conjunto com a Gerência de Segurança da Informação, elaborar e manter as políticas e normas de segurança da informação e cibernética;
- Emitir relatório de conformidade sobre o SGSI para o Comitê Estratégico de Governança, Riscos e Compliance;
- Conduzir a gestão de riscos de segurança da informação;
- Apoiar o processo de gestão de continuidade de negócios;
- Apoiar o processo de gestão de fornecedores, incluindo a etapa de relacionamento na cadeia de suprimentos, no que tange a aquisição de ativos ou serviços de TIC;
- Apoiar a gestão de não-conformidades relacionadas à segurança da informação e cibernética.

## 2.9. ASGEP – Assessoria de Gestão de Pessoas

- Assegurar que todos os colaboradores e terceiros assinem os termos relacionados à segurança da informação;
- Gerenciar mudanças organizacionais, considerando também as que afetam a segurança da informação e cibernética.

## 2.10. Gerência Jurídica

- Incluir, sempre que necessário e quando aplicável, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da RTM;
- Avaliar, quando solicitado pelas áreas ligadas ao tema, as políticas, as diretrizes, as normas e procedimentos de segurança da informação e cibernética da RTM;
- Assegurar a conformidade do processo de Privacidade de Dados com o SGSI – Sistema de Gestão de Segurança da Informação.



## 2.11. Gestores

- Cumprir e fazer cumprir (colaboradores e terceiros sob a sua responsabilidade) a política, as normas e diretrizes de segurança da informação e cibernética;
- Assegurar que a sua área possua acesso e entendimento das políticas, das normas e diretrizes de segurança da informação e cibernética;
- Garantir que todas as diretrizes, procedimentos, controles e operações da sua área, estejam documentados, detalhados e atualizados;
- Assegurar que os colaboradores da sua área realizem todos os treinamentos sobre segurança da informação, cibernética e privacidade de dados;
- Comunicar ao GT | Denúncias e Investigações, de forma imediata, via canal de denúncias e investigações eventuais casos de violação da política, de normas ou diretrizes;
- Incentivar que esta política, demais normas e diretrizes de segurança da informação e cibernética sejam cumpridas de acordo com os preceitos definidos para a sua área de atuação;
- Armazenar evidências dos processos, assim como fornecê-las quando solicitado;
- Garantir na análise e elaboração de projetos internos, com clientes ou terceiros, sempre que necessário e quando aplicável, que sejam realizadas avaliações específicas relacionadas à segurança da informação e cibernética e proteção de dados pessoais ou sensíveis, com o objetivo de proteger os interesses e ativos críticos da RTM.

## 2.12. Colaboradores

- Conhecer, seguir e disseminar as diretrizes estabelecidas nesta política e nos demais normativos de segurança da informação e cibernética;
- Realizar todos os treinamentos sobre segurança da informação, cibernética e proteção de dados;
- Assegurar a correta classificação das informações sob sua responsabilidade;
- Observar e respeitar o grau de confidencialidade definido pelo proprietário da informação;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela RTM;
- Não discutir assuntos confidenciais da RTM em lugares públicos/expostos, incluindo em redes sociais;
- Apoiar na implementação dos controles de segurança da informação em sua alçada de atuação;
- Fazer uso apropriado de sistemas, recursos e serviços de tecnologia da RTM. Incluindo, mas não se limitam a: computadores, notebooks, aparelhos telefônicos, celulares, correio eletrônico, sistemas, internet, entre outros;
- Garantir a integridade e confidencialidade de dados pessoais ou sensíveis aos quais tiver acesso através da RTM, utilizando-os estritamente para o fim a que se destina;



- Acessar apenas informações necessárias às suas atividades. Se porventura obtiver acesso a informações que não competem às suas atividades, deverá imediatamente comunicar a área de segurança da informação e ao seu gestor direto;
- Comunicar ao GT | Denúncias e Investigações, de forma imediata, via canal de denúncias e investigações, qualquer descumprimento ou violação das políticas de segurança da informação e cibernética da RTM;
- Em caso de rescisão de contrato, realizar a devolução de todos os ativos de TIC sob sua responsabilidade e assegurar a devolução de todas as informações de propriedade da RTM;
- Respeitar e seguir as diretrizes e procedimentos implementados pelos normativos da RTM;
- Respeitar os direitos de acessos concedidos a sua função de atuação na RTM e seguir as diretrizes e regras estabelecidas para a gestão de acesso, não utilizando os acessos privilegiados de forma indevida.

## 2.13. Terceiros

- Conhecer, seguir e disseminar as diretrizes estabelecidas nesta política e nas demais políticas de segurança da informação e cibernética para terceiros;
- Apoiar na implementação dos controles de segurança da informação em sua alçada de atuação junto a RTM;
- Fazer uso apropriado de sistemas, recursos e serviços de tecnologia da RTM. Incluindo, mas não se limitam a: computadores, notebooks, aparelhos telefônicos, celulares, correio eletrônico, sistemas, internet, entre outros;
- Respeitar a correta classificação das informações que produza para a RTM;
- Observar e respeitar o grau de confidencialidade definida pelo proprietário da informação na RTM;
- Garantir a integridade e confidencialidade de dados pessoais ou sensíveis aos quais tiver acesso através da RTM, utilizando-os estritamente para o fim a que se destina;
- Acessar apenas informações necessárias às suas atividades na RTM. Se porventura obtiver acesso a informações que não competem às suas atividades, deverá imediatamente comunicar ao gestor do seu contrato, para que o mesmo informe a área de segurança da informação da RTM;
- Comunicar ao GT | Denúncias e Investigações, de forma imediata, via canal de denúncias e investigações, qualquer descumprimento ou violação das políticas de segurança da informação e cibernética da RTM;
- Em caso de rescisão de contrato, realizar a devolução de todos os ativos de TIC sob sua responsabilidade e assegurar a devolução de todas as informações de propriedade da RTM;
- Respeitar e seguir as diretrizes e procedimentos implementados pelos normativos da RTM, sob riscos da execução de consequências (medidas disciplinares, técnicas e administrativas), conforme estabelecidas na Norma.



O *hub integrador* do  
mercado financeiro

### 3. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A governança da segurança da informação está baseada nos seguintes princípios:

- **Estabelecer a segurança da informação em toda a organização:** Garantir que as atividades de segurança da informação sejam entendidas e integradas por toda RTM, assegurando que as tomadas de decisões levem em conta não apenas o negócio, mas também a segurança da informação;
- **Adotar uma abordagem baseada em riscos:** As decisões devem ser baseadas nos riscos e a gestão de risco deve ser única e adequada para toda RTM;
- **Estabelecer a direção de decisões de investimento:** Estabelecer uma estratégia de investimento em segurança da informação com base em resultados de negócios a serem alcançados pela RTM, assegurando um alinhamento entre os requisitos de negócios e os de segurança da informação;
- **Assegurar conformidade com os requisitos internos e externos:** Garantir que as políticas e práticas de segurança da informação atendam aos requisitos regulamentares, estatutários, contratuais, externos e internos;
- **Promover um ambiente positivo de segurança:** Assegurar um ambiente harmonioso, visto que o comportamento humano é um dos elementos fundamentais para manter o nível apropriado de segurança da informação. Coordenar, de forma adequada, os objetivos, papéis, responsabilidades e recursos, buscando garantir o cumprimento dos objetivos de negócio sem falhas;
- **Analisar criticamente o desempenho em relação aos resultados de negócios:** Assegurar que o desempenho da segurança da informação esteja em níveis aceitáveis para atender o negócio atual e futuro da RTM. Isto pode ocorrer por meio de análise críticas, monitoramento, auditorias e melhorias contínuas, associando o desempenho da segurança da informação com o desempenho do negócio da RTM.



## 4. OBJETIVOS

Esta Política estabelece e descreve as diretrizes da RTM relacionadas a segurança da informação e cibernética para assegurar o cumprimento dos princípios de governança de segurança da informação. Princípios estes baseados nos seguintes pilares: confidencialidade, integridade, disponibilidade, autenticidade e não repúdio da informação.

A Política de Segurança da Informação e Cibernética tem, também, como objetivos:

- Assegurar a conformidade com os requisitos estatutários e regulamentares do item 1.3;
- Assegurar a conformidade com os requisitos contratuais;
- Garantir níveis aceitáveis de confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio das informações da RTM;
- Proteger os ativos de dados e informações da RTM;
- Definir e nortear a implementação de controles nos processos, não limitando-se, aos que fazem parte do SGSI - Sistema de Gestão de Segurança da Informação;
- Declarar e formalizar os papéis e responsabilidades de todos os envolvidos no SGSI;
- Estabelecer diretrizes para a segurança da informação e segurança cibernética;
- Garantir a capacidade da RTM de prevenir, conter e erradicar incidentes de segurança da informação e, posteriormente, recuperar o ambiente;
- Garantir a prevenção, detecção e redução de vulnerabilidades relacionadas ao ambiente, inclusive ao cibernético;
- Assegurar o planejamento e implementação do programa de conscientização e treinamento de segurança da informação para todos os colaboradores e terceiros da RTM;
- Garantir a existência de práticas e cultura que tenha como objetivo manter os controles de segurança em patamares aceitáveis, efetuando uma gestão de riscos de segurança assertiva;
- Garantir a continuidade das atividades da RTM, protegendo os processos críticos contra falhas ou desastres significativos;
- Minimizar o impacto negativo no ambiente, nos serviços e produtos da RTM, em casos de acontecimentos de uma falha de segurança.



O *hub integrador* do mercado financeiro

## 5. METODOLOGIA

A metodologia para a Política de Segurança da Informação e Cibernética implantada na RTM baseia-se nos princípios apresentados no item 1.3 – requisitos estatutários e regulamentares – e tem como objetivo garantir a confidencialidade, integridade, disponibilidade, autenticidade e não repúdio da informação. Além disso, por meio da melhoria contínua, garantir que a Política esteja atualizada, assegurando assim, a sua pertinência, adequação e eficácia.



## 6. ESCOPO

O escopo desta Política engloba:

- Segurança da Informação;
- Segurança Cibernética.



## 7. DIRETRIZES GERAIS

As diretrizes presentes neste documento serão as norteadoras para o SGSI - Sistema de Gestão de Segurança da Informação, direcionando para a elaboração de normativos complementares, conforme apropriado e aprovado pelo Comitê responsável.

### 7.1. Estrutura de Gestão da Segurança da Informação

- O Comitê Estratégico de Governança, Riscos e Compliance foi designado para atuar como direcionador estratégico e aprovador do SGSI – Sistema de Gestão de Segurança da Informação;
- Os demais papéis, responsabilidades e autoridades na gestão de segurança da informação e cibernética 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 ao SGSI;
- Devem ser alocados recursos humanos com habilidade, experiência e competência em segurança da informação e cibernética.

### 7.2. Governança da Segurança da Informação

- A Política de Segurança da Informação e Cibernética deverá ser atualizada/revisada conforme normativos internos ou sempre que houver mudanças na RTM, como por exemplo nos objetivos de negócios, no ambiente de risco, nas regulamentações, na sua estrutura organizacional;
- O cumprimento de todas as diretrizes presentes nesta Política e nos normativos complementares deverá ser avaliado de forma periódica, para assegurar sua conformidade, e todos os envolvidos devem estar conscientes dessa avaliação;
- A Política de Segurança da Informação e Cibernética e os normativos complementares deverão ser comunicados às partes pertinentes e, além disso, disponibilizadas para acesso aos que possuem direito;
- Os colaboradores devem assumir uma postura proativa no que diz respeito à proteção das informações da RTM e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações e acesso indevido aos sistemas de informação sob responsabilidade da RTM;
- As estratégias de segurança da informação deverão ser definidas e documentadas;
- Os projetos gerenciados e realizados pela RTM deverão adotar critérios de segurança da informação para o cumprimento desta política.



### 7.3. Conscientização, Educação e Treinamento

Um programa para conscientização, educação e treinamento sobre segurança da informação deverá ser elaborado e executado.

Todos os colaboradores e, quando for necessário, terceiros devem ser conscientizados, educados e treinados.

As principais diretrizes, não limitando-se, são:

- Todos os colaboradores e, quando pertinente, partes externas devem receber conscientização, educação e treinamento sobre segurança da informação;
- Todos os colaboradores e partes externas devem estar conscientes sobre suas responsabilidades na segurança da informação;
- Todos os novos colaboradores, no momento da contratação, devem realizar o treinamento, de acordo com o prazo definido;
- A conscientização, educação e treinamento devem ocorrer de forma periódica e manter assuntos atualizados;
- Devem ser disponibilizadas informações de segurança da informação aos usuários finais sobre a utilização de produtos e serviços oferecidos pela RTM;
- Os colaboradores e, quando pertinente, terceiros devem dar o aceite nas políticas e procedimentos de segurança da informação da RTM;
- Deve-se realizar, após a finalização da conscientização, educação ou treinamento, uma avaliação de entendimento com os participantes;
- O programa deve estar alinhado com todas as políticas, normas e procedimentos implantados na RTM.

### 7.4. Melhoria contínua

Todo o SGSI - Sistema de Gestão de Segurança da Informação deve ser analisado criticamente com o objetivo de manter a pertinência, adequação e eficácia.

Essa análise deve ocorrer em intervalos planejados ou quando ocorrer mudanças significativas na RTM.



O *hub integrador* do  
mercado financeiro

## 8. DIRETRIZES DE S.I. E CIBERNÉTICAS

### 8.1. Acessos

As medidas de controle a serem implementadas pela RTM visam assegurar que o acesso as suas informações e aos seus recursos de processamento da informação só estejam disponíveis para colaboradores e terceiros autorizados.

Uma Política de Identidade e Gestão de Acessos, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida, abordando, no mínimo, os seguintes temas:

- Criação de novos acessos lógicos e permissões;
- Propriedade e transferência de login;
- Senhas, chaves e outros recursos de caráter pessoal.

### 8.2. Ativos

Uma Política de Gestão de Ativos, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

O processo de Gestão de Ativos da RTM deverá:

- Gerenciar todo o ciclo de vida dos ativos;
- Definir as devidas responsabilidades pela proteção dos ativos;
- Garantir que permaneçam operacionais (adequados à finalidade);
- Garantir que sejam contabilizados e fisicamente protegidos.

Regras para o uso aceitável dos ativos devem ser estabelecidas e formalizadas, abordando os seguintes tópicos:

- Correio Eletrônico, Mensageria e Transmissão Segura;
- Equipamentos pessoais - BYOD (Bring your Own Device);
- Recursos corporativos (onedrive, sistemas, aplicações, notebook, celular);
- Instalação de softwares;
- Hardware;
- Tratamento de exceções.

Regras para o tratamento dos ativos devem ser estabelecidas e formalizadas, abordando as seguintes operações:

- Armazenamento;
- Classificação de dados e informações;
- Descarte;
- Rotulagem;
- Transferência física.



### 8.3. Backup

Uma Política de Gestão de Backup, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

As cópias de segurança, bem como suas mídias, deverão ser classificadas de acordo com as regras estabelecidas para o Tratamento de Dados e Informações Corporativas.

As cópias de segurança deverão ser realizadas, de acordo com a estratégia definida e formalizada no Plano Operacional de Backup e *Restore*.

### 8.4. Continuidade de Negócios

Uma Política de Gestão de Continuidade de Negócios, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

Um Plano de Continuidade de Negócios, contendo os princípios básicos e a estrutura necessária para assegurar a resposta de emergência, retomada, restauração e recuperação permanente das operações e atividades essenciais da RTM, deverá ser formalizado.

Deverão ser identificados e atendidos os requisitos necessários para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas em que a RTM possa estar. Além disso, deverão ser estabelecidos e implementados os processos, procedimentos e controles para manter a segurança da informação em momentos adversos.

Cenários de riscos disruptivos devem ser identificados e testados.

Planos de tratamento e respostas a eventos adversos, como emergência, crise e recuperação de desastres, devem ser elaborados, respeitados e seguidos.

### 8.5. Criptografia e Chaves

Uma Política de Gestão de Criptografia e Chaves, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

Padrões fortes de criptografia deverão ser utilizados para proteção de dados e informações em trânsito e em descanso.

Além disso, deverá ser realizada a gestão de todo o ciclo de vida das chaves criptográficas, inclusive o cerimonial de chaves, quando necessário.

### 8.6. Eventos

Uma Política de Gestão de Eventos, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida. As principais diretrizes, não limitando-se, são:



O *hub integrador* do  
mercado financeiro

- A RTM deverá registrar e monitorar o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. Os critérios e requisitos estabelecidos nesta política deverão ser aplicados em todas as áreas da RTM.

Diretrizes relacionadas ao monitoramento do ambiente, deverão ser definidas e abordar os seguintes temas:

- Sistema de monitoramento no ambiente operacional;
- Mecanismos e/ou sistemas que assegurem práticas de prevenção, detecção e/ou correção para garantir a segurança da informação.

Diretrizes relacionadas registros de eventos, deverão ser definidas e abordar os seguintes temas:

- Registro (log) das atividades: do usuário, de exceções, de falhas e de eventos de segurança da informação;
- Proteção e análise de registros (logs).

## 8.7. Fornecedores

Uma Política de Gestão de Fornecedores, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida. As principais diretrizes, não limitando-se, são:

- Deverá ser formalizado um processo de contratação de fornecedores e prestadores de serviços;
- Deverá ser acordado, e documentado, com os fornecedores os requisitos de segurança da informação para acesso aos ativos da RTM;
- Os fornecedores deverão ser monitorados e avaliados e, em todas as operações devem ser contemplados os riscos de segurança da informação associados a cadeia de suprimentos.

Os requisitos de segurança deverão ser definidos e acordados com os fornecedores.

Os fornecedores deverão ser monitorados e avaliados.

## 8.8. Incidentes de TIC e Segurança da Informação

Uma Política de Gestão de Incidentes, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida. As principais diretrizes, não limitando-se, são:

- O tratamento e resposta a incidentes deverá ser realizado de acordo com o planejamento formalizado no Plano de Tratamento e Resposta a Incidentes;
- Deverão ser mantidas estratégias e documentados procedimentos para conter, erradicar e responder incidentes, e também para recuperar o ambiente;
- Canais de comunicação devem ser disponibilizados, internamente e externamente, e utilizados para reportar incidentes;
- Cenários de incidentes de segurança da informação devem ser identificados e testados.



## 8.9. Mudanças

Uma Política de Gestão de Mudanças, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

Regras para mudanças tecnológicas e organizacionais que afetam a segurança da informação deverão ser estabelecidas e formalizadas.

## 8.10. Orientações aos Usuários Finais

Devem ser passadas orientações aos usuários finais, buscando aumentar a eficácia e eficiência da SGSI - Sistema de Gestão de Segurança da Informação, sobre os seguintes temas:

- **Uso Aceitável dos Ativos**

As regras estabelecidas para o uso aceitável dos ativos devem ser comunicadas e respeitadas.

- **Mesa Limpa e Tela Limpa**

Orientações sobre Mesa Limpa e Tela Limpa deve ser elaboradas, comunicadas, respeitadas e seguidas.

- **Dispositivos Móveis**

Regras para uso de dispositivos móveis pessoais deverão ser estabelecidas, comunicadas e respeitadas;

Medidas de segurança para gerenciar riscos pela utilização de dispositivos móveis deverão ser implementadas.

- **Trabalho Remoto**

Regras para trabalho remoto deverão ser estabelecidas, comunicadas e respeitadas;

Medidas de segurança para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto deverão ser implementadas.

- **Restrições de Uso e Instalação de Softwares**

As regras estabelecidas para o uso aceitável dos ativos devem ser comunicadas e respeitadas.

## 8.11. Propriedade Intelectual

Uma Política de Propriedade Intelectual, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida, abordando, no mínimo, os seguintes temas:

- Tratamento da informação produzida ou recebida pelos colaboradores ou terceiros;
- Uso de quaisquer materiais, códigos, informações ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo com a empresa;
- Disponibilização ou transferência de software para terceiros.



## 8.12. Proteção contra *Malware*

A Proteção contra *Malware* visa proteger as informações e os recursos que processam as informações.

Um sistema de proteção contra malware deve ser instalado e configurado no ambiente operacional da RTM.

Deverão ser implementados controles para: prevenção, detecção e recuperação para proteger o ambiente operacional contra *malware*.

As regras aplicadas e os controles implementados deverão ser documentados.

Um programa de conscientização para os usuários deverá ser executado.

## 8.13. Prevenção e Detecção de Intrusão

Um sistema automatizado deverá ser instalado para prevenção e detecção de invasões.

Medidas para prevenção e detecção de invasões deverão ser implementadas.

Um sistema automatizado deverá ser utilizado como auxílio para gerar alertas sempre que houver suspeitas de comprometimento do ambiente operacional.

## 8.14. Proteção e Privacidade de Dados

Uma Política de Privacidade e Proteção de Dados Pessoais, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

Devem ser definidos como os dados pessoais são tratados, coletados, utilizados e divulgados pela RTM.

Um canal deve ser disponibilizado para os donos dos dados entrarem em contato.

Medidas técnicas e controles apropriados para proteção devem ser implementados para garantir a segurança dos dados.

A fim assegurar a prevenção de vazamento de dados, a transferência de dados pessoais e sensíveis deve ocorrer de acordo com as regras estabelecidas.

Um sistema automatizado deverá ser utilizado como auxílio para garantir que as regras estabelecidas na Política de DLP (*Data Loss Prevention*) sejam seguidas.



O *hub integrador* do  
mercado financeiro

## 8.15. Redes

Para não trazer riscos a operação e garantir a segurança nas comunicações, as redes da RTM deverão ser gerenciadas e os seguintes **controles de redes** implementados:

- Restrição de conexão de sistemas e de dispositivos, devendo ser permitidas apenas as conexões que atendam aos requisitos de segurança definidos;
- Autenticação em nível de rede;
- Controles especiais para proteção da confidencialidade e integridade dos dados que trafegam sobre redes públicas ou sobre as redes sem fio (wireless);
- Proteção dos sistemas e aplicações conectados as redes públicas ou as redes sem fio (wireless);
- O acesso remoto à rede corporativa da RTM, principalmente a sistemas críticos, deve ocorrer por meio da VPN – Virtual Private Network (Rede Privada Virtual) ou aplicativo de conexão remota baseado em ZTNA;
- Sistemas SaaS poderão ser acessados por meio da VPN, desde que tenham sido previamente analisados e parametrizados pela Gerência de Segurança da Informação.

A **segmentação da rede** deve ser estabelecida e documentada, contemplando as definições para as redes físicas e lógicas e a definição do perímetro de cada domínio.

**Serviços de rede** incluem o fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede gerenciadas como firewalls e sistemas de detecção de intrusos. Definições de segurança para estes serviços, deverão ser identificadas e documentadas.

## 8.16. Riscos

Uma Política complementar de Gestão de Riscos, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

Regras para a gestão de riscos devem ser estabelecidas e formalizadas, abordando o tratamento dos seguintes tipos:

- Riscos de segurança da informação;
- Riscos cibernéticos.

## 8.17. Segurança Física e do Ambiente

Uma Política de Segurança Física e do Ambiente, com diretrizes complementares a esta Política, deve ser elaborada, respeitada e seguida, abordando, no mínimo, os seguintes temas:

- Definição dos perímetros de segurança física a serem protegidos;
- Controles de acesso nos ambientes físicos da RTM;
- Controles contra desastres naturais;
- Definição de áreas de entrega e carregamento.



## 8.18. Segurança em Nuvem

Como parte da estratégia da RTM, o uso de serviços em nuvem é utilizado para ganho de disponibilidade e confiabilidade.

Para assegurar a conformidade com os requisitos de segurança da informação, devem ser seguidas as principais diretrizes, não limitando-se:

- Os ambientes virtuais devem ser classificados em níveis de segurança;
- A classificação deverá ser realizada entre a equipe responsável pela infraestrutura em nuvem e a Gerência de Segurança da Informação;
- O controle de acesso lógico deverá ser realizado;
- Todo novo serviço deve ser comunicado a Gerência de Segurança da Informação antes de sua contratação e utilização.

## 8.19. Sistemas e Aplicações

Uma Política de Gestão de Sistemas, com diretrizes complementares a esta Política, deverá ser elaborada, respeitada e seguida.

Diretrizes e regras para o desenvolvimento de sistemas e aplicações devem ser estabelecidas e formalizadas, abordando os seguintes tópicos:

- Desenvolvimento seguro;
- Metodologia de desenvolvimento e manutenção de sistemas.

As gerências responsáveis por desenvolvimento e manutenção de sistemas devem acionar a Gerência de Segurança da Informação para assegurar que os padrões utilizados no desenvolvimento de sistemas e aplicações estejam alinhados com a estratégia geral de segurança da informação, bem como ao apetite a riscos da RTM.

## 8.20. Testes de Segurança

A RTM deve realizar testes internos e externos de controles de segurança, para assegurar a conformidade dos requisitos, e documentar as evidências da execução.

## 8.21. Tratamento de Desvios e Exceções

Deve ser formalizado e comunicado um processo disciplinar, para tomar ações contra colaboradores e terceiros que tenham cometido uma violação de segurança da informação.

As sanções disciplinares serão estabelecidas pelo Comitê Estratégico de Governança, Riscos e Compliance.

Todas as sanções serão aplicadas de acordo com as regras estabelecidas na norma de Gestão de Denúncias, Investigações e Consequências, com os demais normativos da RTM e com a legislação vigente.



O *hub integrador* do  
mercado financeiro

## 8.22. Vulnerabilidades Técnicas

Regras para a gestão de vulnerabilidades técnicas devem ser estabelecidas e formalizadas, abordando:

- Integração com o processo de gestão de ativos de TIC;
- Categorização e classificação de vulnerabilidades;
- Execução de varreduras periódicas ou na ocorrência de mudanças;
- Prazo de resposta para o tratamento das vulnerabilidades identificadas;
- Os processos e procedimentos formais devem ser implementados, para: identificar, analisar e avaliar, responder, comunicar e monitorar as vulnerabilidades técnicas;
- Devem ser executados testes no ambiente operacional da RTM.

## 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 desta norma 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

- Política de Gestão de Identidade e Acessos
- Política de Gestão de Ativos
- Política de Gestão de Backup
- Política de Gestão de Continuidade de Negócios
- Política de Gestão de Criptografia e Chaves
- Política de Gestão de Eventos
- Política de Gestão de Fornecedores
- Política de Gestão de Incidentes
- Política de Gestão de Mudanças
- Política de Privacidade e Proteção de Dados Pessoais
- Política de Gestão de Sistemas
- Política de Relacionamento com Terceiros