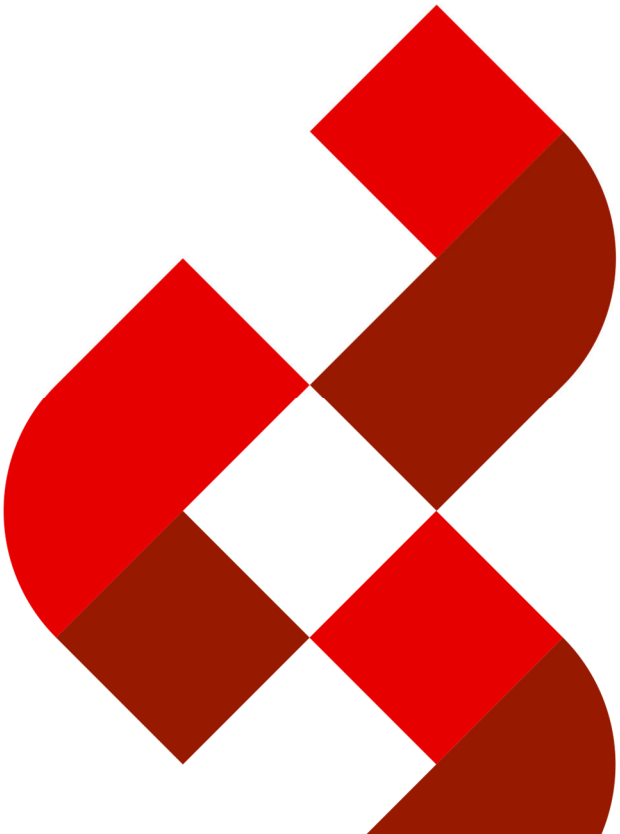
Política de Gestão de Incidentes



POLÍTICA CORPORATIVA

v2.1 - 2024

SUMÁRIO

DOCUMENTO PÚBLICO

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

SIGLAS, ABREVIAÇÕES E DEFINIÇÕES

TERMO	DESCRIÇÃO
Continuidade de Negócios	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
Erradicação	Eliminação de vetores causadores do incidente de segurança da informação
Estratégias de Contenção	Documento que estabelece estratégia e procedimentos para conter, reprimir e controlar um incidente de segurança da informação
Estratégias de Recuperação do Ambiente	Documento que incorpora o roteiro de recuperação para garantir a restauração, de forma controlada, dos sistemas ou ativos afetados pelo incidente de segurança da informação
Evento de Segurança da Informação	É uma ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação
Gestão de Riscos	Desenvolvimento estruturado e aplicação de uma cultura de gestão, políticas, procedimentos e práticas às tarefas de identificação, análise e controle dos riscos
Impacto	Consequência avaliada de um evento em particular
Incidente	Situação que pode representar ou levar a uma interrupção de negócios, perdas, emergências ou crises
Incidente de Segurança da Informação	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
Malware	Definição genérica para qualquer software de computador com intenção maliciosa
Organização	Grupo de pessoas e instalações com uma série de responsabilidades, autoridades e relacionamentos. Exemplo: Companhia, corporação, firma, empresa, instituição de caridade, profissional liberal ou associação, ou partes ou combinações destas
Partes interessadas	Aqueles que possuem algum interesse nos resultados de uma organização
Processo	Atividade ou conjunto de atividades executados por uma organização que produzem ou suportem um ou mais produtos ou serviços
Risco	Algo que pode ocorrer e seus efeitos nos objetivos da organização
Segurança da Informação (S.I.)	Conjunto de ações e boas práticas com o objetivo de proteger os ativos da organização
TIC	Tecnologia da Informação e Comunicação

1. INTRODUÇÃO

1.1. RESUMO

A Política de Gestão de incidentes visa descrever as diretrizes necessárias para prover a gestão dos incidentes de TIC e segurança da informação antes, durante e após os eventos.

1.2. APLICAÇÃO

Às empresas RTM:

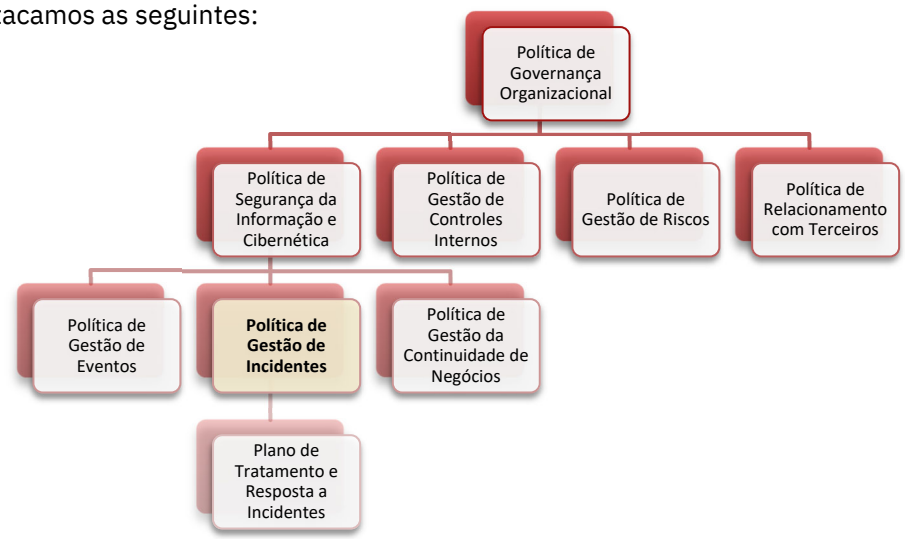
- RTM Rede de Telecomunicações do Mercado Ltda; e
- RTM Infraestrutura em Tecnologia da informação Ltda.

1.3. REQUISITOS ESTATUTÁRIOS E REGULAMENTARES

- ABNT NBR **ISO/IEC 27.002** (Código de prática para controles de segurança 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)
- BACEN **Resolução 304** (disciplina, no âmbito do Sistema de Pagamentos Brasileiro, o funcionamento dos sistemas de liquidação, entre outros)
- **CIS Controls v8** (Consiste em 18 medidas abrangentes que ajudam a fortalecer sua postura de segurança cibernética)
- **LEI 13.709/18** (Lei geral de proteção de dados - LGPD)
- **NIST SP 800-53** (Controles de segurança e privacidade para sistemas de informação)
- **NIST SP 800-61** (Guia de tratamento de incidentes de segurança)
- **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 Incidentes 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 Gestão de Incidentes descrevem as funções exercidas pelos colaboradores da RTM que atuam diretamente neste processo.

2.1. Diretoria de Operações

Compete à Diretoria de Operações:

- Estabelecer e comunicar formalmente os papéis, responsabilidades e níveis de autoridades da estrutura de gestão de incidentes de TIC;
- Assegurar o envolvimento de colaboradores qualificados no estabelecimento, implementação e manutenção dos procedimentos e processos de incidentes de TIC.

2.2. Diretoria de Unidade de Nuvem

Compete à Diretoria de Unidade de Nuvem:

- Estabelecer e comunicar formalmente os papéis, responsabilidades e níveis de autoridades da estrutura de gestão de incidentes de segurança da informação;
- Assegurar o envolvimento de colaboradores qualificados no estabelecimento, implementação e manutenção dos procedimentos e processos de incidentes de segurança da informação.

2.3. Comitê Estratégico de Governança, Riscos e Compliance

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

- Estabelecer as diretrizes para a governança da segurança da informação;
- Analisar o relatório gerencial de incidentes.

2.4. Comitê Executivo de TIC

Compete ao Comitê Executivo de TIC a função de **direcionador estratégico e aprovador**, além das seguintes atribuições:

- Estabelecer as diretrizes para a gestão de incidentes de TIC e SI;
- Definir ferramentas e tecnologias que assegurem eficiência e eficácia na prevenção, no monitoramento, na resolução e no pós-incidente de TIC;
- Analisar o alerta de emergência e, quando necessário, acionar o processo de Gerenciamento da Continuidade de Negócios;
- Aprovar a Política e Planos de Gestão de Incidentes.

2.5. Gerência de Segurança da Informação

Compete a Gerência de Segurança da Informação a função de **proprietária e gestora** do processo Gerenciar Incidentes de SI e as seguintes atribuições:

- Definir e catalogar os incidentes de SI a serem monitorados;
- Planejar a notificação de incidentes de segurança da informação;
- Definir e disponibilizar os canais de comunicação, internamente e externamente, para relatos de incidentes de segurança da informação;
- Definir ferramentas e tecnologias que assegurem eficiência e eficácia na prevenção, no monitoramento, na resolução e no pós-incidente de SI;
- Estabelecer e documentar as ações e os procedimentos operacionais para resposta a incidentes de SI;
- Implantar controles de segurança da informação de acordo com os requisitos mapeados;
- Parametrizar as ferramentas para monitorar o ambiente operacional para identificar e gerar alerta da ocorrência de incidentes de SI;
- Elaborar o relatório anual sobre incidentes, reportando dados e a efetividade do processo de Gerenciamento de Incidentes de SI;
- Planejar o programa de conscientização, treinamento e/ou educação em segurança da informação para as partes interessadas.

2.6. Gerência de Suporte ao Cliente

Compete a Gerência de Suporte ao Cliente a função de **proprietária e gestora** do processo Gerenciar Incidentes de TIC e as seguintes atribuições:

- Planejar a notificação de incidentes de TIC;
- Definir e disponibilizar os canais de comunicação, internamente e externamente, para relatos de incidentes de TIC;
- Estabelecer e documentar as ações e os procedimentos operacionais para resposta a incidentes de TIC;
- Implantar controles de TIC acordo com os requisitos mapeados;
- Elaborar o relatório anual sobre incidentes, reportando dados e a efetividade do processo de Gerenciamento de Incidentes de TIC.

2.7. Gerências de TIC

Compete as Gerências de TIC designadas como proprietárias de ativos de TIC as seguintes atribuições:

- Definir e catalogar os incidentes de TIC a serem monitorados;
- Implantar controles de TIC de acordo com os requisitos mapeados;
- Parametrizar as ferramentas para monitorar o ambiente operacional para identificar e gerar alerta da ocorrência de incidentes de TIC.

2.8. Equipe de Atendimento

- Realizar a triagem, avaliando os eventos e assegurando o correto escalonamento.

2.9. Equipe de Tratamento e Resposta a Incidentes

- Assegurar o registro dos incidentes e das atividades relacionadas durante todo o seu ciclo de vida;
- Assegurar a categorização e classificação do incidente;
- Realizar a análise, investigação e o diagnóstico do incidente, compreendendo o seu impacto;
- Realizar, quando necessário, a contenção do incidente para atenuar os danos e impedir o comprometimento de outros recursos;
- Erradicar os componentes que causaram o incidente;
- Assegurar, caso o ambiente continue comprometido, o correto escalonamento conforme situação atual do incidente;
- Recuperar o ambiente operacional para o seu estado de normalidade de forma controlada;
- Comunicar o encerramento para as partes interessadas;
- Assegurar o correto arquivamento da solução;
- Manter a base de conhecimento de incidentes (lições aprendidas) atualizada.

2.10. Gerência de Governança de TIC

- Coordenar os planos relacionados à Gestão de Incidentes de TIC e S.I;
- Desenvolver um processo para modificar e aprimorar o plano de tratamento e resposta a incidentes, de acordo com as lições aprendidas;
- Assegurar que o programa de conscientização, treinamento e/ou educação em segurança da informação para as partes interessadas seja documentado e executado anualmente;
- Revisar e atualizar os mecanismos de acompanhamento e controles internos do processo.

2.11. Gerência de Governança, Riscos e Compliance

- Assegurar a realização periódica de testes de segurança, durante o ciclo do Plano de Continuidade de Negócios - PCN, incluindo o cenário de ataque cibernético e atualizar os mecanismos de acompanhamento e controles.

3. OBJETIVOS

A Política de Gestão de Incidentes de estabelece diretrizes, responsabilidades e orientações sobre o funcionamento do processo, de forma que os incidentes sejam prevenidos, monitorados, detectados, tratados e encerrados com a finalidade de atenuar ao máximo o impacto nos ativos e consequentemente nos negócios da RTM.

4. METODOLOGIA

A metodologia de Gestão de Incidentes de TIC e S.I implantada na RTM baseia-se nos princípios apresentados no item 1.3 – requisitos estatutários e regulamentares – e tem como objetivo buscar a prevenção e atenuação dos impactos de incidentes por meio de procedimentos e a melhoria contínua do seu processo.

5. ESCOPO

Esta Política abrange os seguintes incidentes, mas não limitando-se a estes:

- SI - Segurança da Informação:
    - Qualquer vulnerabilidade técnica ou evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, redes de computadores, bem como as estruturas físicas e lógica associadas, que comprometa um ou mais princípios básicos da segurança da informação: confidencialidade, integridade, disponibilidade e conformidade;
    - Indisponibilidade do ambiente tecnológico em virtude de, por exemplo, ataque cibernético;
    - Violação de dados confidenciais (informações de clientes, informações estratégicas, dados pessoais, outros);
    - Tentativas ou acessos não autorizados;
    - Violação, explícita ou implícita, de políticas de TIC;
    - Modificações em ativos de TIC, sem o conhecimento, instruções ou consentimento prévio do dono do ativo;
    - Compartilhamento de senhas.
- TIC – Tecnologia da Informação e Comunicação
    - Interrupção não prevista ou programada de um serviço de TIC;
    - Queda da qualidade de um serviço de TIC;
    - Indisponibilidade.

6. DIRETRIZES GERAIS

6.1. Estrutura de Gestão de Incidentes

- A Gerência de Segurança da Informação foi designada como responsável pelo processo de Gerenciamento de Incidentes de segurança da informação;
- A Gerência de Suporte ao Cliente foi designada como responsável pelo processo de Gerenciamento de Incidentes de TIC;
- Os demais papéis, responsabilidades e autoridades na gestão de incidentes 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 Incidentes;
- Devem ser alocados recursos humanos com habilidade, experiência e competência em segurança da informação.

6.2. Conscientização, Educação e Treinamento

- Todos os colaboradores e terceirizados da RTM devem estar cientes da relevância e importância de suas atividades dentro do processo de Gerenciamento de Incidentes de TIC e Segurança da Informação;
- Realizar treinamentos para toda equipe, de acordo com suas responsabilidades dentro do processo.

6.3. Melhoria Contínua

- A gestão do processo de Gerenciamento de Incidentes de TIC e Segurança da Informação deverá ser contínua e sistematicamente atualizada;
- O plano de tratamento e respostas a incidentes deve ser revisado e testado anualmente ou sempre que modificações significativas ocorrerem;
- Os recursos e as documentações do processo de Gerenciamento de Incidentes de TIC e Segurança da Informação devem ser mantidos para garantir que permaneçam eficazes e alinhados com as prioridades do negócio, além de garantir a geração das evidências necessárias;
- Os dados sobre os incidentes ocorridos devem ser mantidos, documentados e, quando necessário, submetidos ao Comitê Estratégico de Governança, Riscos e Compliance, aos órgãos fiscalizadores solicitantes e aos demais envolvidos na ocorrência.

7. DIRETRIZES ESPECIFICAS

7.1. Gestão e Planejamento de Incidentes

- Deve ser implementado e mantido um catálogo de incidentes, incluindo a categorização e a classificação dos incidentes;
- Deve-se definir, disponibilizar e comunicar aos clientes internos e externos os canais apropriados para relatar incidentes;
- Devem ser instituídas regras que estabeleçam os processos de gestão para tratamento e respostas a incidentes;
- Deve ser documentado um plano de tratamento e respostas a incidentes, bem como os procedimentos operacionais relacionados a contenção, erradicação e recuperação, além de comunicado para todas as partes interessadas;
- Deve ser instituída e mantida a equipe de tratamento e resposta a incidentes;
- Deve ser planejado, implementado e documentado um processo de notificação de eventos adversos (incidentes).

7.2. Tratamento e Resposta a Incidentes

- O ambiente operacional deve ser monitorado continuamente por meio de ferramentas e/ou tecnologias que auxiliem na geração de alertas de eventos;
- Os eventos adversos devem ser avaliados e escalonados para o processo de gestão de incidentes;
- O escalonamento deve ser feito com base nas informações de todo o ciclo de vida do incidente até o momento, definindo o encaminhamento para o processo que melhor responder a situação atual;
- Os incidentes devem ser registrados e atualizados desde o momento de sua detecção até a sua resolução final, sendo armazenado todas as evidências;
- Os incidentes devem ser classificados, categorizados e priorizados de acordo com um padrão pré-estabelecido;
- Os incidentes, após confirmados, devem ser analisados, investigados e diagnosticados sua causa-raiz;
- Os incidentes devem, sempre que necessário e possível, ser contidos para impedir a sua expansão;
- Deve-se erradicar e eliminar os componentes dos incidentes;
- O ambiente deve ser restaurado ao seu estado de normalidade;

- O Comitê Executivo de TIC deverá ser notificado sempre que for identificado um incidente classificado como grave ou o tempo de resolução ter excedido o prazo pré-estabelecido;
- O GT | Resiliência Operacional, pertencente ao Comitê Estratégico de Governança, Riscos e Compliance, deverá ser notificado sempre que for identificado um incidente classificado como muito grave e extremamente grave.

7.3. Encerramento de Incidentes

- O chamado técnico deve ser atualizado, inclusive com as evidências e soluções aplicadas, e encerrado;
    - Análises de problemas pós-incidentes devem ser realizadas sempre que a causa-raiz não for constatada, o incidente deve ser vinculado ao problema, para garantia da identificação e da correção definitiva de vulnerabilidades técnicas.
- As partes interessadas devem ser comunicadas sobre o encerramento do chamado técnico;
- As soluções devem ser documentadas na base de conhecimento sempre que possível.

8. PENALIDADES

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

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

ANEXOS

- **ANEXO I:** Matriz de Responsabilidades (RACI)
- **ANEXO II:** Plano de Tratamento e Resposta a Incidentes