DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

rtm

Política de Gestão de Incidentes de Segurança da Informação

POLÍTICA CORPORATIVA

v2.0 - 2023

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

SUMÁRIO

SIGLAS, ABREVIAÇÕES E DEFINIÇÕES 3

1. INTRODUÇÃO 4

2. PAPÉIS E RESPONSABILIDADES 5

3. OBJETIVOS 8

4. METODOLOGIA 8

5. ESCOPO 8

6. DIRETRIZES GERAIS 9

6.1. Estrutura de Gestão de Incidentes 9

6.2. Manutenções e Melhoria Contínua 9

6.3. Conscientização, Educação e Treinamento 9

7. DIRETRIZES ESPECIFICAS 10

7.1. Gestão e Planejamento de Incidentes 10

7.2. Tratamento e Resposta a Incidentes 10

7.3. Encerramento de Incidentes 11

8. PENALIDADES 11

CONTROLES DO DOCUMENTO 13

DOCUMENTO PÚBLICO

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

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

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

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

1. INTRODUÇÃO

1.1. RESUMO

A Política de Gestão de incidentes de segurança da Informação visa descrever as diretrizes necessárias para prover a gestão dos incidentes de segurança da informação a 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 EIRELI.

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)
- **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 v3.2.1** (Padrão de segurança de dados da indústria de cartões de pagamento)
- **SWIFT SIP v3** (Programa de segurança do cliente da Sociedade de Telecomunicações Financeiras Interbancárias Mundiais)

1.4. DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA

A Política de Gestão de Incidentes de Segurança da Informação está alinhada às demais políticas da organização, dentre as quais destacamos as seguintes:

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

2. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades definidos nessa Política de Gestão de Incidentes de Segurança da Informação 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 segurança da informação;
- Assegurar o envolvimento de colaboradores qualificados no estabelecimento, implementação e manutenção dos procedimentos e processos de incidentes de segurança da informação.

2.2. 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 de segurança da informação.

2.3. 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 segurança da informação;
- Emitir, quando necessário, o alerta de emergência para acionar o processo de Gerenciamento de Continuidade do Negócio;
- Aprovar a Política e planos de Gestão de Incidentes de Segurança da Informação.

2.4. Gerência de Segurança da Informação

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

- Definir e catalogar os incidentes de segurança da informação a serem monitorados;
- Planejar a notificação 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;

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

- Estabelecer e documentar as ações e os procedimentos operacionais para resposta a incidentes;
- Implantar controles de segurança da informação de acordo com os requisitos mapeados;
- Monitorar o ambiente operacional para identificar e gerar alerta da ocorrência de incidentes de segurança da informação;
- Elaborar o relatório anual sobre incidentes, reportando dados e a efetividade do processo de Gerenciamento de Incidentes de Segurança da Informação;
- Planejar o programa de conscientização, treinamento e/ou educação em segurança da informação para as partes interessadas.

2.5. Equipe de Atendimento

- Realizar a triagem, avaliando os eventos de segurança da informação e assegurando o correto escalonamento.

2.6. Equipe de Tratamento e Resposta a Incidentes

- Assegurar o registro dos incidentes de segurança da informação e das atividades relacionadas durante todo o seu ciclo de vida;
- Assegurar a categorização e classificação do incidente de segurança da informação;
- Realizar a análise, investigação e o diagnóstico do incidente de segurança da informação, compreendendo o seu impacto;
- Realizar, quando necessário, a contenção do incidente de segurança da informação para atenuar os danos e impedir o comprometimento de outros recursos;
- Erradicar os componentes que causaram o incidente de segurança da informação;
- Assegurar, caso o ambiente continue comprometido, o correto escalonamento conforme situação atual do incidente de segurança da informação;
- 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.

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

2.7. Gerência de Governança de TIC

- Coordenar os planos relacionados à Gestão de Incidentes de Segurança da Informação;
- Desenvolver um processo para modificar e aprimorar o plano de tratamento e resposta a incidentes, de acordo com as lições aprendidas e para incorporar os desenvolvimentos na área de segurança da informação;
- 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.

2.8. 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.

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

3. OBJETIVOS

A Política de Gestão de Incidentes de Segurança da Informação estabelece diretrizes, responsabilidades e orientações sobre o funcionamento do processo, de forma que os incidentes de segurança da informação 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 Segurança da Informação 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 de segurança da informação por meio de procedimentos e a melhoria contínua do seu processo.

Figura 1 - Ciclo de vida da gestão de incidentes de S.I.

5. ESCOPO

Esta Política abrange os incidentes de segurança da informação. São considerados incidentes de segurança da informação, mas não limitando-se a estes:

- 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 ataque cibernético;
- Violação de dados confidenciais (informações de clientes, informações estratégicas, dados pessoais, outros);
- Tentativas interna ou externa de acesso não autorizado;
- Uso ou acesso não autorizado a um sistema;
- Violação, explícita ou implícita, de políticas de TIC;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- Compartilhamento de senhas.

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

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;
- Os demais papéis, responsabilidades e autoridades na gestão de incidentes de segurança da informação 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 de Segurança da Informação;
- Devem ser alocados recursos humanos com habilidade, experiência e competência em segurança da informação.

6.2. Manutenções e Melhoria Contínua

- A gestão do processo de Gerenciamento de Incidentes de 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 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 submetidos ao Comitê Estratégico de Governança, Riscos e Compliance, aos órgãos fiscalizadores solicitantes e aos demais envolvidos na ocorrência.

6.3. 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 Segurança da Informação;
- Realizar treinamentos para toda equipe, de acordo com suas responsabilidades dentro do processo.

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

7. DIRETRIZES ESPECIFICAS

7.1. Gestão e Planejamento de Incidentes

- Deve ser implementado e mantido um catálogo de incidentes de segurança da informação, incluindo a categorização e a classificação dos incidentes;
- Devem ser instituídas regras que estabeleçam os processos de gestão para tratamento e respostas a incidentes de segurança da informação;
- 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 de segurança da informação (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 de segurança da informação;
- 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 de segurança da informação até o momento atual, 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 e categorizados de acordo com um padrão pré-estabelecido;
- Os incidentes, após confirmados, devem ser analisados, investigados e diagnosticados sua causa-raiz;
- 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.

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

7.3. Encerramento de Incidentes

- O chamado técnico só deve ser encerrado após resolução do problema e atualização do registro do incidente - com a inclusão de evidências e soluções aplicadas;
- As partes interessadas devem ser comunicadas sobre o encerramento do chamado técnico;
- Análises de problemas pós-incidentes devem ser realizadas, sempre que a causa-raiz não for constatada, para garantia da identificação e da correção de vulnerabilidades técnicas;
- Uma base de conhecimento de incidentes deve ser criada, atualizada e utilizada.

8. PENALIDADES

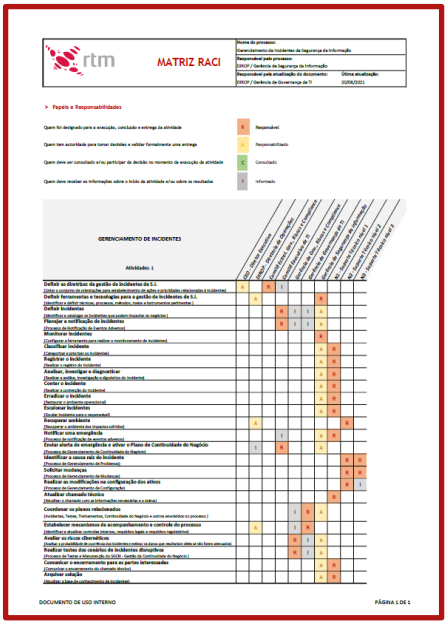
Violações a este normativo estão sujeitas a sanções disciplinares estabelecidas pela RTM e Legislações Vigentes, e serão decididas caso a caso pelo Comitê Estratégico de Governança, Riscos e Compliance.

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).

DocuSign Envelope ID: 48AC03E4-5B50-4E9D-9A86-0BF20B58B3B3

ANEXOS

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



MATRIZ RACI

Nome do processo: Gerenciamento de Incidentes de Segurança da Informação
Responsável pelo processo: DRCP / Gerência de Segurança da Informação
Responsável pela atualização do documento: DRCP / Gerência de Governança de TI
Última atualização: 20/08/2021

> Papéis e Responsabilidades

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

GERENCIAMENTO DE INCIDENTES

Atividades 1	CSO - Chief Security Officer	Gerente de Segurança da Informação	Analista de Segurança da Informação	Analista de Suporte Técnico 1 (Helpdesk)	Analista de Suporte Técnico 2	Analista de Suporte Técnico 3	Analista de Segurança da Informação	Gerente de Segurança da Informação	N1 - Analista Técnico Nível 1	N2 - Analista Técnico Nível 2	N3 - Analista Técnico Nível 3
Definir as diretrizes da gestão de incidentes da S.I. (Criar e contemplar as orientações para estabelecimento de ações e prioridades relacionadas à incidentes)	A		R	I				I			
Definir ferramentas e tecnologias para a gestão de incidentes de S.I. (Identificar e definir recursos, processos, métodos, meios e instrumentos participantes)		A					R				
Definir incidentes (Definir o escopo de incidentes que podem impactar os negócios)				R	I	I	A				
Planejar a notificação de incidentes (Processo de Notificação de Eventos Adversos)				R	I	I	A				
Monitorar incidentes (Configurar e ferramenta para realizar o monitoramento de incidentes)							R				
Classificar incidente (Categorizar a criticidade do incidente)							A	R			
Registrar o incidente (Registrar o incidente na ferramenta)							A	R			
Analisar, investigar e diagnosticar (Realizar a análise, investigação e diagnóstico do incidente)							A	R			
Conter o incidente (Realizar a contenção do incidente)							A	R			
Erradicar o incidente (Remover o ambiente operacional)							A	R			
Escalonar incidentes (Escalar incidentes para o responsável)							A	R			
Recuperar o ambiente (Recuperar o ambiente dos impactos sofridos)		A								R	
Notificar uma emergência (Processo de notificação de eventos adversos)				I			A	R			
Enviar alerta de emergência e ativar o Plano de Continuidade do Negócio (Processo de Gerenciamento de Continuidade do Negócio)		I		R			A				
Identificar a causa raiz do incidente (Processo de Gerenciamento de Problemas)										R	R
Análise Forense (Processo de Gerenciamento de Incidentes)										R	R
Realizar as modificações na configuração dos ativos (Processo de Gerenciamento de Configuração)										R	I
Atualizar chamado técnico (Atualizar o chamado com as informações recuperadas e o status)								R			
Coordenar os planos relacionados (Incidentes, Testes, Treinamentos, Continuidade do Negócio e outros envolvidos no processo)					I	R	A				
Estabelecer mecanismos de acompanhamento e controle do processo (Identificar e avaliar controles internos, requisitos legais e requisitos regulatórios)		A			I	R					
Analisar os riscos cibernéticos (Avaliar a probabilidade de ocorrência de incidentes e estimar os danos que resultarão deles e são fonte ameaças)					R	I	A				
Realizar testes dos cenários de incidentes disruptivos (Processo de Teste e Manutenção do SGCN - Gestão de Continuidade do Negócio)					R	I	A				
Comunicar o encerramento para as partes interessadas (Simplificar o encerramento do chamado técnico)							A	R			
Ampliar análise (Atualizar a base de conhecimento de incidentes)							A	R			

DOCUMENTO DE USO INTERNO — PÁGINA 1 DE 1

rtm

Plano de Tratamento e Resposta a Incidentes de Segurança da Informação

PLANO TÁTICO

v5.0 - 2023