Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá

Anexo VIII - Norma para Plano de Resposta a Incidentes

Maricá, abril de 2025

Presidente

Cláudio de Souza Gimenez

Diretor de Infraestrutura

Laércio Aguiar da Rocha

Equipe Técnica

Emerson Lacerda Alencar

Giovanni Di Carlo

Márcio Santarém Nogueira

Histórico de Revisões

Versão	Data	Histórico	Autor	Revisor
1.0	abril de 2025	Versão inicial	Emerson L. Alencar Márcio S. Nogueira	Laércio A. Rocha

Sumário

1. PREMISSAS

1.1. É fundamental que todos os servidores públicos, diretorias, fornecedores, prestadores de serviços e demais parceiros vinculados compreendam o seu papel crucial no contexto da Segurança da Informação (SI). É um dever seguir rigorosamente as diretrizes e orientações estabelecidas na Política de Segurança da Informação (PSI) do ICTIM, a fim de evitar exposição indevida das informações e dos recursos de processamento a situações adversas, tais como comprometimento, alteração, furto e desvio.

2. CONCEITOS

2.1. Com o avanço tecnológico e a digitalização crescente, as preocupações com incidentes de segurança tornam-se uma prioridade nas organizações. Estar preparado para enfrentar esses eventos é crucial para a continuidade das operações, tornando essencial a elaboração de um plano de ação bem estruturado.

2.2. Em face à A Lei Geral de Proteção de Dados Pessoais (LGPD), ou Lei nº 13.709/2018, além da preocupação com a segurança dos dados que já existia, agora há também os aspectos legais referentes a proteção dos dados pessoais tratados que precisam ser observados, o que tornou a matéria ainda mais importante.

2.3. É essencial compreender que nem todo incidente de segurança envolve dados pessoais; no entanto, todo incidente que envolve dados pessoais é, por definição, um incidente de segurança. Portanto, além da equipe responsável, o Encarregado pelo Tratamento de Dados Pessoais (DPO) deve ser incluído, seguindo as orientações e normas da Autoridade Nacional de Proteção de Dados (ANPD).

2.4. A norma em questão fundamenta-se nas recomendações da ISO 27035, que se divide em três partes, oferecendo orientações detalhadas para a gestão de incidentes. Isso complementa especialmente a ISO 27001 e a ISO 27002, que abordam o Sistema de Gestão de Segurança da Informação e sua implementação.

3. DIRETRIZES

3.1. Competem a Assessoria de TI a implantação de um **Plano de Resposta à Incidentes de Segurança da Informação**, a disponibilização de um Canal para Comunicação de Eventos de Segurança para receber os reportes de eventos de segurança. Esse Canal será o GLPI.

3.2. A Gestão de Incidentes em Segurança da Informação deve ser organizada em um conjunto de processos capazes de contemplar os seguintes itens:

a. Detecção;

b. Aviso;

c. Avaliação;

d. Resposta;

e. Tratamento;

f. Aprendizagem.

3.3. O Canal para Comunicação de Eventos de Segurança deverá ter sua forma de contato anunciada a todo ICTIM de forma a receber os reportes de eventos de Segurança da Informação e dar o destino à equipe especializada contemplando as seguintes fases:

a. Documentação;

b. Triagem;

c. Priorização;

d. Comunicação à Assessoria de TI.

3.4. A Assessoria de TI deve ser composta por corpo técnico capacitado para receber e tratar os eventos de Segurança da Informação envolvendo o Encarregado pelo Tratamento de Dados Pessoais (DPO) sempre que o incidente tenha relação com dados da pessoa natural, sejam estes dados pessoais ou sensíveis.

3.5. O Processo de Gerenciamento de Incidentes deve contemplar um escalonamento e ações de envolvimento de acordo com o tipo do evento, conforme os itens a seguir:

a. Acionamento da Assessoria de TI;

b. Comunicações devidas;

c. Aplicação do Plano de Recuperação de Desastres, quando necessário;

d. Recuperação de um Incidente;

e. Aplicação do Plano de Continuidade de Negócios, quando necessário;

3.6. Os reportes que caracterizarem um **incidente de segurança** devem passar por um processo de gerenciamento de incidentes que envolva:

a. Avaliação;

b. Monitoramento;

c. Classificação;

d. Análise;

e. Ações Corretivas;

f. Relatórios dos Incidentes;

g. Comunicação a todas as partes interessadas internas e externas;

h. Aprendizado e Melhorias.

3.7. Os relatórios criados para controle histórico, aprendizado e aperfeiçoamento deverão conter os seguintes campos:

a. Data e hora;

b. Nome da pessoa que reporta o incidente;

c. Onde ocorreu o incidente;

d. Qual o problema;

e. Qual o efeito que o incidente causou;

f. Como foi descoberto.

3.8. Devem ser construídos procedimentos para auxiliar a Assessoria de TI a lidar com os Incidentes de Segurança através de formulários e orientações que contemplem:

a. Análise do incidente e sua causa;

b. Medidas para minimizar as consequências;

c. Ações para evitar que o incidente ocorra novamente;

d. Quais partes devem ser comunicadas (partes afetadas e partes responsáveis pela solução).

3.9. De acordo com a relevância e gravidade do incidente, a correta coleta de evidências do incidente de segurança é fundamental, não somente para a análise e aprendizado, mas para o respaldo do ICTIM e devidas ações legais que possam ser necessárias. São pontos a serem observados no tratamento de evidências:

a. O envolvido jurídico ou amparo da lei diante de qualquer implicação legal que uma evidência possa ter;

b. Evidências só tem valor legal se são registros completos e se não foram adulteradas sob hipótese alguma;

c. Cópias de provas eletrônicas precisam ser idênticas às originais;

d. Evidências geradas em momentos em que um sistema não está funcionando corretamente têm sua credibilidade comprometida, salvo se esta evidência é exatamente a prova do mau funcionamento do sistema.