Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá

Anexo I - Guia de Boas Práticas para Segurança da Informação

Maricá, abril de 2025

Presidente

Cláudio de Souza Gimenez

Diretor de Infraestrutura

Laercio 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. Todos os usuários devem estar cientes do papel crucial que desempenham no contexto da Segurança da Informação (SI). É imperativo que sigam integralmente as orientações contidas neste documento, a fim de evitar exposição da informação e dos recursos de processamento a situações adversas, como comprometimento, alteração, furto e desvio.

2. CONCEITOS

2.1. Cada vez mais integrados ao dia a dia das pessoas, os recursos de Tecnologia da Informação (TI) deixaram de ser meramente acessórios para se tornarem essenciais em todas as esferas da vida. Da esfera do lazer ao ambiente profissional, as facilidades e vantagens proporcionadas pelo uso adequado da tecnologia são inúmeras. A busca contínua pelo aprimoramento de processos, desenvolvimento pessoal e adoção das melhores práticas na utilização desses recursos desempenha um papel crucial no reforço dos três pilares fundamentais da Segurança da Informação: integridade, disponibilidade e confidencialidade.

2.2. Em Segurança da Informação, é crucial compreender quatro conceitos fundamentais: ativos, vulnerabilidades, ameaças e riscos.

a. **Ativos:** Representam o conjunto de elementos que buscamos proteger, incluindo pessoas, propriedades e informações.

b. **Vulnerabilidades:** Referem-se a fraquezas, falhas ou brechas que podem ser exploradas por uma ameaça para obter acesso a um ativo.

c. **Ameaças:** Englobam todo evento ou ação, seja intencional ou acidental, capaz de explorar uma vulnerabilidade para obter, alterar ou danificar um ativo.

d. **Riscos:** Representam o potencial de alteração, perda ou dano de um ativo causado pela exploração de uma vulnerabilidade por parte de uma ameaça.

3. BOAS PRÁTICAS

3.1. Leia com atenção todas as **recomendações** conjuntas descritas na **P.S.I.** – Política de Segurança da Informação do ICTIM, em caso de duvidas, busque **esclarecimentos** no setor responsável, sua plena compreensão das tarefas aqui apontadas é de crucial importância e fundamental para o sucesso dessas normas.

3.2. Priorize a classificação dos sistemas e recursos que utiliza de acordo com sua importância, considerando a **criticidade dos processos** e das **informações envolvidas**. Estabeleça uma periodicidade para a **troca de senhas**, dando maior frequência aos recursos mais críticos.

3.3. A menos que sua organização o exija para um conjunto específico de acessos, **evite reutilizar senhas**, garantindo a segregação de credenciais. Isso impede que uma credencial comprometida seja utilizada para acessar outros sistemas ou recursos.

3.4. Sempre que possível, opte pela **autenticação multifator** (MFA), mas certifique-se de proteger o dispositivo utilizado para confirmar a autenticação. É recomendável usar autenticadores com códigos de expiração rápida para aumentar a segurança.

3.5. A aplicação de **políticas de mesa limpa** é fundamental para a Segurança da Informação, pois reduz a exposição de informações sensíveis, prevenindo divulgação não autorizada, perda, fraude ou outros danos.

3.6. Evite abrir e-mails com links e anexos sem uma expectativa prévia de recebimento. Em caso de dúvida, verifique diretamente com a fonte e chame o suporte técnico, pois há técnicas para **enganar usuários** e direcioná-los a páginas falsas ou baixar código malicioso.

3.7. Reduza o uso de pen drives e mídias removíveis no ambiente corporativo, pois são comuns **fontes de propagação de vírus, aumentando o risco de contaminação**.

3.8. Esteja atento a ligações, e-mails e mensagens em nome de instituições respeitáveis. **Evite fornecer informações e verifique os contatos** nos canais oficiais dessas instituições. Em caso de dúvida, entre em contato você mesmo para confirmar a autenticidade.

3.9. Familiarize-se com as ferramentas tecnológicas que utiliza. Conhecer as ameaças existentes e como evitá-las reduz significativamente o **risco de exploração de vulnerabilidades**. Procure orientação em caso de dúvidas.

3.10. Aprofunde seu conhecimento sobre a Lei Geral de Proteção de Dados, integrando o tema às **boas práticas de Segurança da Informação**. A Prefeitura Municipal de Maricá disponibilizou o manual da LGPD para auxiliar neste entendimento e o ICTIM produziu uma apostila sobre o assunto.