Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá

Anexo V - Norma para Utilização de E-Mails e Serviços de Mensagens Instantâneas

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. O **correio eletrônico** (e-mail) e os serviços de mensagens instantâneas proporcionam agilidade e praticidade ao trabalho cotidiano. No entanto, ambos são considerados dois dos principais meios por onde ocorrem **ciberataques.** Estima-se que 95% de todo o conteúdo enviado por e-mail globalmente seja composto por lixo eletrônico (SPAM).

2.2. **SPAM** é definido como "mensagens não solicitadas ou irrelevantes enviadas pela internet, geralmente para um vasto público, com a finalidade de publicidade, **phishing**, disseminação de **malwares**, entre outros."

2.3. **Phishing** refere-se a técnicas utilizadas para o **roubo de identidade**, nas quais e-mails e mensagens instantâneas são utilizados como meio de abordagem. Essas técnicas envolvem a criação de **artifícios enganosos** que induzem os usuários a clicarem em links e acessarem sites falsos, projetados para **coletar informações sensíveis**, como senhas, IDs e dados de contas. O sucesso do phishing se deve ao envio dessas mensagens a um grande número de destinatários aleatórios. Há também uma variação mais sofisticada dessa prática, chamada **spear phishing.**

2.4. **Spear phishing** é uma técnica que visa um **público específico**, envolvendo uma pesquisa prévia para a elaboração de um **ataque direcionado**, o que a torna **mais eficaz**. Esse tipo de ataque é um dos principais vetores para a introdução dos temidos **ransomwares**.

2.5. Os **ransomwares** são malwares que **empregam criptografia** para ***impedir o acesso a arquivos*** e ***sistemas de computador*** que foram infectados, exigindo um pagamento como forma de **resgate**. Esses programas têm se tornado uma das principais preocupações atuais, e sua incidência está diretamente relacionada às **atividades cotidianas dos usuários** e ao **grau de conhecimento** que possuem sobre as tecnologias que utilizam.

3. DIRETRIZES

3.1. O usuário deve cumprir as **diretrizes estabelecidas** na **Norma para Credenciais e Senhas**, além das orientações complementares a seguir, que têm como objetivo **fortalecer as proteções** com foco na ***Segurança da Informação.***

a. Não deixar softwares de correio eletrônico e mensagens instantâneas **abertos** durante sua ausência. Feche as sessões ou bloqueie a tela.

b. Não usar seu e-mail como **nome de usuário** de serviços de mensagem eletrônica, da mesma forma não o anexar nas informações públicas destes serviços. Estas informações poderão ser **capturadas e utilizadas** para a prática de envio de **SPAM** e **phishing**.

c. Os programas de **e-mail corporativo** disponibilizados aos usuários devem ser utilizados **exclusivamente** para mensagens de âmbito profissional sendo **vedado o uso pessoal**.

d. **Não é permitida** a utilização de e-mail **não** institucional para o exercício da **atividade funcional**.

e. **Não devem ser abertos arquivos**, **links** ou **executados programas** provenientes de e-mails e mensagens instantâneas, sem a certeza de sua procedência e existência de prévia expectativa do recebimento do conteúdo.

f. **Não é permitido** o cadastramento do **e-mail institucional** em site, serviços de notificação ou listas de mailing na internet, tais como **redes sociais** e **sites de comércio eletrônico**, salvo o estritamente necessário à atribuição funcional.

g. **Não é permitido** acessar contas de correio eletrônico de **terceiros**, salvo para fins de auditoria pela equipe de TI responsável.

h. O usuário **não pode** utilizar seu e-mail para transmissão de:

i. **Malwares** (vírus e demais códigos maliciosos).

ii. **Spam** (mails e mensagens não solicitados com conteúdo duvidoso, enganoso ou propagandas).

iii. **Mineradores** (Softwares que usam a capacidade de processamento dos computadores para somar a pools de mineração de criptomoedas de terceiros).

iv. **Crackers** (Softwares para “quebrar” um método de segurança).

v. **Keyloggers** (Softwares para captura das ações do usuário, como a digitação de uma conta, login e senha).

vi. **Sniffers** (Softwares para captura de pacotes de rede).

vii. Correntes;

viii. Boatos ou assemelhados;

ix. Músicas, vídeos e jogos;

x. Pornografia;

xi. Propagandas de qualquer espécie;

xii. Conteúdo que viole o direito de propriedade;

xiii. Quaisquer conteúdos ilegais pelas leis brasileiras;

xiv. Qualquer tipo de material inconveniente e/ou inadequado que cause constrangimento e desconforto a outrem.