# Norma para Utilização de E-Mails e Mensageria

PREFEITURA

Mais **cidade**. Mais **vida**.

## Normativa para Utilização de E-Mails e Mensageria da Prefeitura Municipal de Porto Alegre

Secretaria Municipal de Planejamento e Assuntos Estratégicos

Coordenação de Planejamento e Gestão de Tecnologia da Informação e Comunicação

(SMPAE – CGTI)

Versão 1.0

Última atualização 14 de Setembro de 2022

## PREMISSAS

Todos os servidores públicos, secretarias, órgãos, fornecedores, prestadores de serviço e demais parceiros vinculados devem ter conhecimento de seu importante papel no contexto de **Segurança da Informação (SI)** sendo um dever seguirem as diretrizes e orientações contidas na **Política de Segurança da Informação (PSI)** em sua íntegra, assim evitando expor a informação e os recursos de processamento a situações adversas como comprometimento, alteração, furto e desvio.

## CONCEITOS

Correio eletrônico (e-mail) e serviços de mensagem instantânea trazem velocidade e facilidades ao trabalho diário. No entanto estes são dois dos principais vetores para ciberataques. Estima-se que 95% de todo o conteúdo que circula por e-mail no mundo é lixo eletrônico (*SPAM*).

*SPAM* é classificado como: “mensagens irrelevantes ou não solicitadas enviadas através da internet, tipicamente para um grande número de usuários, para propósitos de publicidade, *phishing*, distribuição de *malwares*, etc**”.**

*Phishing* são técnicas para roubo de identidade utilizando e-mail e mensagens instantâneas como porta de entrada, produzindo artifícios enganosos, de forma que o usuário seja induzido a clicar em links e acesse sites falsos preparados para capturar informações sensíveis, como senhas, IDs e contas. *Phishing* atinge sucesso por volume, uma vez que são enviados para um grande número de destinatários aleatoriamente. Há uma variação mais elaborada chamada de *spear phishing.*

*Spear phishing* são projetados para atingirem um público selecionado, onde um trabalho de pesquisa é feito e produzido um ataque direcionado a atingir este alvo específico, sendo mais eficiente. *Spear phishing* é um dos maiores vetores para a entrada dos temidos *ransomwares.*

*Ransomwares* são *malwares* que utilizam criptografia para bloquear o acesso a arquivos e sistemas de computador infectados, solicitando pagamento pelo resgate (*ransom*). Eles têm sido uma das maiores preocupações da atualidade e suas ocorrências estão diretamente ligadas às ações diárias dos usuários e o nível de conhecimento que estes tem sobre a tecnologia que utilizam.

## DIRETRIZES

Fica o usuário obrigado a seguir as diretrizes contidas na Norma para Credenciais e Senhas, as diretrizes da sessão VIII da OS 007/2018, bem como as demais diretrizes complementares a seguir, que objetivam ampliar as proteções com o enfoque na Segurança da Informação.

- Não deixar softwares de correio e mensagens instantâneas abertos durante sua ausência, feche as sessões ou bloqueie a tela.
- Não usar seu e-mail como nome de usuário de serviços de mensagem eletrônica, da mesma forma não anexar o mesmo nas informações públicas destes serviços. Estas informações poderão ser capturadas e utilizadas para a prática de envio de *SPAM* e *phishing.*
- Os programas de e-mail e serviços de mensagem instantânea disponibilizados aos usuários devem ser utilizados exclusivamente para mensagens de âmbito profissional sendo vedado o uso pessoal.
- Não é permitida a utilização de *e-mail* não institucional para o exercício da atividade funcional.
- 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.
- Não é permitido o cadastramento do *e-mail* e/ou da conta de mensagem instantânea 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.
- Não é permitido acessar contas de correio eletrônico de terceiros, salvo para fins de auditoria pela equipe de TI responsável.
- O usuário não pode utilizar seu e-mail e software de mensagem instantânea para transmissão do seguinte:
    - *Malwares (vírus e demais códigos maliciosos).*
    - *Spam (mails e mensagens não solicitados com conteúdo duvidoso, enganoso, ou propagandas)*.
    - Mineradores (Softwares que usam a capacidade de processamento dos computadores para somar a *pools* de mineração de criptomoedas de terceiros).
    - Crackers (Softwares para “quebrar” um método de segurança).
    - Keyloggers (Softwares para captura das ações do usuário, como a digitação de uma conta, login e senha).
    - Sniffers (Softwares para captura de pacotes de rede);

- Correntes;
- Boatos ou assemelhados;
- Músicas, vídeos e jogos;
- Pornografia;
- Propagandas de qualquer espécie;
- Conteúdo que viole o direito de propriedade;
- Quaisquer conteúdos ilegais pelas leis brasileiras;
- Qualquer tipo de material inconveniente e/ou inadequado que cause constrangimento e desconforto a outrem.

## Histórico de Revisões

| Versão | Data | Alterações | Autor | Revisor |
|---|---|---|---|---|
| 1.0 | 14/09/2022 | Versão inicial | (CGTI-SMPAE) Fernando Delazeri Eduardo Hoppe | (CGTI-SMPAE) Eduardo Hoppe |