

PORTARIA MUNICIPAL Nº 240, DE 03 DE MARÇO DE 2021

DISPÕE SOBRE ADOÇÃO DE POLÍTICAS PÚBLICAS MUNICIPAIS DE SEGURANÇA DA INFORMAÇÃO NA PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE SALTO E DA OUTRAS PROVIDÊNCIAS CORRELATAS.

LAERTE SONSIN JÚNIOR, Prefeito da Estância Turística de Salto, no Estado de São Paulo, usando das atribuições legais que lhe são conferidas.

RESOLVE

Artigo 1º – DETERMINAR, no âmbito da Prefeitura Municipal da Estância Turística de Salto, a adoção de Políticas Públicas Municipais de Segurança da Informação, objetivando:

- I. Implementar a gestão da segurança de informação em todas as Unidades Administrativas do Poder Público;
- II. Adotar abordagem sistemática e coerente, dotada de planejamento, operação e controle das atividades de segurança da informação;
- III. Implementar controles de segurança para assegurar a interoperabilidade e o intercâmbio de informações no Poder Público;
- IV. Estabelecer referencial de segurança de informação para os sistemas de informação a fim de nortear as aquisições, desenvolvimentos e suas respectivas evoluções;
- V. Realizar a gestão de atividade das ameaças, vulnerabilidades, incidentes e riscos proporcionando suporte à prestação de serviços da Administração Pública Municipal e suas operações;
- VI. Garantir conformidade, padronização e normatização das atividades de gestão de segurança da informação nas diversas Unidades Administrativas;
- VII. Manter cadastramento atualizado de usuários de sistemas e redes de informações municipais, permitindo identificação de possíveis infratores ou de condutas ameaçadoras a sua integridade;



VIII. Ajudar na implementação da Lei Federal nº 13.790, de 14 de agosto de 2018 – *Lei Geral de Proteção de Dados – LGPD*, visando o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico, tecnológico e a inovação, a livre iniciativa, a concorrência e a defesa do consumidor, assim como aos direitos humanos, desenvolvimento da personalidade, a dignidade e ao exercício da cidadania pelas pessoas naturais em suas relações com o Poder Público;

IX. Implementar o Plano Diretor Municipal de Tecnologia de Informação – PDMTI, para detalhamento de processos e gerenciamento de operações, priorizando as ações organizadas e estratégias, em melhor uso dos recursos em tecnologia.

Artigo 2º – A utilização de senhas (forma de identificação e acesso do usuário, sendo recurso pessoal e intransferível que protege identidade e evita falsificações) no Poder Público será permeada pelas seguintes recomendações:

I. A senha é de total responsabilidade de seu usuário, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação.

II. A senha inicial só será fornecida ao próprio usuário, de forma pessoal. Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade de seu destinatário;

III. É proibido o compartilhamento de senhas para funções de administração de sistemas;

IV. As senhas não poderão ser anotadas ou deixadas em local próximo do computador, que permita plena visualização ou acesso;

V. As senhas deverão seguir os seguintes pré-requisitos: tamanho mínimo de 08 (oito) caracteres; existência de caracteres pertencentes ao menos de 03 (três) dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais e não devem ser baseadas em informações pessoais de fácil dedução ou de caráter pessoal;

VI. O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações: desligamento do servidor; mudança ou alteração de função que torne o acesso incompatível com as novas funções e quando por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação, devendo o respectivo setor comunicar em todas as situações acima elencadas;



VII. Fica vedado a utilização de senhas de acesso à internet *wireless* para equipamentos não pertencentes a Administração Pública Municipal.

Artigo 3º – A utilização de e-mail institucional (forma de comunicação interna) no Poder Público será permeada pelas seguintes recomendações:

I. Será destinado tão somente para fins profissionais, relacionados às atividades de seus usuários;

II. Fica autorizado o monitoramento de mensagens eletrônicas, tão somente com o intuito de bloquear ameaças externas ou outros conteúdos maliciosos que violem a Política Municipal de Segurança da Informação;

III. É proibido a realização de envio, por endereço eletrônico institucional, de mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens em correntes virtuais, campanhas, promoções ou conteúdos partidários;

IV. É proibido o envio de arquivos de origem desconhecida anexados a mensagens eletrônicas, que torne os meios eletrônicos vulneráveis ou faça propagação de ameaças;

V. É proibido a falsificação de informações de endereçamento, adulteração de cabeçalhos para esconder a identidade de remetentes ou destinatários;

VI. Não utilizar meios institucionais internos para interferir negativamente nas atividades profissionais individuais no Poder Público ou em sua imagem;

VII. Produzir, transmitir ou divulgar mensagens que contenham ameaças eletrônicas ou qualquer outra extensão que represente risco à segurança; que vise obter acesso não autorizado a outro computador, servidor ou rede; vise interromper serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado; vise burlar qualquer sistema de segurança; objetive vigiar secretamente ou assediar outro usuário; vise acessar informações confidenciais sem explícita autorização do usuário – destinatário; possua conteúdo impróprio, obsceno ou ilegal; faça promoção de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros ou inclua material protegido por direitos autorais sem a permissão do detentor de direitos.

Artigo 4º – A utilização de estações de trabalho (unidades operacionais eficientes, aparelhadas e equipadas para desenvolvimento e execução de ações de trabalho, sob responsabilidade identificada de seu operador) no Poder Público será permeada pelas seguintes recomendações:

A.

Sup

I. É de responsabilidade do usuário o zelo e acompanhamento pelos equipamentos, devendo mantê-los em plenas condições;

II. É vedado a personalização de equipamentos com objetos de natureza pessoal ou a retirada de sua identificação patrimonial;

III. É vedada a abertura deliberada de qualquer equipamento para realização de reparos, vez que ocorra necessidade, deverá o usuário dirigir-se a setor adequado e solicitar atendimento mediante abertura de Ordem de Serviço – OS;

IV. As estações de trabalho apenas estarão acessíveis aos usuários mediante configuração de contas limitadas;

V. É proibida a instalação deliberada de programas nas estações de trabalho pelos usuários, devendo em caso de necessidade ser solicitado ao setor responsável;

VI. As estações de trabalho devem ser mantidas bloqueadas durante a ausência de seus usuários;

VII. Todos os documentos e arquivos institucionais relativos à atividade desempenhada pelo usuário, devem ser armazenadas em local próprio do servidor, mantendo rotinas de controle de acesso de terceiros e de *backup*;

VIII. Documentos identificados como críticos devem ser somente armazenados no servidor;

IX. É vedado qualquer realização de manutenção em equipamentos não pertencentes ao Poder Público;

Artigo 5º – Esta Portaria entra em vigor na data de sua emissão, revogando disposições em contrário, podendo ocorrer adoção de outras medidas complementares por cada Setor Administrativo.

Prefeitura da Estância Turística de Salto

Salto/SP, aos 03 de março de 2021

LAERTE SONSIN JUNIOR

Prefeito

Registrada na Secretaria Municipal de Administração em 03 de março de 2021, com a devida publicidade

CAIO VINICIUS PICININ

Secretário Municipal de Administração