



Prefeitura Municipal de **TAPIRATIBA**

DECRETO Nº 575/2022, DE 22 DE AGOSTO DE 2022

“Institui a Política de Segurança da Informação no Âmbito da Administração direta e indireta no Município de Tapiratiba e dá outras providências.”

RAMON JESUS VIEIRA, Prefeito do Município de Tapiratiba, Estado de São Paulo, usando das atribuições que lhe são conferidas por lei,

DECRETA:

Art. 1º - Fica instituída a Política de Segurança da Informação no âmbito da Prefeitura do Município de Tapiratiba.

§ 1º - A Política de Segurança da Informação constitui um conjunto de diretrizes e normas que estabelecem o princípio de controle, proteção e monitoramento das informações processadas, armazenadas e custodiadas pela Administração Municipal, aplicando-se a todos os órgãos do Poder Executivo Municipal.

Art. 2º - Para efeito deste Decreto ficam estabelecidos os seguintes conceitos:

I - autenticidade: garantia que a informação é procedente e fidedigna, capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;

II - confidencialidade: Toda informação deve ser acessada por quem de direito, até que se torne pública. Assegurar que informações confidenciais e críticas não sejam subtraídas dos sistemas organizacionais por meio de ciberataques, espionagem, entre outras práticas.

III - dado: parte elementar da estrutura do conhecimento, computável, mas, incapaz de, por si só, gerar conclusões inteligíveis ao destinatário;

IV - disponibilidade: garantia de que as informações e os recursos de tecnologia da informação estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso;

V - informação: conjunto de dados que, processados ou não, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VI - integridade: garantia de que as informações estejam protegidas contra manipulações e alterações indevidas, tendo preservação da precisão, consistência e confiabilidade das informações e sistemas;

VII - legalidade: garantia de que todas as informações sejam criadas e gerenciadas de acordo com a legislação em vigor;



Prefeitura Municipal de **TAPIRATIBA**

- VIII - log: registro de atividades gerado por programa de computador que possibilita a reconstrução, revisão e análise das operações, procedimento ou evento em sistemas de informação;
- IX - não repúdio ou irretratabilidade: garantia de que um usuário não consiga negar uma operação ou serviço que modificou ou criou uma informação;
- X - recursos da tecnologia da informação: recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar a informação, dentre estes podemos destacar os computadores, notebooks, tablets, pendrives, impressoras, scanners, mouse, teclado, softwares, etc;
- XI - risco: relação entre probabilidade e impacto, ajudando a determinar onde concentrar investimentos em segurança da informação;
- XII - segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas (ISO/ IEC 27001);
- XIII - senha: conjunto alfanumérico de caracteres destinado a assegurar a identidade do usuário e permitir seu nível de acesso aos recursos da tecnologia da informação não disponíveis ao público, de uso pessoal e intransferível;
- XIV - tecnologia da informação e comunicação: solução ou conjunto de soluções sistematizadas baseadas no uso de recursos tecnológicos que visam resolver problemas relativos à geração, tratamento, processamento, armazenamento, veiculação e reprodução de dados, bem como subsidiar processos que convertem dados em informação;
- XV - usuário: funcionário, servidor, comissionado, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor ou qualquer outro indivíduo ou organização que venham a ter relacionamento, direta ou indireta, com os órgãos e entidades da Administração Municipal;
- XVI - violação: qualquer atividade que desrespeite as diretrizes estabelecidas nesta política ou em quaisquer das demais normas que a complementa.
- XVII - conformidade: toda informação deve estar em conformidade com os padrões, regras e principalmente com a legislação vigente.
- XVIII - ameaça: causa potencial de um incidente indesejado, que pode resultar em dano à Prefeitura Municipal.
- XIX - backup: salvaguarda de informações, realizada por meio de reprodução e ou espelhamento de uma base de arquivos, com a finalidade de plena capacidade de recuperação em caso de incidente, ou ainda, constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada.



Prefeitura Municipal de **TAPIRATIBA**

XX - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

XXI - repositórios digitais: Plataformas de armazenamento na Internet, exemplo de iCloud, Google Drive, OneDrive, Dropbox, etc.

XXII - login ou ID de usuário: identificação única do usuário, permitindo o seu acesso e controle na utilização dos recursos da tecnologia da informação.

XXIII - malware: é um termo genérico para qualquer tipo de “malicious software” (“software malicioso”) projetado para se infiltrar no seu dispositivo sem o seu conhecimento. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos.

XXIV - data center: local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma organização.

XXV - Spam: mensagem eletrônica não solicitada a qual geralmente é enviada em massa.

XXVI - Peer-to-peer ou P2P: consiste em um conjunto de computadores que se comunicam entre si de forma descentralizada, são nós centrais responsáveis por gerir as ligações entre eles sem a necessidade de um centralizador(servidor). Muito utilizado para compartilhamento de arquivos.

XXVII - Proxy: servidor intermediário o qual torna possível o acesso a internet por meio de uma máquina externa. Tem a função de intermediário entre as solicitações dos usuários que utilizam os recursos da internet e os servidores nos quais esses recursos estão hospedados.

XXVIII - Colaborador: toda e qualquer pessoa física, contratada, concursada ou comissionada ou prestadora de serviços por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da administração da Prefeitura Municipal de Tapiratiba.

Art. 3º - Constituem objetivos da Política de Segurança da Informação:

I - dotar a Prefeitura do Município de Tapiratiba de instrumento jurídico, normativo e institucional que a capacite de forma técnica e administrativa, com o objetivo de assegurar a confidencialidade, a integridade, a autenticidade, o não repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sigilosas da Administração Municipal;

II- estabelecer e controlar os níveis de acesso de usuários internos e externos aos sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;

III - assegurar a interoperabilidade entre os sistemas de segurança da informação;



Prefeitura Municipal de **TAPIRATIBA**

IV - incorporação da cultura da segurança da informação, por todos os colaboradores, como um elemento essencial em seus hábitos e atitudes dentro e fora da organização.

Art. 4º - A Política de Segurança da Informação instituída neste Decreto reger-se-á pelos seguintes princípios:

I - tratamento da informação como patrimônio, tendo em vista que a divulgação das informações estratégicas de qualquer natureza pertencentes à Administração deve ser protegida de forma adequada, com vistas a evitar alterações, acessos ou destruição indevidos;

II - classificação da informação, garantindo-lhe o adequado nível de proteção, considerando:

a) a avaliação da necessidade do tipo de acesso pelo usuário, adotando-se como parâmetro o grau de confidencialidade da informação;

b) a definição de confidencialidade da informação em consonância com as atividades desempenhadas pelo usuário, deverá conter os limites de acesso, tais como leitura, atualização, criação e remoção, entre outros.

III - controle de acesso às informações, tendo como orientação a classificação definida no inciso II deste artigo, respeitando a legislação vigente e considerando, ainda, que:

a) o acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades;

b) no caso de acesso a sistemas informatizados, deverão ser utilizados sistemas e tecnologias autorizadas pela Administração;

IV - continuidade do uso da informação, sendo necessária, para o funcionamento dos sistemas, pelo menos uma cópia de segurança atualizada e guardada em local remoto, com nível de proteção equivalente ao nível de proteção da informação original, observada as seguintes regras:

a) para a definição das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação de ambiente;

b) os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem ter controle de acesso físico, condições ambientais adequadas e ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências;

V - educação em segurança da informação, devendo ser observado pelo usuário a correta utilização das informações e dos recursos computacionais disponibilizados.

Art. 5º - As medidas a serem adotadas para fins de proteção da informação deverão considerar:



Prefeitura Municipal de **TAPIRATIBA**

- I - os níveis adequados de integridade, confidencialidade e disponibilidade da informação;
- II - a compatibilidade entre a medida de proteção e o valor do ativo protegido;
- III - o alinhamento com as diretrizes da Administração Municipal;
- IV - as melhores práticas para a gestão da segurança da informação;
- V - os aspectos comportamentais e tecnológicos apropriados.

Art. 6º - Compete ao Departamento de Informática:

- I - elaborar e revisar continuamente os procedimentos e a normatização relacionada ao processo de gestão da segurança da informação;
- II - avaliar propostas de modificação da Política de Segurança da Informação encaminhadas pelos demais órgãos administrativos da Administração Municipal;
- III - planejar, elaborar e propor estratégias e ações para institucionalização da política, normas e procedimentos relativos à segurança da informação;
- IV - avaliar a eficácia dos procedimentos relacionados à segurança da informação, propondo e implementando medidas que visem a melhoria do processo de gestão da segurança da informação no âmbito da Administração Municipal;
- V - apurar os incidentes de segurança críticos e dar o encaminhamento adequado;
- VI - promover a conscientização, o treinamento e a educação em segurança da informação.
- VII - realizar backup diário dos dados armazenados nos servidores internos da Prefeitura.

Parágrafo único - Não compete ao Departamento de Informática fazer backup diário ou periódico de informações armazenadas localmente nos computadores, porém, o mesmo deverá orientar os usuários quanto às melhores práticas para realização de backups para aplicativos instalados em computadores locais e quanto a importância de salvar os arquivos mais importantes na rede da Prefeitura.

Art. 7º - É dever do usuário, em consonância com a Política de Segurança da Informação estabelecida neste Decreto:

- I - Todo prejuízo ou dano que vier a sofrer ou causar à Prefeitura Municipal de Tapiratiba ou a terceiros, em decorrência da não obediência às diretrizes e normas referidas.
- II - zelar pelo sigilo da sua senha;
- III - zelar pela segurança das informações, fechando ou bloqueando o acesso aos equipamentos de informática ou softwares quando não estiver utilizando;



Prefeitura Municipal de **TAPIRATIBA**

IV - zelar pela integridade física dos equipamentos de informática utilizados, evitando submetê-los a condições de riscos, mantendo-os afastados de líquidos e alimentos, não danificando as placas de patrimônio, não colando qualquer tipo de adesivo nos equipamentos ou qualquer material e/ ou utensílio que possa danificá-los, e comunicando ao órgão competente qualquer anormalidade ou defeito;

V - zelar pela segurança da informação que esteja sob sua custódia em razão de seu exercício funcional.

VI - Cumprir as normas definidas na Política de Segurança.

VII - Reportar, de imediato, ao superior hierárquico, qualquer incidente de segurança, ex.: dispositivos desconhecidos conectados ao computador; acessos indevidos ou suspeitas iminentes.

VIII - Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

IX - É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

X - As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos, compreensíveis por linguagem humana (não criptografados), não devem se basear em informações pessoais, como próprio nome, de familiares, data de nascimento, endereço, placa de carro e não devem ser constituídas de combinações óbvias de teclado, como seqüências.

XI - Os usuários devem alterar sua senha em caso de suspeita de que terceiros tenham obtido acesso a sua conta.

Os usuários devem estar cientes dos riscos associados aos hardwares e softwares de seu uso, com a sua condição e cumprir rigorosamente o que está previsto no Termo de Responsabilidade concedido pela Prefeitura Municipal de Tapiratiba.

Art. 8º - É proibido aos usuários:

I - fornecer por qualquer motivo, seu login e senha para acesso a outrem;

II - fazer uso do login e da senha de terceiro;

III - utilizar os recursos da tecnologia da informação em desacordo com os princípios éticos da Administração Pública;

IV - visualizar, acessar, expor, armazenar, distribuir, editar ou gravar material de natureza pornográfica, racista, jogos, música, filmes e outros relacionados, por meio de uso de recursos de computadores da Prefeitura;

V - acessar sites ou serviços que representem risco aos dados ou à estrutura de redes da Prefeitura;



Prefeitura Municipal de **TAPIRATIBA**

VI - fazer cópias não autorizadas dos arquivos/software desenvolvidos ou adquiridos pela Prefeitura.

VII - qualquer procedimento de manutenção física ou lógica, configuração ou modificação, instalação, desinstalação, sem o consentimento prévio e acompanhamento do Departamento de TI. A Prefeitura Municipal de Tapiratiba é detentora dos equipamentos fornecidos, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da prefeitura.

VIII - Os usuários não poderão utilizar os recursos da Prefeitura Municipal de Tapiratiba para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, constrangimento ou programas para controle de outros computadores.

IX - O acesso aos softwares peer-to-peer como o Bittorrent e demais softwares semelhantes não são permitidos.

X - Não é permitido o acesso à internet por meio de proxy não autorizado pela Prefeitura Municipal de Tapiratiba.

XI - Arquivos pessoais ou não pertinentes aos assuntos da Prefeitura Municipal de Tapiratiba (fotos, músicas, vídeos, etc.) não poderão ser copiados ou movidos para a rede. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem prévio aviso. Diretórios ou pastas de acesso público não deverão ser utilizados para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica.

§ 1º - Arquivos em geral que estejam duplicados e os que não forem de interesse da administração, deverão ser excluídos.

XII - Os usuários da Prefeitura Municipal de Tapiratiba não devem executar nenhum tipo de comando ou programa que possa sobrecarregar serviços sem a prévia solicitação e a autorização do Departamento de TI.

Art. 9º - Acesso Remoto Externo:

Com o objetivo de estabelecer critérios para a disponibilização do serviço de acesso remoto externo à rede corporativa da Prefeitura Municipal de Tapiratiba, bem como as regras para sua utilização, visando a prevenção do acesso não autorizado às informações.

O acesso remoto aos serviços corporativos é exclusivo aos colaboradores que oficialmente executem atividade vinculada à atuação institucional da Prefeitura Municipal de Tapiratiba e que necessitem deste serviço para execução de suas atividades institucionais, desde que autorizados pelos seus superiores hierárquicos documentalmente entregues ao Departamento de TI.

I - A liberação de acesso remoto só será efetivada mediante após avaliação e aprovação pelo Departamento de TI para que evitem ameaças à integridade e sigilo das informações contidas na rede corporativa da Prefeitura Municipal de Tapiratiba. Será feita uma



Prefeitura Municipal de **TAPIRATIBA**

análise criteriosa podendo ser negado o acesso remoto caso comprometa a segurança do ambiente.

II - A solicitação do acesso remoto deve conter, as seguintes informações:

- a) Data de Solicitação;
- b) Tipo de Solicitação;
- c) Tempo de validade do acesso remoto;
- d) Justificativa;
- e) Dados do solicitante;
- f) Dados do usuário;

III - Será disponibilizado formulário para solicitação e controle de Acesso Remoto.

IV - A disponibilização de acesso remoto à rede corporativa da Prefeitura para outras organizações deve obedecer às seguintes regras:

- a) Direitos de acesso definidos por contrato;
- b) Acesso temporário e limitado às necessidades;
- c) Revisão periódica dos direitos de acesso;
- d) utilização de soluções que permitam controlar e implementar regras de acesso.

V - O serviço de acesso remoto deverá ser cancelado de acordo com as seguintes regras:

- a) Finalização do período especificado na solicitação;
- b) Perda da necessidade do uso do serviço;
- c) Transferência do usuário para outra unidade;
- d) Identificação de uso indevido no acesso concedido.

VI - As conexões remotas à rede corporativa da Prefeitura deverão seguir as regras:

- a) Utilização de autenticação;
- b) As senhas e as informações que trafegam entre a estação remota e a rede corporativa da Prefeitura são criptografadas;
- c) Todas as conexões e acessos serão registrados em log, para posterior auditoria.

VII - Cada usuário deve manter suas credenciais de acesso: login e senha em sigilo, e não fornecer a outra pessoa, a não ser que seja devidamente autorizado.

VII - É vedada a utilização do acesso remoto para fins não relacionados às atividades da prefeitura.

Art. 10 - Ao perder o vínculo com a Prefeitura todos os acessos do usuário aos recursos da tecnologia da informação serão transferidos para o novo usuário, suas contas de e-mails do domínio da prefeitura trocadas e caso haja conteúdo particular, o mesmo será apagado.



Prefeitura Municipal de **TAPIRATIBA**

Parágrafo único - Fica o Departamento de Recursos Humanos responsável por repassar ao Departamento de Informática, a qualquer tempo, as demissões/exonerações, do quadro de funcionários, para que as providências acima sejam tomadas.

Art. 11 - É vedado o uso de equipamentos de informática particulares conectados à rede de informática da Prefeitura, sem a prévia autorização documentada entregue ao Departamento de TI.

Art. 12 - São considerados usos inadequados dos equipamentos de informática:

I - instalar softwares de qualquer espécie em computador da Prefeitura sem o conhecimento do Departamento de TI e sua devida autorização expressa devidamente documentada;

II - reconfigurar a rede corporativa ou inicializá-la sem prévia autorização expressa;

III - efetuar montagem, alteração, conserto ou manutenção em equipamentos da Prefeitura sem o conhecimento do Departamento de TI e sua devida autorização expressa devidamente documentada;

IV - alterar o local de instalação dos equipamentos de informática, sem o conhecimento do Departamento de TI e sua devida autorização expressa devidamente documentada;

V - instalar dispositivo ou utilizar internet móvel, sem prévia autorização expressa;

VI - conectar equipamento particular na rede de computadores da Prefeitura, sem prévia autorização expressa;

VII - utilizar mecanismos para burlar o usuário/administrador, concedendo privilégios aos demais usuários;

Art. 13 - É considerado uso inadequado da internet:

I - acessar informações consideradas inadequadas ou não relacionadas às atividades administrativas, especialmente sites de conteúdo agressivo (racismo, pedofilia, nazismo, etc.), de drogas, pornografia e outros relacionados;

II - fazer download de arquivos e outros que possam tornar a rede local vulnerável a invasões externas e ataques a programas de código malicioso em suas diferentes formas;

III - violar os sistemas de segurança da Prefeitura;

IV - tentar ou efetivamente burlar as regras definidas de acesso à internet;

V - alterar os registros de acesso à internet;

VI - realizar ataque ou invadir computadores da Prefeitura;

VII - utilizar acesso à internet provido pela Prefeitura para transferência de arquivos que não estejam relacionados às suas atividades;



Prefeitura Municipal de **TAPIRATIBA**

VIII - divulgar informações confidenciais da Prefeitura em grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas na forma da lei.

Art. 14 - É considerado uso inadequado ao serviço de e-mail:

I - utilizar o correio eletrônico para envio sem autorização de mensagens não solicitadas para vários destinatários.

II - enviar sem autorização mensagens pelo endereço eletrônico de seu departamento ou usando o nome ou endereço de correio eletrônico de outra pessoa.

III - enviar qualquer mensagem por meios eletrônicos que torne seu remetente, Prefeitura Municipal de Tapiratiba, ou suas unidades, vulneráveis a ações cíveis ou criminais.

IV - divulgar sem autorização do Departamento relacionado, qualquer informação ou imagem de tela de sistemas, documentos e afins, as quais não sejam estritamente relacionadas ao requerente em questão.

V - falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes ou destinatários, com o objetivo de evitar as punições previstas.

VI - apagar mensagens pertinentes de correio eletrônico quando a Prefeitura Municipal de Tapiratiba estiver sujeita a qualquer tipo de investigação;

VII - divulgar mensagem que:

- a) contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Prefeitura.
- b) conttenham ameaças eletrônicas como spam, mail bombing, virus, etc.
- c) contenha arquivo executável (.exe, .com, .bat, .pif, .vbs, .js, .src, .dll) ou qualquer outra extensão que demonstre risco à segurança.
- d) vise obter acesso não autorizado a outro computador, servidor ou rede;
- e) intuito de interromper serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- f) vise burlar qualquer sistema de segurança;
- g) vigie sem consentimento ou assediar outro usuário;
- h) acesse indevidamente informações que podem causar prejuízo a qualquer pessoa;
- i) inclua imagens criptografadas ou máscaras
- j) contenha anexos superiores a 15MB ou contenha conteúdo considerado impróprio, ilegal ou obsceno;
- k) caráter difamatório, calunioso, ofensivo, violento, pornográfico entre outros;
- l) contenha perseguição relacionada a sexo, raça, incapacidade mental ou física, entre outros;



Prefeitura Municipal de **TAPIRATIBA**

- m) vise acessar informações confidenciais sem autorização;
- n) tenha fins políticos.
- o) inclua material protegido por direitos autorais sem a permissão do autor.

Art. 15 - Os equipamentos de tecnologia e serviços para acesso à internet são de propriedade da prefeitura que se necessário pode após devida análise, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

Art. 16 - O download e a utilização de programas de entretenimento, jogos ou músicas de qualquer formato, poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos superiores imediatos.

Art. 17 - O chefe imediato do usuário deverá comunicar quaisquer ações que comprometam a segurança, a integridade, o desempenho e a descaracterização de equipamentos e redes da Prefeitura.

Art. 18 - O usuário, a critério de seu chefe imediato e de acordo com as necessidades do serviço, poderá ter acesso a sua conta de correio eletrônico.

§ 1º - As contas oficiais de e-mail da Prefeitura devem ser utilizadas, exclusivamente, para transmitir e receber informações relacionadas às atividades administrativas.

§ 2º - As contas de e-mail particulares não terão suporte do Departamento de Informática, podendo ser bloqueado o acesso sem prévio aviso.

§ 3º - O uso de correio eletrônico da Prefeitura Municipal de Tapiratiba é para fins corporativos e relacionados às atividades do usuário dentro da prefeitura. É vedado o uso deste correio eletrônico para fins pessoais.

Art. 19 - Todo caso de exceção às determinações da Política de Segurança da Informação deve ser analisado de forma individual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que o fundamentaram.

Art. 20 - A não observância da Política de Segurança da Informação pelos usuários configura descumprimento de dever funcional, indisciplina ou insubordinação, conforme o caso, sujeitando o infrator à incidência das sanções cabíveis, nos termos da legislação vigente.



Prefeitura Municipal de
TAPIRATIBA

Art. 21 - Este Decreto entra em vigor na data de sua publicação.

Art. 22 - Revogam-se as disposições em contrário.

Prefeitura Municipal de Tapiratiba, 22 de agosto de 2022.

RAMON JESUS VIEIRA
PREFEITO MUNICIPAL

Publicada por afixação, no quadro próprio de editais, na sede da Prefeitura Municipal e no Painei da Cidadania, na mesma data.