

**DECRETO Nº 7.964, DE 3 DE NOVEMBRO DE 2025**

***Dispõe sobre os procedimentos de segurança da informação, controle de acesso, integridade dos dados e proteção dos sistemas no âmbito da Administração Pública Municipal de Capanema - PR.***

O Prefeito do Município de Capanema, no uso das atribuições previstas na Lei Orgânica Municipal e demais dispositivos legais aplicáveis, e

Considerando a necessidade de proteger os dados produzidos e mantidos pela administração pública através de seus sistemas;

Considerando as exigências da Lei Geral de Proteção de Dados (Lei nº 13.709/2018);

Considerando as boas práticas de governança, integridade e segurança cibernética;

Considerando a necessidade de regulamentar o controle de acesso aos sistemas municipais;

**DECRETA:**

**Art. 1º** Este Decreto estabelece os procedimentos, diretrizes e responsabilidades para segurança da informação, controle de acesso, integridade dos dados e uso seguro dos sistemas no âmbito da Administração Pública Municipal de Capanema.

**Art. 2º** As regras previstas neste Decreto aplicam-se a:

- I - todos os órgãos da Administração Direta e Indireta;
- II - servidores efetivos, comissionados, estagiários, terceirizados e colaboradores;
- III - empresas contratadas que utilizem, acessem ou tratem dados municipais.

**Art. 3º** Para fins desta Decreto, considera-se:

- I - Dados pessoais: informações relacionadas a pessoa natural identificada ou identificável;
- II - Dados sensíveis: dados definidos no art. 5º, II, da LGPD;
- III - Sistema de informação: conjunto de softwares, plataformas, bancos de dados e aplicativos utilizados pela municipalidade;

IV - Controle de acesso: processo de autorização, permissão e restrição de usuários aos sistemas;

V - Integridade dos dados: garantia de que a informação não seja alterada indevidamente.

**Art. 4º** O acesso aos sistemas municipais será realizado mediante identificação individual, por login e senha ou credencial equivalente, sendo vedado o compartilhamento de senhas entre usuários.

**Art. 5º** A criação, alteração e exclusão de usuários deverá ser:

I - solicitada formalmente pelo gestor da unidade;

II - autorizada pela Secretaria Municipal de Administração e/ou pela Secretaria Municipal da Fazenda Pública;

III - registrada e arquivada para fins de auditoria.

**Art. 6º** Cada usuário terá acesso apenas ao nível necessário para o desempenho de suas funções, observando o princípio do menor privilégio.

**Art. 7º** Fica obrigatório o bloqueio imediato de acessos quando:

I - houver desligamento do servidor;

II - mudança de lotação que altere a necessidade de acesso;

III - suspeita de mau uso ou risco à segurança.

**Art. 8º** Os sistemas municipais deverão adotar, sempre que possível, mecanismos de:

I - autenticação forte;

II - registro de logs de acesso e atividades;

III - controle de versão dos dados;

IV - cópias de segurança (backup) com periodicidade definida.

**Art. 9º** É proibida a instalação de programas, aplicativos ou extensões não autorizados nos equipamentos da prefeitura, especialmente os que ofereçam riscos de malware, rastreamento ou vulnerabilidade.

**Art. 10.** Os servidores deverão utilizar apenas os e-mails institucionais para envio de informações administrativas, especialmente dados pessoais ou documentos sigilosos.

**Art. 11.** Todos os sistemas que tratem dados pessoais deverão possuir:

I - proteção criptográfica quando aplicável;

II - política de retenção e exclusão de dados;

III - controle de logs por no mínimo 12 meses;

IV - mecanismo de prevenção a alterações não autorizadas.

**Art. 12.** O tratamento de dados pessoais por servidores e colaboradores deverá observar:

- I - finalidade pública;
- II - transparência;
- III - necessidade;
- IV - minimização dos dados;
- V - prevenção e segurança.

**Art. 13.** Documentos físicos e digitais contendo dados pessoais ou sensíveis deverão ser armazenados de forma segura, com acesso restrito.

**Art. 14.** É vedado ao servidor copiar, extrair, compartilhar ou divulgar dados a terceiros sem autorização formal da chefia imediata e observância da LGPD.

**Art. 15.** Os equipamentos de informática da municipalidade destinam-se exclusivamente às atividades de trabalho.

**Art. 16.** É proibida a utilização dos sistemas e equipamentos para:

- I - fins pessoais;
- II - instalar softwares piratas;
- III - acessar conteúdos ilícitos ou impróprios;
- IV - armazenar dados sem relação com as atividades públicas.

**Art. 17.** A SECAD, através do Departamento de Tecnologia da Informação manterá registros de:

- I - acessos aos sistemas;
- II - tentativas de acesso indevido;
- III - alterações realizadas nos dados;
- IV - movimentações críticas.

**Art. 18.** Os registros serão disponibilizados quando solicitados pelo Controle Interno, Tribunal de Contas ou autoridades competentes.

**Art. 19.** O servidor é responsável por:

- I - manter sigilo sobre informações sensíveis;
- II - zelar pelo uso correto de sua credencial;
- III - comunicar imediatamente suspeitas de acessos indevidos.

**Art. 20.** A SECAD, através do Departamento de Tecnologia da Informação será responsável por:

- I - gerenciar acessos;
- II - prestar suporte técnico;

- III - monitorar riscos de segurança;
- IV - implementar melhorias contínuas.

**Parágrafo único.** O gerenciamento de acessos ao Sistema Contábil e Financeiro (SCP ou Webplano) será realizado pelo Gabinete do Secretário da SEFAZ.

**Art. 21.** O descumprimento desta Instrução poderá ensejar responsabilização administrativa, civil e penal.

**Art. 22.** Os casos omissos serão dirimidos pela SECAD e SEFAZ.

**Art. 23.** Este Decreto entra em vigor na data de sua publicação, revogando disposições contrárias.

Gabinete do Prefeito do Município de Capanema, Estado do Paraná, **aos 3 dias do mês de novembro de 2025.**

  
**Neivor Kessler**  
Prefeito Municipal