PREFEITURA MUNICIPAL DE SÃO LOURENÇO DO OESTE

Estado de Santa Catarina

GUIA DE BOAS PRÁTICAS EM TECNOLOGIA DA INFORMAÇÃO

Versão 2026

Revisado com base na LGPD, Decretos Municipais de Governo Digital e Políticas de Segurança da Informação

Base legal:

Decreto Municipal nº 9.026/2025 – PDTI 2025-2026
Decreto Municipal nº 9.032/2025 – Política de Proteção de Dados Pessoais (LGPD)
Decreto Municipal nº 9.036/2025 – Governo Digital
Decreto Municipal nº 9.047/2025 – Política de Proteção da Infraestrutura de TI
Decreto Municipal nº 9.048/2025 – Termo de Uso dos Serviços Públicos Digitais
Decreto Municipal nº 9.142/2025 – Política de Segurança da Informação (PSI)
Lei Federal nº 13.709/2018 – LGPD | Lei Federal nº 14.129/2021 – Governo Digital

1. Finalidade

Este Guia orienta servidores públicos, estagiários, colaboradores terceirizados e demais usuários dos sistemas municipais quanto ao uso adequado, ético e seguro dos recursos tecnológicos da Administração Pública Municipal de São Lourenço do Oeste – SC.

Sua aplicação é obrigatória e decorre dos Decretos Municipais nº 9.036, 9.047 e 9.142/2025, alinhando-se à Lei Geral de Proteção de Dados (LGPD – Lei Federal nº 13.709/2018) e à Lei do Governo Digital (Lei Federal nº 14.129/2021).

2. Procedimentos Operacionais

2.1. Solicitação de Acessos e Senhas

- Criação, liberação e reativação de acessos devem ser solicitadas pela chefia imediata via memorando ou chamado no Sistema 1DOC.
- A recuperação de senhas pode ser feita pelo próprio usuário por Chamado Técnico no 1DOC ou por e-mail institucional.
- O compartilhamento de senhas é terminantemente proibido, salvo autorização formal e registrada pelo Departamento de TI (art. 9º, Decreto nº 9.142/2025).

2.2. Recuperação de Arquivos

- A restauração de arquivos excluídos exige o caminho completo do arquivo ou pasta.
- Arquivos criados e excluídos no mesmo dia podem não ser recuperáveis, dependendo do ciclo de backup.

2.3. Solicitação de Equipamentos

- Realizada por memorando, com detalhamento da finalidade e uso pretendido.
- A disponibilidade está condicionada à política de TI vigente e ao PDTI 2025-2026 (Decreto nº 9.026/2025).

2.4. Suporte Técnico

- Todas as solicitações devem ser abertas via Sistema 1DOC.
- O solicitante deve acompanhar o andamento do chamado e fornecer informações complementares quando necessário.

2.5. Aquisição de Equipamentos ou Sistemas

- Toda contratação deve ser previamente avaliada pelo Departamento de TI quanto à viabilidade técnica e segurança.
- Sistemas que envolvam tratamento de dados pessoais devem conter cláusulas específicas de proteção de dados (art. 16, Decreto nº 9.032/2025).

2.6. Solicitação de Imagens de Câmeras

- Solicitação realizada via memorando, sujeita à análise e autorização do Diretor do Departamento de TI.
- O acesso a imagens segue os princípios de finalidade, necessidade e proporcionalidade previstos na LGPD.

2.7. Continuidade dos Serviços de TI e Indisponibilidades

O Departamento de Tecnologia e Gestão da Informação (DTGI) opera com metas formais de disponibilidade dos sistemas e adota um Plano de Recuperação de Desastres (DRP) para situações de interrupção não planejada, conforme definido no PDTI 2025-2026 (Decreto nº 9.026/2025).

Metas de disponibilidade (SLA):

99,5%Horário comercial
98% Fora do horário comercial
≤ 30 min - Tempo máximo de inatividade/mês

O que fazer em caso de indisponibilidade de sistemas:

- Registre imediatamente um chamado via Sistema 1DOC ou contate o DTGI diretamente por telefone/e-mail institucional.
- Informe o sistema afetado, o setor, o horário de início da falha e o impacto nas atividades.
- Não tente resolver problemas de rede, servidor ou sistema por conta própria.
- Em casos de indisponibilidade prolongada ou crítica, o DTGI acionará o Plano de Recuperação de Desastres (DRP).

3. Boas Práticas de Segurança da Informação

As diretrizes desta seção derivam da Política de Segurança da Informação (Decreto nº 9.142/2025) e da Política de Proteção da Infraestrutura de TI (Decreto nº 9.047/2025). Seu cumprimento é obrigatório para todos os usuários.

3.1. Proteção de Dados Pessoais (LGPD)

- Dados pessoais só devem ser coletados quando houver finalidade clara, legítima e compatível com as competências públicas do órgão.
- O armazenamento deve ser seguro, com acesso restrito a pessoas autorizadas.
- Qualquer vazamento, perda ou acesso indevido a dados pessoais deve ser comunicado imediatamente ao Encarregado (DPO – Data Protection Officer), ao Departamento de TI e ao superior hierárquico (art. 12, Decreto nº 9.142/2025).
- É vedado o uso de dados de cidadãos para finalidade diversa da que motivou sua coleta.

3.2. Cuidados com Senhas e Acessos

- Utilize senhas complexas: mínimo de 8 caracteres, combinando letras maiúsculas e minúsculas, números e caracteres especiais.
- Altere sua senha periodicamente — a cada 45 dias, conforme art. 9º do Decreto nº 9.142/2025.
- Nunca reutilize senhas anteriores.
- Bloqueie o computador sempre que se ausentar da estação de trabalho (atalho: Windows + L).
- Jamais informe sua senha a terceiros por e-mail, telefone ou qualquer outro meio.

3.3. Navegação Segura

- Evite clicar em links desconhecidos ou realizar downloads sem orientação técnica.
- Verifique se o endereço do site é seguro: prefixo https:// e ícone de cadeado no navegador.
- Não acesse sites de conteúdo duvidoso, entretenimento ou redes sociais pessoais em dispositivos institucionais sem autorização.

3.4. E-mails Maliciosos e Phishing

Conforme art. 3º do Decreto nº 9.047/2025, os usuários devem adotar as seguintes práticas:

- Não abra anexos nem clique em links de remetentes desconhecidos.
- Desconfie de mensagens com erros ortográficos, URLs suspeitas ou solicitações urgentes fora do padrão.
- Reporte imediatamente ao Departamento de TI qualquer e-mail suspeito.
- Nunca forneça senhas ou dados pessoais em resposta a e-mails, mesmo que o remetente aparente ser legítimo.

3.5. Uso de Dados e Sistemas

- É proibido utilizar e-mails, dados ou sistemas institucionais para fins pessoais.
- Informações oficiais devem circular exclusivamente por canais corporativos autorizados.
- O e-mail corporativo limita-se a atividades profissionais relacionadas ao cargo (art. 3º, inciso I, Decreto nº 9.047/2025).
- Comunicações via WhatsApp ou outros aplicativos institucionais devem ser exclusivamente para assuntos de trabalho.

4. Cuidados com Equipamentos

- Desligue o computador e o monitor ao fim do expediente.
- Mantenha líquidos afastados dos equipamentos.
- Evite sobrecarga de tomadas e extensões elétricas.
- Não cubra equipamentos em funcionamento — o bloqueio da ventilação pode causar superaquecimento.
- Não instale programas, aplicativos ou extensões sem autorização expressa do Departamento de TI.
- Comunique imediatamente qualquer dano, mau funcionamento ou perda de equipamento ao Departamento de TI.

5. Política de Armazenamento e Active Directory

Conforme arts. 5º e 6º do Decreto nº 9.047/2025 e art. 6º do Decreto nº 9.142/2025:

- Arquivos de trabalho devem ser salvos na unidade de rede institucional (identificada como G: ou outra letra, ou conforme orientação do Departamento de TI), que realiza backup diário automático.
- É terminantemente proibido o armazenamento de arquivos pessoais — fotos, vídeos, músicas ou quaisquer dados de uso privado — em servidores ou drives institucionais, sejam locais ou em nuvem.
- O ambiente de rede (Active Directory) é configurado para uso exclusivo de documentos e sistemas de trabalho.
- O uso inadequado do espaço de armazenamento institucional pode resultar em responsabilização funcional e sanções administrativas.
- O PDTI 2025-2026 estabelece como diretriz estratégica a preferência por soluções em nuvem para sistemas e armazenamento institucional, visando escalabilidade, segurança e continuidade dos serviços. Migrações e novas contratações em nuvem passam por avaliação prévia do DTGI e aprovação do Comitê de Governança Digital (Decreto nº 9.026/2025, seção 3.1.3).

6. Uso de Inteligência Artificial (IA)

ATENÇÃO — Leitura obrigatória antes de usar ferramentas de IA

O uso de ferramentas de Inteligência Artificial no ambiente de trabalho envolve riscos específicos à segurança da informação e à proteção de dados pessoais.
Leia com atenção as orientações desta seção antes de utilizar qualquer ferramenta de IA.

6.1. O que é e para que serve

Ferramentas de Inteligência Artificial (IA) generativa — como assistentes de texto, geradores de conteúdo, tradutores automáticos e ferramentas de análise de documentos — podem apoiar servidores em tarefas administrativas, redação de textos, pesquisas e organização de informações.

O PDTI 2025-2026 reconhece a automação e a Inteligência Artificial entre as diretrizes estratégicas da gestão municipal de TI (seção 3.1.2 do PDTI), reafirmando o potencial dessas tecnologias para otimizar processos administrativos e ampliar a eficiência do serviço público — desde que utilizadas com segurança e responsabilidade.

Seu uso pode ser permitido quando estritamente voltado a finalidades institucionais, desde que observadas as restrições desta seção e as normas de segurança da informação vigentes no Município.

6.2. Vedações expressas

Em conformidade com os princípios da confidencialidade, integridade e proteção de dados previstos no Decreto nº 9.142/2025 (art. 4º) e na Política de Proteção de Dados Pessoais (Decreto nº 9.032/2025), é expressamente proibido:

- Inserir dados pessoais de cidadãos em ferramentas de IA externas — incluindo nomes, CPFs, endereços, dados de saúde, renda, filiação ou qualquer informação que permita identificar uma pessoa natural.
- Submeter documentos sigilosos, processos administrativos, contratos, pareceres jurídicos ou qualquer informação classificada como confidencial a plataformas de IA não homologadas pelo Departamento de TI.
- Copiar e colar em ferramentas de IA conteúdos de sistemas internos, planilhas de dados nominais, relatórios de controle ou bases de dados da Prefeitura.
- Usar respostas geradas por IA como base para decisões administrativas sem revisão crítica e validação humana prévia.

Por que não inserir dados de cidadãos em ferramentas de IA externas?

Plataformas de IA externas processam e, em muitos casos, armazenam os dados inseridos em servidores fora do controle do Município. Isso configura compartilhamento de dados pessoais sem base legal adequada, violando a LGPD (art. 7º e seguintes) e os Decretos Municipais nº 9.032 e 9.142/2025.

Em caso de incidente, a Prefeitura responde como controladora dos dados perante a ANPD.

6.3. Usos permitidos e recomendados

O servidor pode utilizar ferramentas de IA para atividades que não envolvam dados pessoais, sigilosos ou restritos, tais como:

- Redigir ou revisar textos genéricos, ofícios-modelo, comunicados internos e apresentações que não contenham dados pessoais nem informações restritas.
- Pesquisar legislação, normas técnicas, manuais públicos e conteúdos de domínio público.
- Gerar estruturas de documentos, planilhas ou formulários em branco para uso posterior.
- Apoiar estudos, capacitações e atividades de formação profissional com conteúdos genéricos.
- Traduzir textos institucionais que não contenham dados pessoais ou informações sigilosas.

6.4. Responsabilidade sobre o conteúdo gerado por IA

- O servidor é integralmente responsável pelo conteúdo que submeter a ferramentas de IA e pelo resultado que utilizar em contexto institucional.
- Respostas de IA podem conter erros, imprecisões ou informações desatualizadas. Todo conteúdo gerado deve ser revisado criticamente antes de ser usado em documentos oficiais.
- Não é permitido assinar ou publicar documentos oficiais cujo conteúdo seja integralmente gerado por IA sem revisão e validação humana.
- O uso de IA para falsificar documentos, simular assinaturas ou realizar qualquer ato fraudulento é crime e sujeita o servidor a sanções administrativas, civis e penais.

6.5. Ferramentas homologadas

- Somente ferramentas de IA previamente avaliadas pelo Departamento de TI poderão ser utilizadas em atividades institucionais que envolvam documentos internos.
- A avaliação considerará critérios de segurança, privacidade por design, localização dos dados e conformidade com a LGPD.
- Dúvidas sobre quais ferramentas estão homologadas devem ser encaminhadas ao Departamento de TI via Sistema 1DOC.

6.6. Incidentes envolvendo IA

- Caso dados pessoais ou sigilosos sejam inadvertidamente inseridos em alguma ferramenta de IA, o servidor deve comunicar imediatamente ao Encarregado (DPO – Data Protection Officer), ao Departamento de TI e ao superior hierárquico.
- O incidente será tratado conforme o Plano de Resposta a Incidentes previsto nos arts. 12 e 13 do Decreto nº 9.142/2025.

Lembre-se: a IA é uma ferramenta de apoio, não um substituto para o julgamento profissional.
Decisões administrativas, pareceres técnicos e atos que produzam efeitos jurídicos exigem análise humana qualificada. Use a Inteligência Artificial com responsabilidade e senso crítico.

7. Digitalização de Processos e Atendimento Digital ao Cidadão

A transformação digital dos processos administrativos e do atendimento ao cidadão constitui prioridade estratégica da Administração Pública Municipal de São Lourenço do Oeste – SC, em conformidade com o Decreto Municipal nº 9.036/2025 (Governo Digital), o PDTI 2025-2026 (Decreto nº 9.026/2025) e a Lei Federal nº 14.129/2021 (Lei do Governo Digital).

7.1. Digitalização de Processos Internos

A tramitação de processos administrativos internos deve ser realizada prioritariamente por meio da plataforma de gestão digital municipal, substituindo progressivamente os fluxos em papel. Esta diretriz aplica-se a todos os setores da Administração Municipal e visa garantir rastreabilidade, agilidade, transparência e segurança na condução dos processos institucionais.

Para o cumprimento desta diretriz, os usuários devem observar:

- A abertura, tramitação e encerramento de processos administrativos devem ser realizados exclusivamente pelos sistemas municipais homologados pelo Departamento de TI, em especial o Sistema de Gestão Digital.
- Os fluxos de aprovação, despacho e assinatura devem ser conduzidos dentro da própria plataforma, sendo vedada a tramitação paralela por canais não oficiais, como aplicativos de mensagens ou e-mails particulares.

7.2. Atendimento Digital ao Cidadão

Em consonância com os princípios do Governo Digital e com o compromisso da Administração Municipal com a eficiência e a acessibilidade dos serviços públicos, os setores devem priorizar a oferta de atendimento online para todos os serviços que permitam essa modalidade sob a perspectiva técnica e legal.

Para tanto, devem ser observadas as seguintes diretrizes:

- Cada setor deve identificar, em conjunto com o Departamento de TI, os serviços passíveis de digitalização e disponibilização em canais eletrônicos, com vistas à ampliação progressiva do portfólio de serviços online.
- O atendimento presencial deve ser mantido como alternativa garantida ao cidadão, especialmente para casos que envolvam vulnerabilidade digital, exigência legal de presença física ou necessidade de validação documental.
- Os serviços digitalizados devem observar os princípios de simplicidade, acessibilidade e clareza, assegurando que o cidadão compreenda e utilize os canais disponíveis com autonomia.
- Dúvidas e solicitações relacionadas à implantação de serviços digitais devem ser encaminhadas ao Departamento de Tecnologia e Gestão da Informação via Sistema de Gestão Digital.

8. Incidentes de Segurança e Auditorias

Conforme arts. 10, 11 e 12 do Decreto nº 9.142/2025:

- Todo incidente de segurança — vazamento de dados, acesso não autorizado, perda de equipamento, ataque de phishing — deve ser comunicado imediatamente ao Encarregado (DPO – Data Protection Officer), ao superior hierárquico e ao Departamento de TI.
- O Departamento de Tecnologia realiza auditorias regulares em estações de trabalho, redes, e-mails e dispositivos remotos.
- Em caso de violação das diretrizes, o Departamento de TI poderá restringir ou suspender acessos imediatamente.
- Os dados coletados em auditorias poderão ser disponibilizados a autoridades judiciais ou superiores hierárquicos, conforme previsto no art. 11 do Decreto nº 9.142/2025.

9. Penalidades pelo Descumprimento

O descumprimento das diretrizes deste Guia sujeita o servidor ou colaborador às seguintes sanções (arts. 7º e 15 dos Decretos nº 9.047 e 9.142/2025):

- Advertência verbal ou escrita.
- Treinamento obrigatório em segurança da informação.

- Sanções administrativas e disciplinares previstas no Estatuto dos Servidores Públicos Municipais.
- Rescisão contratual, no caso de terceirizados e prestadores de serviço.
- Medidas judiciais cíveis e penais, nos casos de violações graves — especialmente aquelas que resultem em dano a dados pessoais de cidadãos.

10. Compromisso e Responsabilidade

Ao utilizar os sistemas e recursos de TI do Município, o servidor e o colaborador comprometem-se a:

- Atuar com responsabilidade, ética e transparência.
- Proteger os dados pessoais e institucionais sob sua guarda.
- Cumprir a legislação vigente — LGPD, Marco Civil da Internet, Lei de Governo Digital e os Decretos Municipais aplicáveis.
- Contribuir para um ambiente digital seguro, eficiente e orientado ao interesse público e ao cidadão.
- Manter-se atualizado por meio dos treinamentos e capacitações promovidos pelo Município (art. 12, Decreto nº 9.032/2025 e art. 7º, Decreto nº 9.142/2025).

São Lourenço do Oeste – SC, 2026.

YAN CARLOS PIETA
Diretor do Departamento de Tecnologia e Gestão da Informação
Secretaria Municipal de Administração e Fazenda
Prefeitura Municipal de São Lourenço do Oeste – SC