POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Prefeitura Municipal de Bragança Paulista

Documento:	PSI-PMBP-001
Versão:	1.0
Data de Emissão:	2025
Próxima Revisão:	2026
Elaborado por:	Everton Ferreira
Cargo:	Responsável pela Tecnologia da Informação
Aprovado por:	Andre Elesbão
Cargo:	Prefeito Municipal de Bragança Paulista
CNPJ:	46.352.746/0001-65
Endereço:	Av. Antônio Pires Pimentel, 2015 – Centro – Bragança Paulista/SP – CEP 12914-900
Classificação:	Interno – Uso Restrito

1. FINALIDADE

Esta Política de Segurança da Informação estabelece as regras básicas para proteger as informações da Prefeitura Municipal de Bragança Paulista, garantindo a continuidade dos serviços públicos, a proteção de dados pessoais de cidadãos e servidores e o cumprimento da legislação vigente, em especial a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) e a Lei de Acesso à Informação (LAI – Lei nº 12.527/2011).

2. ABRANGÊNCIA

Esta política aplica-se a:

• Todos os servidores efetivos, comissionados, temporários, estagiários e terceirizados;

• Todas as Secretarias, unidades e órgãos da Administração Direta;

• Fornecedores e prestadores de serviço que acessem sistemas ou dados da Prefeitura;

• Todos os recursos de tecnologia da informação: computadores, notebooks, celulares corporativos, redes, e-mail, sistemas e dados.

3. PRINCÍPIOS BÁSICOS

A gestão da segurança da informação na Prefeitura Municipal de Bragança Paulista é orientada pelos seguintes princípios:

I. Confidencialidade – A informação deve ser acessível apenas às pessoas autorizadas.

II. Integridade – A informação deve ser correta, completa e não alterada de forma indevida.

III. Disponibilidade – A informação e os sistemas devem estar acessíveis quando necessários ao serviço público.

IV. Responsabilidade – Cada usuário é responsável pelo uso correto dos recursos e pela proteção das informações que acessa.

V. Legalidade – Todas as atividades devem estar em conformidade com a LGPD, a LAI e demais leis aplicáveis.

4. REGRAS GERAIS DE USO DOS RECURSOS DE TI

1. Os recursos de tecnologia da informação existem para fins de trabalho e prestação de serviços públicos.

2. O uso pessoal eventual é tolerado, desde que não prejudique o serviço, não viole leis e não comprometa a segurança das informações.

3. É expressamente proibido:

• Instalar programas sem autorização da área de TI;

• Acessar conteúdos ilegais, ofensivos ou inadequados ao ambiente de trabalho;

• Utilizar e-mail ou sistemas da Prefeitura para fins comerciais particulares ou político-partidários;

• Compartilhar usuário e senha com qualquer pessoa, inclusive colegas de trabalho.

1. A Prefeitura poderá monitorar o uso dos sistemas para fins de segurança, auditoria e conformidade legal, nos termos da legislação aplicável.

5. CONTAS DE ACESSO E SENHAS

1. Cada servidor, estagiário ou terceirizado deve ter seu próprio usuário, pessoal e intransferível.

2. As senhas devem:

• Ser difíceis de adivinhar; recomenda-se o uso de frases-senha (exemplo: "TrabalhoNaPref2026!");

• Ter no mínimo 12 caracteres;

• Não ser anotadas em locais visíveis nem compartilhadas com ninguém;

• Ser trocadas imediatamente em caso de suspeita de comprometimento.

1. Quando o servidor ou terceirizado se desliga, seu acesso deve ser bloqueado pela TI no mesmo dia do desligamento.

2. Contas sem uso por período superior a 45 dias serão automaticamente bloqueadas.

6. PROTEÇÃO DOS EQUIPAMENTOS E SISTEMAS

2. Os equipamentos de TI da Prefeitura devem:

• Ter antivírus ativo e atualizado;

• Receber atualizações de segurança regularmente;

• Ser bloqueados (tela de bloqueio) quando o usuário se ausentar, com ativação automática em até 10 minutos.

3. É proibido conectar à rede interna da Prefeitura:

• Computadores pessoais sem autorização prévia da TI;

• Equipamentos desconhecidos ou não inventariados.

4. Sistemas com dados de cidadãos, servidores, folha de pagamento, saúde e arrecadação devem ter:

• Acesso restrito por perfil de função (somente quem precisa acessa);

• Rotinas de cópia de segurança (backup) definidas e monitoradas pela TI.

7. PROTEÇÃO DE DADOS PESSOAIS (LGPD)

5. Os dados pessoais de cidadãos, servidores e terceiros devem ser tratados:

• Apenas para finalidades relacionadas às atividades da Prefeitura;

• Pelo tempo estritamente necessário, conforme a legislação vigente.

6. É proibido:

• Consultar dados pessoais sem necessidade relacionada ao serviço;

• Divulgar dados pessoais fora da Prefeitura sem autorização formal;

• Enviar listas com dados sensíveis (saúde, situação socioeconômica, dados fiscais) por e-mail sem proteção adequada.

7. Solicitações de cidadãos sobre seus dados (acesso, correção ou exclusão, quando aplicável) devem ser encaminhadas ao Encarregado pela Proteção de Dados (DPO) ou à área designada para esse fim.

8. USO DE INTERNET, E-MAIL E MENSAGENS

1. O e-mail institucional deve ser utilizado para comunicações relacionadas ao trabalho.

2. Ao comunicar-se em nome da Prefeitura, o servidor deve manter linguagem respeitosa e profissional.

3. É proibido:

• Clicar em links suspeitos ou abrir anexos de remetentes desconhecidos sem verificação prévia;

• Repassar correntes, boatos, promoções duvidosas ou conteúdos de origem não verificada;

• Utilizar o e-mail institucional para fins pessoais, comerciais ou político-partidários.

8. Em caso de dúvida sobre a autenticidade de um e-mail ou mensagem, o servidor deve:

• Não clicar em links nem baixar arquivos;

• Encaminhar o caso à área de TI para análise.

9. INCIDENTES DE SEGURANÇA

Considera-se incidente de segurança, entre outros:

• Vazamento ou suspeita de vazamento de dados;

• Perda ou roubo de notebook, celular ou dispositivo com dados da Prefeitura;

• Infecção por vírus, ransomware ou programas maliciosos;

• Acessos não autorizados a sistemas ou tentativas repetidas de login;

• Golpes digitais envolvendo dados ou pagamentos da Prefeitura (inclusive fraudes via PIX).

Todo servidor é obrigado a comunicar imediatamente à TI ou ao seu gestor qualquer situação suspeita em sistemas, equipamentos ou comunicações.

Ao receber o relato, a TI poderá:

• Desconectar equipamentos da rede;

• Suspender acessos comprometidos;

• Acionar a Controladoria, o Jurídico ou outros órgãos competentes, conforme necessário.

10. RESPONSABILIDADES

Prefeito e Secretários:

• Apoiar esta política, dar exemplo e garantir condições para sua aplicação.

Área de Tecnologia da Informação:

• Criar e encerrar contas de acesso;

• Manter antivírus, atualizações e backups;

• Apoiar a investigação de incidentes de segurança;

• Orientar as secretarias sobre boas práticas.

Gestores das Secretarias:

• Garantir que suas equipes conheçam e cumpram esta política;

• Informar à TI sobre entrada e saída de servidores e terceirizados;

• Comunicar imediatamente incidentes que afetem sua área.

Todos os usuários (servidores, estagiários e terceirizados):

• Respeitar integralmente as regras desta política;

• Proteger suas credenciais e os equipamentos que utilizam;

• Reportar situações suspeitas sem demora.

11. CONSEQUÊNCIAS PELO DESCUMPRIMENTO

O descumprimento desta política poderá resultar em:

• Advertência verbal ou escrita;

• Restrição ou suspensão de acesso a sistemas da Prefeitura;

• Abertura de processo administrativo disciplinar, conforme o Estatuto dos Servidores Municipais e normas internas;

• Rescisão contratual, no caso de terceirizados e prestadores de serviço;

• Comunicação às autoridades competentes quando houver indícios de crime ou dano a terceiros.

As medidas serão aplicadas de forma proporcional à gravidade e à intencionalidade do ato, observando o devido processo legal.

12. REVISÃO DESTA POLÍTICA

Esta política será revisada, no mínimo:

• A cada **12 meses**; ou

• Sempre que houver:

• Mudança relevante na legislação (LGPD, LAI e afins);

• Incidente grave de segurança da informação;

• Alteração significativa na infraestrutura de TI ou na estrutura organizacional.

13. APROVAÇÃO

Elaborado por:

Nome:

Cargo: _

Assinatura: ___

Data: / / 2026

Aprovado por:

Nome:

Cargo: Prefeito Municipal de Bragança Paulista

Assinatura: ___

Data: / / 2026