PREFEITURA MUNICIPAL DE BOTUCATU

BOTUCATU, 13 / 10 / 2025
POLÍTICA DE SEGURANÇA PARA USO DO E-MAIL INSTITUCIONAL

1. OBJETIVO

- Estabelecer diretrizes e normas de segurança da informação para a criação, uso, manutenção e desativação de contas de e-mail institucional da Prefeitura Municipal de Botucatu, visando garantir a confidencialidade, integridade, disponibilidade e autenticidade das comunicações eletrônicas oficiais.

2. ABRANGÊNCIA

- Aplica-se a todos os servidores concursados ou comissionados da prefeitura municipal de Botucatu.

3. PRINCÍPIOS

- I — Legalidade e observância da Lei Geral de Proteção de Dados (Lei nº 13.709/2018);
- II — Responsabilidade individual pelo uso da conta;
- III — Prevenção contra vazamento de informações e incidentes de segurança;
- IV — Rastreamento e auditoria de atividades quando necessário;
- V — Preservação da imagem institucional do Município.

4. SEGURANÇA DE CONTA E SENHAS

4.1 Responsabilidade
- Cada usuário é responsável pela guarda e sigilo de suas credenciais (usuário e senha).

4.2 É proibido:
- Compartilhar senhas, repassá-las a terceiros ou armazená-las em locais visíveis;
- Deixar sessões abertas em computadores compartilhados ou públicos.

4.3 Criação de contas e senhas

4.3.1 Contas

- O padrão nome.sobrenome@botucatu.sp.gov.br ou setor@botucatu.sp.gov.br será adotado para a criação das contas. Em caso de nomes iguais, a Divisão de TI definirá a diferenciação adequada. As informações para criação da conta devem ser preenchidas integralmente.
- E-mails não pessoais (ex.: prefeitura@botucatu.sp.gov.br) deverão possuir um responsável direto designado.

4.3.2 Senhas

- Mínimo de 8 caracteres;
- Combinação de letras maiúsculas, minúsculas, números e símbolos;
- Troca obrigatória a cada 60 dias, com aviso automático 5 dias antes do vencimento.

4.4 Acesso

- O acesso fora da rede municipal deve ser feito exclusivamente por conexões seguras (HTTPS) pelo endereço https://webmail.botucatu.sp.gov.br, podendo requerer autenticação multifator (MFA).
- O acesso dentro da rede municipal também deve ser feito via HTTPS, admitindo exceções apenas para aplicativos homologados (Outlook, Thunderbird), mediante solicitação formal e análise da Divisão de TI.
- Nesses casos, o acesso poderá ser restrito à rede interna da Prefeitura.

5. ENVIO E RECEBIMENTO DE MENSAGENS

5.1 Uso institucional

- O e-mail institucional deve ser utilizado exclusivamente para fins de interesse público e comunicação funcional.

5.2 É vedado o envio de:

- Correntes, mensagens de cunho político-partidário, religioso ou comercial;
- Conteúdos ofensivos, discriminatórios ou que causem constrangimento;
- Arquivos executáveis (.exe, .bat, .vbs etc.) sem justificativa técnica e prévia aprovação da TI.

5.3 Limites técnicos

- Mensagens e anexos devem respeitar o limite técnico estabelecido pela Divisão de TI (até 50 MB).
- Cada mensagem não deve conter mais de 50 destinatários para evitar aumento do SPAM Score do domínio.
- Em disparos massivos, utilizar Cópia Oculta (CCO).

5.4 Boas práticas

- Priorizar formatos abertos (PDF, ODT, CSV etc.);
- Toda mensagem deve conter assinatura institucional, incluindo: Nome do remetente; Nome da instituição; Nome do departamento; Ramal ou telefone do setor.

5.5 Recomendações adicionais

- Limite prático seguro: até 50 destinatários (preferencialmente via Cco).
- Segmentação: enviar em blocos (ex.: 50-50-50) com intervalos de 5 minutos.
- Endereço preferencial: use e-mail nominal (ex.: joao.silva@botucatu.sp.gov.br).

5.6 Fatores que elevam o SPAM Score e devem ser evitados a todo custo:

- Envio em massa sem personalização;
- Endereço remetente genérico (ex.: noreply@dominio.gov.br);
- Palavras “sensíveis” (promoção, urgente, clique aqui etc.);
- Anexos grandes ou executáveis.

6. ARMAZENAMENTO E RETENÇÃO

- O e-mail institucional é propriedade do Município e não deve ser utilizado como armazenamento pessoal.

O usuário deve:

- Arquivar documentos oficiais em sistemas próprios (ex.: processo eletrônico, protocolo digital);
- Evitar anexos repetidos;
- Respeitar as cotas de armazenamento.

- Mensagens antigas poderão ser removidas automaticamente conforme política de retenção da TI.
- Mensagens da lixeira serão apagadas automaticamente após 30 dias.

7. PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

- 7.1 É proibido repassar dados pessoais sensíveis (CPF, RG, saúde, financeiros etc.) sem finalidade administrativa clara e sem proteção adequada (criptografia, acesso restrito).
- 7.2 Documentos sigilosos devem ser enviados preferencialmente via sistemas autenticados e criptografados, nunca em anexo aberto (Por exemplo: processos digitais, ERP da prefeitura e/ou outros sistemas informatizados utilizados por esta municipalidade)
- 7.3 Todos os usuários devem respeitar a LGPD e as políticas internas de Governança de Dados e Segurança da Informação.

8. INCIDENTES DE SEGURANÇA

- 8.1 O usuário deve notificar imediatamente a equipe de TI em caso de:
- Suspeita de invasão ou acesso indevido;
- Recebimento de phishing, ransomware ou mensagens fraudulentas;
- Perda ou extravio de dispositivo móvel com e-mail institucional.

- 8.2 A Divisão de TI poderá bloquear temporariamente o acesso para investigação, registrando todos os procedimentos.

- 8.3 A auditoria de logs será feita apenas por pessoal autorizado, conforme a legislação vigente.

9. USO EM DISPOSITIVOS MÓVEIS

- É vedada a configuração de e-mail em dispositivos pessoais (celulares, tablets, notebooks).
- O usuário deve, quando precisar acessar sua caixa postal pelo celular, utilizar o endereço https://webmail.ativar bloqueio de tela, criptografia e rastreamento remoto (quando disponíveis).
- Em caso de desligamento ou troca de equipamento, o usuário deve remover a conta institucional e confirmar a exclusão junto à TI.

10. MONITORAMENTO E AUDITORIA

- A Prefeitura poderá monitorar o uso das contas exclusivamente para fins de segurança, observando a razoabilidade e o sigilo conforme o Marco Civil da Internet (Lei nº 12.965/2014).
- Os logs de acesso e envio poderão ser armazenados por até 5 anos ou conforme o prazo legal aplicável.

11. RESPONSABILIDADES

- Usuário: uso ético e responsável; proteção de senhas e dados; comunicação imediata de incidentes.
- Gestor da Unidade: comunicar desligamentos e mudanças de vínculo; promover conhecimento das normas por palestras ou memorandos.
- Secretaria de TI: criar, monitorar, auditar e apagar contas; manter infraestrutura segura; emitir relatórios; realizar backups diários das contas por pelo menos 30 dias.

12. SANÇÕES

O descumprimento desta Política poderá resultar em:

- I — Advertência formal;
- II — Suspensão temporária da conta;
- III — Responsabilização administrativa conforme o Estatuto do Servidor;
- IV — Encaminhamento à Procuradoria ou ao Ministério Público em casos graves.

13. VIGÊNCIA

Esta Política entra em vigor na data de sua publicação, devendo ser revisada anualmente ou sempre que houver atualização tecnológica, normativa ou legal aplicável.