Decreto nº 1879 de 17 de novembro de 2025.

Dispõe sobre a Política de Segurança da Informação no âmbito do Município de Cambuci.

O Prefeito do Município de Cambuci, no uso das suas atribuições e em cumprimento ao disposto na Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD):

Decreta:

Art. 1º Fica aprovada, na forma do Anexo, a Política de Segurança da Informação no âmbito do Município de Cambuci.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Cambuci, 17 de novembro de 2025.

Murillo Silva Defanti
Prefeito Municipal de Cambuci

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Conforme a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)

Objetivo

Esta Política de Segurança da Informação tem como objetivo estabelecer diretrizes e controles para garantir a **confidencialidade, integridade e disponibilidade** das informações tratadas pela Prefeitura Municipal de Cambuci, em conformidade com a **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

Abrangência

Aplica-se a todos os **colaboradores, terceiros, prestadores de serviços, parceiros e demais partes que tratem dados pessoais** em nome da Prefeitura Municipal de Cambuci, independentemente do vínculo contratual ou da forma de tratamento (manual ou automatizado).

Princípios da Proteção de Dados

A Prefeitura Municipal de Cambuci compromete-se a seguir os princípios estabelecidos no Art. 6º da LGPD:

- Finalidade
- Adequação
- Necessidade
- Livre acesso
- Qualidade dos dados
- Transparência
- Segurança
- Prevenção
- Não discriminação
- Responsabilização e prestação de contas

Classificação da Informação

As informações serão classificadas conforme seu grau de sensibilidade:

- Pública
- Interna
- Confidencial
- Dados Pessoais
- Dados Sensíveis

Proteção de Dados Pessoais

- Dados pessoais devem ser coletados apenas quando estritamente necessários e com base legal adequada.
- O tratamento deve ser transparente, com informações claras ao titular sobre a finalidade e forma de tratamento.

- O acesso aos dados pessoais será restrito apenas a pessoas autorizadas.

Criação de Senhas

As senhas de acesso a sistemas da empresa devem atender aos seguintes requisitos mínimos:

- Mínimo de **8 caracteres**.
- Incluir **letras maiúsculas, minúsculas, números e caracteres especiais**.
- Evitar uso de palavras comuns, nomes pessoais, datas de nascimento ou sequências óbvias (ex: 123456, qwerty).
- Senhas não podem ser iguais às últimas **5 senhas utilizadas**.

Renovação de Senhas

- As senhas devem ser alteradas periodicamente, a cada **90 dias**, ou imediatamente em caso de suspeita de comprometimento.
- Não é permitido reutilizar senhas antigas ou similares.

Proteção e Armazenamento

- É proibido anotar senhas em papéis, planilhas, e-mails ou arquivos não criptografados.
- Senhas devem ser armazenadas, quando necessário, **criptografadas** com algoritmos seguros.
- Sistemas devem exigir **bloqueio automático** após tentativas malsucedidas consecutivas de login.

Autenticação Adicional

- Sempre que possível, deve ser implementada **autenticação de dois fatores (2FA)** para sistemas que contenham dados pessoais ou sensíveis.
- A 2FA pode incluir: código por aplicativo autenticador, biometria ou token.

Responsabilidade do Usuário

- O usuário é o **único responsável** pela guarda e uso seguro de sua senha.
- O compartilhamento de senhas é **terminantemente proibido**, mesmo entre membros da mesma equipe.
- Caso ocorra o compartilhamento indevido, o usuário será responsabilizado por quaisquer consequências decorrentes.
- Sistemas que armazenem ou tratem **dados pessoais** devem ter controles de acesso baseados em senhas seguras.
- O acesso deve ser **registrado e auditável**, garantindo rastreabilidade em conformidade com os princípios da LGPD.
- Cada usuário terá acesso apenas às informações necessárias para o desempenho de suas funções.

Segurança Física e Lógica

- Ambientes físicos com acesso a informações sensíveis devem ter controle de entrada.
- Sistemas e redes devem contar com proteção contra ameaças (antivírus, firewall, criptografia, etc.).

Gestão de Incidentes de Segurança

- Todo incidente de segurança da informação deve ser comunicado imediatamente ao Encarregado de Dados (DPO).
- Será conduzida uma investigação e, se necessário, feita comunicação à ANPD e aos titulares afetados, conforme art. 48 da LGPD.

Treinamento e Conscientização

- Todos os colaboradores receberão treinamentos periódicos sobre segurança da informação e proteção de dados pessoais.

Retenção e Descarte de Dados

- Os dados pessoais serão mantidos somente pelo período necessário ao cumprimento de sua finalidade ou conforme exigido por lei.
- O descarte de dados será feito de forma segura, com garantia de que não possam ser recuperados.

Contratação de Terceiros

- Terceiros que tratem dados pessoais em nome da empresa deverão assinar acordos de confidencialidade e estar em conformidade com esta política e com a LGPD.

Backup

Aplica-se a todos os dados e sistemas corporativos, especialmente aqueles que contenham **dados pessoais e dados pessoais sensíveis**, tratados por colaboradores, terceiros, fornecedores ou prestadores de serviços que operem em nome da Prefeitura Municipal de Cambuci.

Os sistemas críticos devem ter backups realizados **diariamente**.

Sistemas não críticos poderão ter backups em periodicidade **semanal** ou conforme definido por sua criticidade.

Backup Completo: cópia integral dos dados.

Armazenamento

- Os backups devem ser armazenados em **ambientes seguros**, com controle de acesso e, preferencialmente, em **local físico diferente** do ambiente de produção (ex: armazenamento em nuvem com criptografia ou datacenter secundário).
- Devem ser utilizados meios confiáveis (discos rígidos seguros, serviços de nuvem certificados, etc.).

Criptografia e Proteção

- Os dados serão retidos apenas pelo período necessário à sua finalidade, conforme definido em política de retenção de dados ou obrigação legal.
- Findo o prazo, os backups contendo dados pessoais serão **devidamente eliminados**, com segurança (eliminação definitiva, impossibilitando recuperação).

Testes de Restauração

- Devem ser realizados testes periódicos de **restauração de dados**, no mínimo uma vez a cada trimestre, para garantir a integridade dos backups e a eficiência dos procedimentos de recuperação.

Monitoramento e Registro

- Todos os procedimentos de backup e restauração devem ser **registrados** (logs), possibilitando auditoria e rastreabilidade.
- Tentativas de acesso indevido aos backups devem ser monitoradas e reportadas.
-

Direitos dos Titulares de Dados

A Prefeitura Municipal de Cambuci garante aos titulares o exercício de seus direitos, tais como:

- Acesso aos dados
- Correção de dados incompletos ou desatualizados
- Anonimização, bloqueio ou eliminação de dados desnecessários
- Portabilidade dos dados
- Revogação do consentimento
- Informação sobre compartilhamento de dados

As solicitações deverão ser feitas por meio dos canais oficiais da empresa e serão respondidas nos prazos estabelecidos pela LGPD.

Responsabilidades

- **Colaboradores:** devem cumprir esta política, manter sigilo das informações acessadas e reportar incidentes.
- **Gestores:** são responsáveis por garantir que suas equipes conheçam e cumpram esta política.
- **Encarregado de Dados (DPO):** responsável por orientar, receber comunicações dos titulares e interagir com a ANPD.

Penalidades pelo Descumprimento

O descumprimento desta política poderá acarretar:

- Medidas disciplinares internas
- Rescisão contratual
- Responsabilização civil, administrativa e penal, conforme previsto em lei.

Atualizações

Esta política será revisada periodicamente ou sempre que houver alterações legais ou mudanças nos processos de tratamento de dados.