Decreto nº 1878 de 17 de novembro de 2025.

Dispõe sobre a Política de Resposta a Incidentes 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 Resposta a Incidentes 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 resposta a incidentes (conforme a LGPD)

1. **Objetivo da Política**
   - Garantir a pronta resposta a incidentes de segurança envolvendo dados pessoais.
2. **Definição de Incidente de Segurança**
   - Qualquer evento adverso real ou suspeito que comprometa dados pessoais (ex: vazamentos, acessos indevidos, ataques cibernéticos, perda de dispositivos, etc.).
3. **Papéis e Responsabilidades**
   - Envolvimento de um Encarregado (DPO)
   - Definição de equipe de resposta (TI, Jurídico, Comunicação, etc.)
   - Acionamento da alta direção, se necessário
4. **Classificação de Incidentes**
   - Por nível de gravidade (baixo, moderado, alto, crítico)
   - Análise de risco à privacidade
5. **Comunicação e Notificação**
   - Procedimento para comunicar à ANPD e aos titulares
   - Prazos e meios de comunicação (2 dias úteis)
6. **Registro e Documentação**
   - Todos os incidentes devem ser registrados (mesmo os de baixo impacto)
   - Histórico de ações e decisões tomadas
7. **Treinamento e Simulações**
   - Treinamentos periódicos para a equipe
   - Simulações de incidentes (exercícios de resposta)
8. **Fluxo De Identificação De Incidentes Com Dados – Lgpd**

1 - Detecção do Evento

2 – Registro Inicial do Incidente

3 – Análise e Classificação do Incidente

4 – Verificação dos Dados Pessoais Envolvidos

5 – Avaliação de Risco ao Titular

6 – Acionamento do Encarregado (DPO) e Comitê de Resposta

7 – Decisão sobre comunicação à ANPD e aos Titulares

8 – Implementação de Medidas Corretivas e de Contenção

9 – Registro Completo e Relatório Final

10 – Ações Preventivas e Aprendizado

9. ETAPAS DETALHADAS

Detecção do Evento

- Origem: sistema de segurança, usuário interno, cliente, fornecedor, etc.
- Alerta de firewall, e-mail suspeito, extravio de notebook, etc.

2. Registro Inicial

- Data/hora, local, sistemas afetados, quem identificou, descrição inicial.
- Deve ser feito em sistema próprio ou planilha de controle com trilha de auditoria.

3. Análise Técnica

- Verificar o tipo de incidente: acesso não autorizado? vazamento? perda?
- Classificar como incidente com/sem impacto a dados pessoais.

4. Verificação de Dados Pessoais

- Os dados afetados envolvem:
  - Dados identificáveis?
  - Dados sensíveis (ex: biometria, saúde)?
  - Dados de crianças/adolescentes?
- Volume de dados e categorias de titulares.

5. Avaliação de Risco ao Titular

- O incidente gera risco ou dano relevante (financeiro, moral, reputacional, etc.)

6. Acionamento do DPO e Comitê

- O Encarregado de Dados deverá liderar a avaliação da necessidade de notificação, sendo envolvidos o Jurídico, TI, Segurança da Informação e Comunicação.

7. Comunicação à ANPD e Titulares (Art. 48)

- Se o incidente **pode acarretar risco ou dano relevante**, deve-se notificar:
  - ANPD
  - Titulares afetados

- Prazos: 2 dias
- Informações obrigatórias:
  - Natureza dos dados afetados
  - Titulares envolvidos
  - Medidas técnicas e administrativas adotadas
  - Riscos
  - Justificativa de eventual atraso
  - Medidas de mitigação

8. Medidas Corretivas

- Contenção (ex: isolamento de rede, revogação de acessos)
- Mitigação (ex: reset de senhas, envio de alertas a clientes)
- Correção de falhas de segurança

9. Relatório Final e Documentação

- Registro completo em relatório técnico e jurídico.
- Armazenar por período mínimo definido pela política interna (5 anos).
- Usado como prova de conformidade.

10. Ações de Melhoria Contínua

- Atualização de políticas e controles
- Treinamentos internos
- Revisão do Plano de Resposta a Incidentes

Fluxo de detecção e contenção de incidentes.

1. Detecção	Receber alerta ou denúncia	TI / Qualquer colaborador	E-mail, SIEM, canal de denúncia
2. Registro	Inserir dados no formulário de incidentes	TI / DPO	Planilha ou sistema
3. Avaliação	Verificar dados pessoais envolvidos	TI / Jurídico / DPO	Checklist
4. Decisão	Notificar ANPD e titulares (se necessário)	DPO / Jurídico	Formulário ANPD
5. Correção	Aplicar correções técnicas	TI / Segurança	Firewall, logs, backups
6. Encerramento	Relatório final e melhoria contínua	DPO / Segurança	Documento interno