Prezado(a) Gestor(a), Este questionário faz parte de uma pesquisa acadêmica para a dissertação de mestrado na Fundação Getulio Vargas (FGV-SP). O objetivo é realizar um levantamento sobre o uso de tecnologias de cidades inteligentes e as práticas de segurança de dados e conformidade com a Lei Geral de Proteção de Dados (LGPD) nos municípios brasileiros e as boas práticas de gestão de dados. Sua colaboração é fundamental para o sucesso desta pesquisa.

QUESTIONÁRIO DE PESQUISA
Seção 1: Uso de Tecnologias de Cidades Inteligentes Nesta seção, buscamos entender quais tecnologias o município utiliza para monitoramento e gestão urbana.

1.1. O município utiliza câmeras para segurança pública? (x) Sim ( ) Não

1.2. Se sim, essas câmeras utilizam tecnologia de reconhecimento facial?
Sim (x) Não ( ) Não se aplica

1.3. O município utiliza imagens de satélite, drones ou fotos aéreas para fins de fiscalização ou gestão (ex: atualização do valor venal do IPTU)? (x) Sim ( ) Não

1.4. O município monitora as condições do trânsito com o auxílio de dados de aplicativos como Google Maps ou Waze? (x) Sim ( ) Não

1.5. O município disponibiliza aplicativos ou sites oficiais para que a população possa solicitar serviços, registrar demandas ou participar de consultas públicas? (x) Sim ( ) Não

1.6. O município utiliza outras tecnologias de sensores no ambiente urbano (ex: sensores em lixeiras, radares de velocidade, sensores de qualidade do ar, etc.)? (x) Sim ( ) Não Se sim, por favor, liste quais: RADAR DE VELOCIDADE

Seção 2: Segurança da Informação e Privacidade de Dados Esta seção aborda as práticas adotadas para proteger os dados coletados e garantir a conformidade com a LGPD. Bloco A: Conformidade com a LGPD.

2.1. O município possui mecanismos para verificar a integridade dos dados e prevenir acessos não autorizados? (x) Sim ( ) Não

2.2. Os dados pessoais coletados são armazenados de forma anonimizada (impossibilitando a identificação do indivíduo)? ( ) Sim (x) Não

2.3. Os dados pessoais sensíveis (como dados de saúde ou biometria) são armazenados com pseudonimização (substituição do dado por um código)? ( ) Sim (x) Não

2.4. Caso os dados sejam pseudonimizados, o acesso à informação que permite reverter a pseudonimização é restrito apenas a agentes autorizados? ( ) Sim (x) Não

2.5. O município solicita o consentimento do cidadão (Termo de Consentimento) antes de coletar e tratar seus dados pessoais? (x) Sim ( ) Não

2.6. O município elabora o Relatório de Impacto à Proteção de Dados (RIPD) para atividades de tratamento de dados que apresentam alto risco? (x) Sim ( ) Não Bloco B: Governança e Segurança Técnica

2.7. Os dados são armazenados em bancos de dados separados (clusterizados) de acordo com sua natureza ou nível de sensibilidade? ( ) Sim
(x) Não

2.7.1. Se sim, cada banco de dados separado possui uma camada de criptografia distinta? ( ) Sim (x) Não

2.8. A criptografia é aplicada aos dados desde o momento de sua coleta (criptografia by design)? ( ) Sim, a criptografia é aplicada desde a concepção ( ) Não, a criptografia é aplicada posteriormente (x) Os dados não são criptografados

2.9. Onde os dados coletados pelo município são armazenados? ( ) Em servidores próprios (infraestrutura local) ( ) Em servidores de terceiros (data center físico contratado) ( ) Em serviços de nuvem (ex: AWS, Google Cloud, Azure) ( ) Outros: _____ (x) Os dados não são armazenados de forma centralizada

2.10. O município utiliza a tecnologia blockchain para proteger os registros de dados? ( ) Sim (x) Não

2.11. Os sistemas de acesso aos dados registram logs que permitem auditar quem acessou, quando e o que foi feito? (x) Sim ( ) Não

2.12. O acesso às informações é granular, ou seja, cada funcionário só pode acessar os dados estritamente necessários para sua função? (x) Sim ( ) Não

2.13. Para acessar dados sensíveis, é exigido mais de um fator de autenticação (ex: senha + token)? ( ) Sim (x) Não

2.14. As soluções de antivírus em todos os computadores com acesso a bancos de dados são atualizadas de forma imediata? ( ) Sim (x) Não

2.15. As atualizações de segurança (patches) para sistemas operacionais e bancos de dados são aplicadas imediatamente após sua disponibilização pelos fabricantes? (x) Sim ( ) Não

2.16. A instalação de novos programas nos computadores com acesso a dados é controlada e restrita apenas a administradores autorizados? (x) Sim, apenas usuários autorizados podem instalar ( ) Não, qualquer usuário pode instalar programas

Seção 3: Treinamento e Capacitação

3.1. Os servidores e funcionários que lidam com dados pessoais recebem treinamentos periódicos sobre a LGPD e segurança da informação? (x) Sim ( ) Não

3.2. Se sim, qual a frequência desses treinamentos? ( ) Mais de uma vez por semestre ( ) Semestralmente ( ) Anualmente (x) Com frequência menor que anual

Seção 4: Orçamento e Investimento

4.1. Qual percentual do orçamento de tecnologia do município é especificamente destinado à segurança da informação e proteção de dados?

(x) Menos de 1% ( ) Entre 1% e 5% ( ) Entre 5,1% e 10% ( ) Entre 10,1% e 20%
( ) Mais de 20% Seção

5: Resposta a Incidentes

5.1. O município já sofreu algum ataque cibernético (ex: ransomware) ou incidente de vazamento de dados? ( ) Sim (x) Não

5.2. Se sim, quais foram as principais medidas adotadas para conter e remediar o incidente? (resposta aberta) Agradeço imensamente sua disponibilidade e contribuição para esta pesquisa.
Atenciosamente,