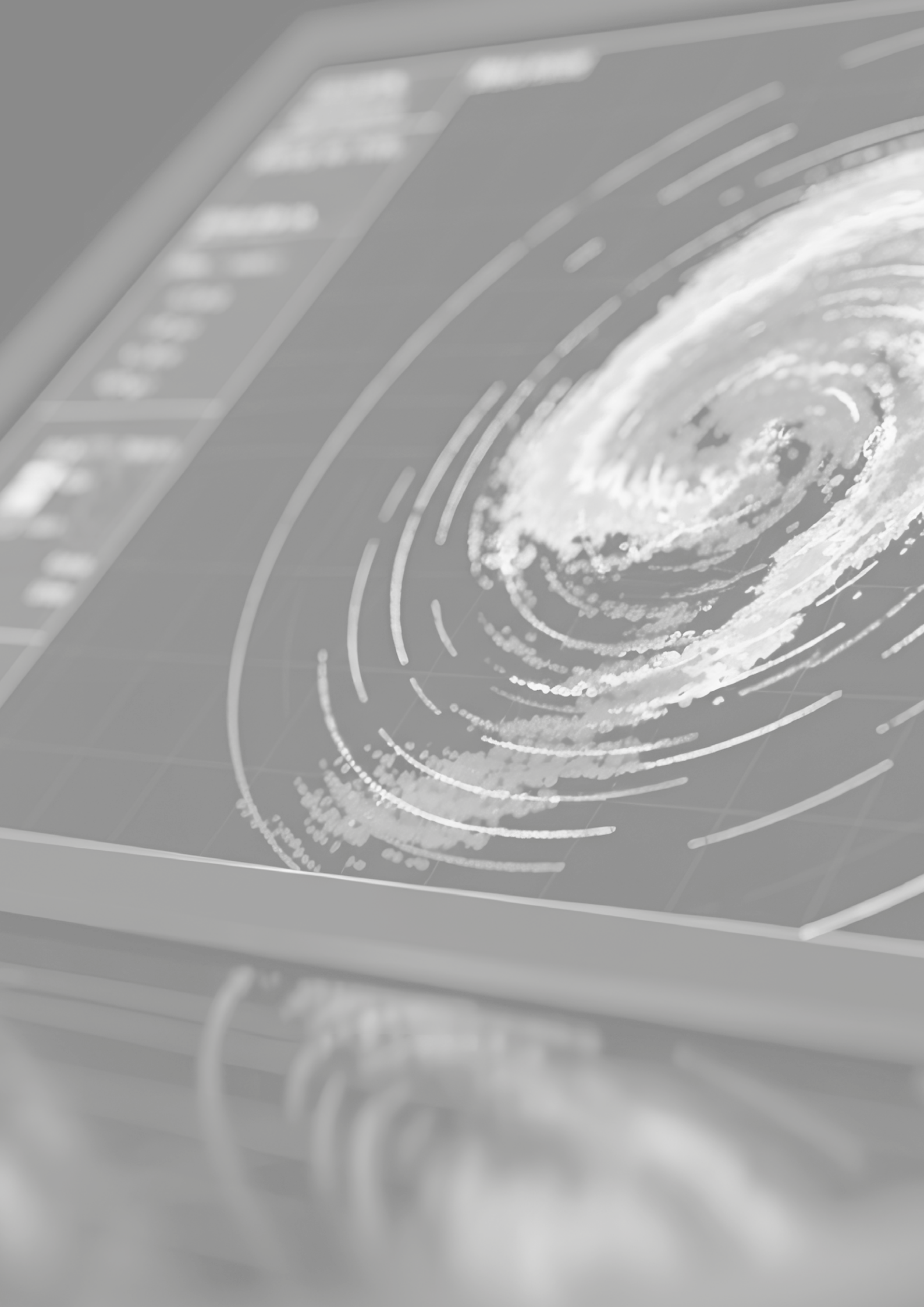
CIDADES INTELIGENTES 360

Caderno Técnico

Segurança

Secretaria de Desenvolvimento Econômico

SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS



CIDADES INTELIGENTES 360

Caderno Técnico

Segurança

Secretaria de Desenvolvimento Econômico

SÃO PAULO GOVERNO DO ESTADO SÃO PAULO SÃO TODOS

São Paulo, 2025

©Secretaria do Desenvolvimento Econômico
Av. Escola Politécnica, 82 –
Jaguaré
CEP05350-000
São Paulo SP
Telefone 55 (11) 3718-6500

© Instituto de Pesquisas Tecnológicas – IPT
Av. Professor Almeida Prado, 532 –
Cidade Universitária "Armando Salles Oliveira
CEP05508-901
São Paulo SP
Telefone 55 (11) 3767-4000
e-mail ipt@ipt.br
www.ipt.br

Cidades Inteligentes: Cadernos técnicos
Coordenadores
Maria Luiza Otero D'Almeida Lamardo – IPT (malu@ipt.br)
Caio Olmos Marinelli – SDE (comarinelli@sde.sp.gov.br)

Cidades Inteligentes: Caderno Técnico Segurança

Coordenador: Carlos Roberto Metzker de Oliveira (carlosmo@ipt.br)
Autores (ordem alfabética): Antonio Fernando Berto; Adriana Camargo de Brito; Douglas da Silva Santos; Guilherme Akyo Cremonesi; Ivan Faccinetto Botteger; Julio Cesar Sabadini de Souza; Luciana Alves de Oliveira; Luiz Fernando Batista da Silva; Marcelo Fscher Gramani; Marcelo de Mello Aquilino; Marcos Vinicius Martinez Sylverio; Ricardo Gomes de Freitas Nuno de B. Pereira; Oswaldo Sanches Junior.

Autores dos Anexos: (Maria Luiza Otero D Almeida Lamardo); B (Adriana Camargo Brito; Adriano Galindo Leal; Cristina Maria Ferreira da Silva; Denis Bruno Virissimo; Wagner Luiz Gava).

Apoio:
Edna Baptista dos Santos Gubitoso (bibliografias); Augusto Max Colin, Luiz Gustavo Pinto de Moraes Silviano e Rita de Cassia Parise (revisão do projeto gráfico e de imagens); Luciana Casciny Pacífico (Anexo A); Nereide de Oliveira (Anexo A)

Diagramação
Phábrica de Produções:
Alecsander Coelho, Daniela Bissiguini, Érsio Ribeiro, Kauê Rodrigues,
Paulo Ciola, Rebeca Tonello, Thiago Cordeiro

Capa
Freepik / Phábrica de Produções

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Cadernos técnicos cidades inteligente [livro eletrônico] : caderno técnico segurança / [coordenação Maria Luiza Otero D'Almeida Lamardo, Caio Olmos Marinelli, Carlos Roberto Metzker de Oliveira]. -- 1. ed. -- São Paulo : Instituto de Pesquisas Tecnológicas do Estado de São Paulo, 2025. -- (IPT Publicação ; 3076)

PDF
Vários autores.
Bibliografia.
ISBN: 978-65-5702-050-0

1. Cidades inteligentes 2. Criminalidade - Aspectos sociais 3. Desastres naturais - Prevenção 4. São Paulo (Cidade) - Governo e administração 5. Segurança pública 6. Tecnologia I. Lamardo, Maria Luiza Otero D'Almeida. II. Marinelli, Caio Olmos. III. Oliveira, Carlos Roberto Metzker de. IV. Série.

25-315823.0 CDD-307.76

Índices para catálogo sistemático:
1. Cidades inteligentes : Segurança pública : Sociologia urbana 307.76
Aline Graziele Benitez - Bibliotecária - CRB-1/3129

Apresentação

O processo de urbanização crescente tem remetido a questões que precisam ser contornadas para que seus sintomas não venham a interferir de modo negativo no funcionamento das cidades e na qualidade de vida dos cidadãos.

Hoje é necessário ter um olhar mais abrangente sobre as cidades, que devem ser funcionais em todos os seus aspectos, além de preparadas para reagir ou minimizar os efeitos de eventos adversos.

Um dos grandes desafios enfrentados pelos gestores municipais é o de tornar suas cidades inteligentes. Neste contexto, a Secretaria de Desenvolvimento Econômico do Estado de São Paulo, SDE, teve a iniciativa de, com o apoio do Instituto de Pesquisas Tecnológicas do Estado de São Paulo, IPT, elaborar cinco cadernos técnicos, em temas essenciais para uma cidade, abordando conceitos e pontos relevantes relacionados a cidades inteligentes. Os temas dos cadernos técnicos são os indicados a seguir.

- Caderno Técnico Governança e Planejamento Urbano
- Caderno Técnico Conectividade
- Caderno Técnico Mobilidade Urbana
- Caderno Técnico Serviços
- Caderno Técnico Segurança

Espera-se com esta iniciativa fornecer, para as prefeituras do Estado de São Paulo, um quadro diverso de conceito e soluções, que, embora não tratado de forma exaustiva, venha apoiar os gestores municipais na construção e execução de seus planejamentos, visando tornar seus respectivos municípios Cidades Inteligentes.

Sumário

1. Introdução 9
1.1 Cidades Inteligentes, Resilientes e Sustentáveis 10
1.2 Os Cadernos Técnicos 13
1.3 O Caderno Técnico Segurança 13

2. Segurança: conceitos 16

3. Segurança: gestão e resposta a desastres 19
3.1 Gestão de Riscos e Desastres 19
3.2 Orientação para Implementação de Gestão de Riscos e Desastres 21
3.3 Tecnologias para Gestão de Riscos e Desastres 22
3.4 Considerações Sobre Desastres Naturais 25

4. Segurança: detecção e resposta a incêndios 29
4.1 Barreiras Tecnológicas e Operacionais na Segurança Contra Incêndio 30
4.2 Detecção Inteligente de Incêndios 34
4.3 Resposta a Sinistros em Tempo Real 36
4.4 Base de Dados de Informações 38
4.5 Tecnologias para Detecção e Resposta a Incêndios 40
4.6 Sistemas Digitais para Segurança Contra Incêndio 44

5. Segurança pública 46
5.1 Sistemas Inteligentes de Vigilância por Vídeo 48
5.2 Câmeras Corporais (*Bodycams*) 56
5.3 Sistemas de Identificação Biométrica 60
5.4 Vigilância Baseada em Veículos Aéreos não Tripulados (Vants) 66
5.5 Ambientes Multissensoriais 71
5.6 Considerações sobre o uso de Tecnologia digitais 74

6. Segurança: Iluminação inteligente 77
6.1 Postes de Iluminação Inteligente com Sensores Integrados 80
6.2 Câmeras de Monitoramento Integradas à Iluminação 82
6.3 Iluminação Responsiva por Presença 84
6.4 Iluminação com Botão De Pânico Integrado 85
6.5 Inteligência Artificial (IA) Aplicada à Iluminação Pública 88
6.6 Postes Multiuso 91
6.7. Geolocalização e Mapeamento de Iluminação Deficitária 93
7. Pré-requisitos para soluções inteligentes 98
7.1 Perfil das Cidades 98
7.2 Infraestrutura atual no Estado de São Paulo 99
ANEXOS 102
ANEXO A - Documentos Legais e Normas Técnicas 103
ANEXO B - Inteligência Artificial: Conceitos e Desafios 111
ANEXO C - Indicadores para Cidades Inteligentes, Resilientes e Sustentáveis 119

1 Introdução

Cidades são ambientes complexos que trazem muitos desafios aos seus gestores, entre eles o de as tornarem sustentáveis, inteligentes e resilientes, conceitos que interagem entre si (Figura 1.1).

Figura 1.1 – Imagem de interação entre Cidades sustentáveis, inteligentes e resilientes

Fonte: Autores, 2025

Considerando como foco principal em uma cidade o cidadão, em toda sua totalidade, ou seja, como elemento demandante, como por exemplo de serviços de qualidade, e gerador, como por exemplo de resíduos, a tendência verificada no Brasil de migração do campo para as cidades (Tabela 1.1) torna os desafios ainda maiores para os gestores municipais, agravando questões que precisam ser contornadas para que seus sintomas não venham a interferir de modo negativo no funcionamento das cidades e na qualidade de vida dos cidadãos

Tabela 1.1 – Brasil 1960-2022 – População residente.

Censo	População em área urbana (milhões)	População em área rural (milhões)	População total (milhões)	População em área urbana (%)	População em área rural (%)
1960	32,0	39,0	71,0	45,1	54,9
1970	52,9	41,6	94,5	56,0	44,0
1980	82,0	39,1	121,1	67,7	32,3
1991	110,9	36,0	146,9	75,5	24,5
2000	137,8	31,8	169,6	81,3	18,8
2010	160,9	29,8	190,7	84,4	15,6
2022	177,5	25,6	203,1	87,4	12,6

Fonte: Censo IBGE (2010)[1] e Siqueira e Britto (2024)[2]

A tendência de migração do campo para as cidades não é apenas no Brasil, mas mundial. Segundo o relatório *World Population Prospects 2024*[3], das Nações Unidas, a população mundial que em 2024 atingiu 8,2 bilhões de pessoas deverá atingir 10,3 bilhões na década de 2080, e, então, permanecer ao redor desse valor. A migração do campo para a cidade também deverá ocorrer de forma relativamente significativa, chegando a 70% por volta de 2050[3,4].

Ao caminhar no sentido de tornar suas cidades inteligentes, resilientes e sustentáveis, os gestores municipais devem estar cientes de que não há soluções padronizadas e universais para tal e, tampouco, modelos prontos para replicarem. Frequentemente soluções existentes devem ser adaptadas.

Particularidades, especificidades e singularidades locais devem ser consideradas na elaboração do planejamento de cidades inteligentes, resilientes e sustentáveis. Deste modo, é importante:

- **planejar** (estabelecer objetivos e processos necessários para obter resultados de acordo com os propósitos da comunidade);
- **fazer** (implementar processos e alcançar metas);
- **acompanhar** (monitorar e medir processos frente à política, objetivos e compromissos da comunidade, e relatar os resultados);
- **corrigir** (tomar medidas necessárias para melhorar o desempenho).

Como o que não se mede, não se conhece, não se controla e não se melhora, é fundamental que cada gestor municipal defina os indicadores e métricas relevantes, que servirão como parâmetros de referência em sua cidade (ver Anexo C).

1.1 Cidades Inteligentes, Resilientes e Sustentáveis

Cidades Inteligentes

Muitas são as definições de cidades inteligentes, provavelmente pelo termo inteligente ser de certa forma vago e, assim, permitir várias interpretações. Há a questão de conferir à cidade a capacidade de sentir e reagir de maneira dinâmica a situações simples e complexas com auxílio de tecnologias e, principalmente, com infraestrutura para aquisição e processamento massivos de dados e há, também, a questão de criar condições sociais e institucionais melhores para o capital humano. É desejável que a abordagem a essas questões seja complementar.

A Carta Brasileira Cidades Inteligentes[5] traz a definição abaixo transcrita para cidades inteligentes:

> Cidades inteligentes são cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação.

A norma ABNT NBR ISO 37122 [6] traz no seu item 3.4 a definição abaixo transcrita para cidades inteligentes:

> Cidade que aumenta o ritmo em que proporciona resultados de sustentabilidade social, econômica e ambiental e que responde a desafios como mudanças climáticas, rápido crescimento populacional e instabilidade de ordem política e econômica, melhorando fundamentalmente a forma como engaja a sociedade, aplica métodos de liderança colaborativa, trabalha por meio de disciplinas e sistemas municipais e usa informações de dados e tecnologias modernas para fornecer melhores serviços e qualidade de vida para os que nela habitam (residentes, empresas e visitantes), agora e no futuro previsível, sem desvantagens injustas ou degradação do ambiente natural.

Cidades Resilientes

Cidades resilientes são aquelas que têm capacidade de se recuperar rapidamente de impactos causados por desastres, humanos ou naturais. Também têm capacidade de prever os impactos causados por esses desastres e de se antecipar a eles.

A norma ABNT NBR ISO 37123[7] traz no seu item 3.7 a definição abaixo transcrita para cidades resilientes:

> Cidade capaz de preparar-se, recuperar-se e adaptar-se aos choque e tensões.

Cidades Sustentáveis

Cidades sustentáveis são aquelas que adotam uma abordagem holística e não compartimentada, facilitando a cooperação de todas as partes interessadas em construir um sistema de gestão voltado para desenvolvimento sustentável.

O desafio do desenvolvimento sustentável é global, mas as estratégias para alcançá-lo nas cidades são locais e podem ser diferentes de cidade para cidade. Cada cidade deve respeitar seus *limites planetários* e considerar as limitações impostas por eles. A norma ABNT NBR ISO 37101[8] define, em sua introdução, o conceito de *limites planetários* como abaixo transcrito.

> O conceito de 'limites planetários' descreve um *framework* no qual a humanidade necessita viver, de forma a continuar a se desenvolver e prosperar para as próximas gerações. Mudanças climáticas, consumo de água, mudanças no uso do solo e perda da biodiversidade são exemplos de limites planetários. Ultrapassar estes limites pode gerar mudanças ambientais bruscas e irreversíveis, ao passo que respeitá-los reduz riscos significativamente. Limites planetários podem ser desagregados, de forma a selecionar medidas que podem ser atribuídas ao nível da comunidade, levando em conta uma situação específica.

Sustentabilidade e suas derivadas

O conceito de Sustentabilidade surgiu em 1987 com um relatório das Nações Unidas[9] que chamava a atenção para a importância de se ter um desenvolvimento sustentável, para garantir as necessidades do presente e também das gerações futuras. Ao longo dos anos, de modo incremental, ações foram surgindo, tendo em mente que o desenvolvimento sustentável deve ser dinâmico e atender o futuro e as necessidades presentes, conforme indica o relatório das Nações Unidas (Figura 1.2).

Figura 1.2 – Ações relacionada ao desenvolvimento sustentável

Fonte: Autor, 2025

Dentre as derivadas relacionadas ao desenvolvimento sustentável merece destaque a Agenda 2030 e a questão do Clima.

Agenda 2030

A Agenda 2030[10] é um plano global proposto pelas Nações Unidas em 2015 e adotado por seus países membros que tem como principal objetivo promover o desenvolvimento sustentável em suas dimensões econômica, social e ambiental até o ano de 2030. Ela é baseada em 17 Objetivos de Desenvolvimento Sustentável, que abordam questões sociais, econômicas e ambientais (Figura 1.3).

Figura 1.3 – Objetivos do desenvolvimento Sustentável (ODS)

Fonte: Nações Unidas Brasil , 2025 [10]

Clima (CPOs)

As Conferências das Partes (COPs) de países membros das Nações Unidas sobre Mudanças Climáticas, tem como objetivo maior conter o aquecimento da temperatura do planeta, por meio da estabilização das concentrações atmosféricas de gases de efeito estufa (GEE), limitando ou reduzindo suas emissões. Os gases de efeito estufa são: o dióxido de carbono (CO_2); o metano (CH_4); o oxido nitroso (N_2O), o ozônio (O_3) e os gases fluoretados.

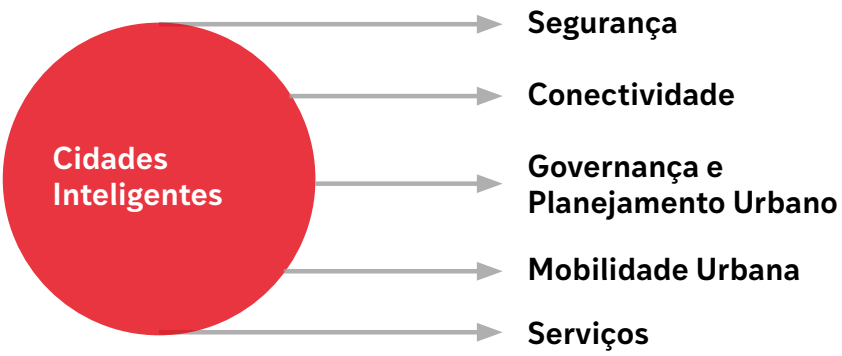
Entre os principais acordos sobre o clima estão o Protocolo de Kyoto[11], por propor metas de controle para os gases de efeito estufa e introduzir a possibilidade do carbono tornar-se uma moeda de troca e o Acordo de Paris [12], pelo compromisso de manter o aumento da temperatura média global bem abaixo de 2°C acima dos níveis pré-industriais e de buscar esforços para limitar aumento da temperatura a 1,5°C acima dos níveis pré-industriais. Tão importante quanto às questões climáticas é a preservação dos recursos naturais e da biodiversidade.

1.2 Os Cadernos Técnicos

Para apoiar os gestores municipais, cinco cadernos técnicos foram elaborados (Figura 1.4), tendo como foco principal cidades inteligentes, as quais possuem três qualidades[13]: a primeira é ser "instrumentada", com capacidade de capturar dados do mundo real de dispositivos pessoais, sensores e aparelhos; a segunda é ser "interconectada", capaz de transmitir os dados entre diferentes serviços da cidade; e a terceira é ser "inteligente", o que implica o uso de ferramentas analíticas para otimizar as atividades operacionais.

Embora o tema principal seja cidades inteligentes, os cadernos técnicos também abordam, ainda que de forma secundária, aspectos das cidades sustentáveis e resilientes

Figura 1.4 –Cadernos Técnicos



Fonte: Autores, 2025

Os cadernos técnicos não pretendem esgotar os temas tratados, mas apenas pontuar questões consideradas primordiais em cada tema. Espera-se que as informações neles contidas sirvam de apoio aos gestores municipais no processo de tornar suas cidades mais inteligentes.

1.3 O Caderno Técnico Segurança

As tendências tecnológicas que devem influenciar fortemente o setor de segurança urbana nos próximos anos incluem o uso crescente de inteligência artificial para análise preditiva, a popularização de sensores ambientais conectados e a atuação integrada de serviços de resposta emergencial por meio de plataformas digitais. Esses avanços levarão a cidades mais conectadas, resilientes e seguras. A consolidação de uma política pública baseada em inovação, integração e inteligência territorial é um passo essencial para transformar a segurança urbana em um serviço moderno, eficaz e acessível à população.

O Caderno Técnico Segurança apresenta possibilidades de modernização da segurança urbana a partir da integração de tecnologias aplicadas ao conceito de cidades inteligentes. Ao longo do documento, são descritas soluções digitais que, adaptadas à realidade local, podem ampliar significativamente a capacidade de prevenção, detecção e resposta a emergências.

A implantação das soluções digitais, no entanto, depende de requisitos fundamentais, como infraestrutura tecnológica mínima (energia elétrica e conectividade), equipes treinadas para operar e interpretar os dados gerados pelos sistemas, e um arcabouço legal que assegure o uso ético e seguro das informações.

O Caderno Técnico Segurança também destaca a importância de aproveitar estruturas e conceitos já existentes no Estado de São Paulo, como as redes de câmeras dos programas Muralha Paulista e Smart Sampa, as centrais de monitoramento em operação e os drones já utilizados por forças de segurança pública — ativos que podem ser aprimorados com o uso de novas tecnologias e pela integração entre órgãos da própria prefeitura.

O Caderno Técnico Segurança, está organizado nos seguintes tópicos:

- Conceitos de Segurança (capítulo 2);
- Gestão e Resposta a Desastres (capítulo 3);
- Detecção e Resposta a Incêndios (capítulo 4);
- Segurança Pública (capítulo 5);
- Iluminação Inteligente (capítulo 6);
- Implantação e infraestrutura (capítulo 7).

Além dos capítulos mencionados o Caderno Técnico Segurança traz três Anexos, que complementam as informações trazidas nos capítulos.

- Anexo A – Documentos legais e normas técnicas.
- Anexo B – Inteligência artificial: conceitos e desafios.
- Anexo C – Indicadores: cidades inteligentes, resilientes e sustentáveis.

Referências bibliográficas

1. IBGE. Sinopse do Censo Demográfico 2010. Rio de Janeiro: IBGE, 2010. Disponível em: https://censo2010.ibge.gov.br/sinopse/index.php?dados=8. Acesso em: 10 mar. 2025.

2. SIQUEIRA, B.; BRITTO, V. Censo 2022: 87% da população brasileira vive em áreas urbanas. Rio de Janeiro: IBGE, 2024. Disponível em: https://censo2010.ibge.gov.br/sinopse/index.php?dados=8. Acesso em: 10 mar. 2025

3. UNITED NATIONS. World Population Prospects 2024: Summary of Results. New York: United Nations, 2024. (UN DESA/POP/2024/TR/NO. 9)

4. NAÇÕES UNIDAS. ONU prevê que cidades abriguem 70% da população mundial até 2050. 2019. Disponível em: https://news.un.org/pt/story/2019/02/1660701. Acesso em: 11 fev. 2025.

5. MINISTÉRIO DO DESENVOLVIMENTO REGIONAL. Carta Brasileira Cidades Inteligentes. Disponível em: https://cartacidadesinteligentes.org.br/files/carta_brasileira_cidades_inteligentes.pdf. Acesso em: 03 mar. 2025.

6. ABNT. NBR ISO 37122:2020. Versão corrigida 2021. Cidades e comunidades sustentáveis. Indicadores para cidades inteligentes. Rio de Janeiro: ABNT, 2020. Disponível em: https://www.abntcatalogo.com.br/grd.aspx. Acesso em: 01 mar. 2025.

7. ABNT. NBR ISO 37123:2021: Cidades e comunidades sustentáveis. Indicadores para cidades resilientes. Disponível em: https://www.abntcatalogo.com.br/grd.aspx. Acesso em: 04 mar. 2025.

8. ABNT. NBR ISO 37101:2017. Versão corrigida 2021. Errata 1:2024: Desenvolvimento sustentável de comunidades - Sistema de gestão para desenvolvimento sustentável - Requisitos com orientações para uso. Rio de Janeiro: ABNT, 2021.

9. UNITED NATIONS. Our Common Future. Report of the World Commission on Environment and Development, From One Earth to One World. New York: United Nations, 1987. Disponível em: http://www.un-documents.net/ocf-ov.htm. Acesso em: 05 mar. 2025

10. NAÇÕES UNIDAS BRASIL. Como as Nações Unidas apoiam os Objetivos de Desenvolvimento Sustentável no Brasil. Disponível em: https://brasil.un.org/pt-br/sdgs. Acesso em: 05 mar. 2025.

11. Ministério do Meio Ambiente. Protocolo de Kyoto. Disponível em: https://antigo.mma.gov.br/clima/convencao-das-nacoes--unidas/protocolo-de-quioto.html . Acesso em 05 mar.2025

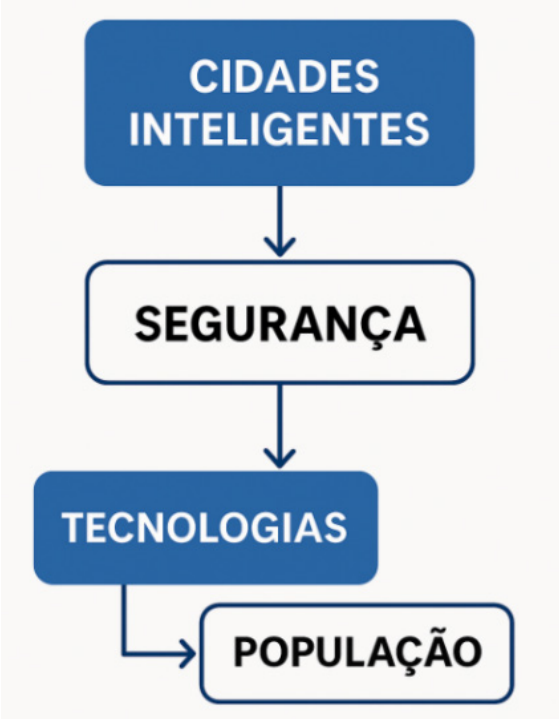
12. MINISTÉRIO DO MEIO AMBIENTE. Acordo de Paris. Disponível em; https://antigo.mma.gov.br/clima/convencao-das-nacoes-unidas/acordo-de-paris.html. Acesso em 05. mar. 2025

13. HARRISON, C.; ECKMAN, B.; HAMILTON, R.; HARTSWICK, P.; KALAGNANAM, J., PARASZCZAK, J., WILLIAMS, P. Foundations for smarter cities. IBM Journal of Research and Development, v. 54, 2010. https://doi.org/10.1147/JRD.2010.2048257.

2 Segurança: conceitos

Os municípios do estado de São Paulo enfrentam desafios crescentes devido à urbanização acelerada, à digitalização de serviços e as ameaças de criminalidade, desastres naturais, ataques cibernéticos e falhas operacionais. Este caderno oferece diretrizes práticas para prefeitos, gestores públicos e equipes técnicas, orientando a implantação e implementação de soluções de segurança em cidades inteligentes. O objetivo é promover ambientes urbanos resilientes, sustentáveis e focados no bem-estar da população, integrando segurança física, digital e operacional por meio de tecnologias avançadas. A Figura 2.1 apresenta o organograma da integração desses conceitos.

Figura 2.1 – Organograma das dimensões da segurança em cidades inteligentes e sua integração com tecnologias e participação cidadã.



Fonte: Imagem gerada por Chatgpt em 18/04/2025).

Cidades inteligentes utilizam tecnologias de informação e comunicação (TICs) para coletar e analisar dados em tempo real, otimizando a gestão urbana e elevando a qualidade de vida. Segundo Halegoua[1], elas integram sensores, inteligência artificial (IA) e sistemas interconectados para antecipar incidentes e coordenar

respostas rápidas. Ferramentas como vide monitoramento inteligente, sensores de presença, iluminação pública conectada e centros de controle permitem detectar ameaças precocemente. Por exemplo, câmeras com análise comportamental identificam riscos em espaços públicos, enquanto sensores ambientais alertam sobre inundações ou incêndios, protegendo vidas e reduzindo danos.

A segurança física é a base da proteção urbana, abrangendo a salvaguarda contra crimes, vandalismo, acidentes e desastres. Tecnologias como controle de acesso biométrico e iluminação inteligente, que ajusta a intensidade conforme a presença de pessoas, aumentam a segurança e otimizam o consumo energético. Contudo, com a crescente conectividade, a cibersegurança é indispensável. Sistemas urbanos dependem de redes digitais que, se comprometidos, podem paralisar serviços essenciais, como transporte e saúde. O relatório da UN-Habitat de 2022[2] destaca que cidades inteligentes devem adotar criptografia, autenticação multifator e monitoramento contínuo para proteger dados e infraestruturas. Nos municípios paulistas, capacitar servidores e implementar protocolos robustos de cibersegurança é uma prioridade. Portanto este é um eixo importante a ser considerado na aplicação de tecnologias em cidades inteligentes, mas não será abordado diretamente neste caderno.

A segurança operacional garante a continuidade dos serviços diante de falhas técnicas ou eventos inesperados. Manutenção preventiva, redundância de sistemas e planos de contingência evitam interrupções. Em blecautes, por exemplo, sistemas de backup mantêm semáforos inteligentes e hospitais funcionando. A integração dessas dimensões — física, digital e operacional — é essencial. Kitchin[3] argumenta que a resiliência urbana depende da articulação entre tecnologias, governança e participação cidadã, criando sistemas que antecipam crises.

A participação popular é crucial. Cidades inteligentes seguras são participativas, promovendo corresponsabilidade por meio de canais digitais, como aplicativos de denúncia, e campanhas de conscientização. Em São Paulo, iniciativas como o Geosampa, que disponibiliza dados urbanos para monitoramento e planejamento, exemplificam o uso de tecnologia para engajar a sociedade[4]. Engajar cidadãos fortalece a confiança no poder público e fomenta uma cultura de prevenção.

Este caderno organiza suas diretrizes em quatro eixos: **Gestão e Resposta a Desastres, Iluminação Inteligente para Segurança, Detecção e Prevenção de Incêndios e Segurança Pública**. Cada eixo é detalhado oferecendo um guia para os gestores paulistas. Com foco nas particularidades dos municípios, de metrópoles a pequenas cidades, o documento apresenta soluções escaláveis, sendo um desafio crítico devido à sua complexidade e impactos. A Figura 2.2 apresenta visualmente esses eixos.

Figura 2.2 – Eixos do Caderno de Segurança

Fonte: Imagem gerada por Chatgpt em 18/04/2025.

Cidades inteligentes representam um pilar fundamental para garantir a proteção de vidas, patrimônios e o meio ambiente, utilizando tecnologias avançadas e sistemas digitais interconectados. Segundo Halegoua[1], as cidades inteligentes integram tecnologias de informação e comunicação (TICs) para coletar e analisar dados em tempo real, funcionando como sistemas preditivos de alerta e resposta. A inteligência artificial (IA) desempenha um papel central nesse cenário, permitindo a análise de grandes volumes de dados e promovendo o engajamento do cidadão na construção de cidades resilientes[5].

Ao adotar essas estratégias, os municípios paulistas poderão construir cidades mais seguras e preparadas para o futuro. Este caderno incentiva investimentos em tecnologias inteligentes, capacitação de equipes e parcerias com a sociedade, priorizando a proteção, a resiliência urbana e o bem-estar da população.

Referências bibliográficas

14. HALEGOUA, G. R. **Smart cities.** Cambridge, Massachusetts: MIT Press, 2020.

15. UN-Habitat. **World cities report 2022**: Envisaging the future of cities. Nairobi: United Nations Human Settlements Programme, 2022. https://digitallibrary.un.org/record/3984713?v=pdf. Acesso em: 18 abr. 2025.

16. KITCHIN, R. **The data revolution**: Big data, open data, data infrastructures and their consequences. London: SAGE Publications, 2014. https://methods.sagepub.com/book/mono/the-data-revolution/toc. Acesso em: 18 abr. 2025.

17. SÃO PAULO (Cidade). **Geosampa**: Portal de mapas e informações da cidade, 2024. http://geosampa.prefeitura.sp.gov.br/. Acesso em: 18 abr. 2025.

18. KARRI, C.; MACHADO, J. J. M.; TAVARES, J. M. R. S.; JAIN, D. K.; DANNANA, S.; GOTTAPU, S. K.; GANDOMI, A. H. Recent technology advancements in smart city management: a review. **Computers, Materials & Continua**, v. 81, n. 3, p. 3617–3663, 2024. https://doi.org/10.32604/cmc.2024.058461.

19. Segurança: GESTÃO E RESPOSTA A DESASTRES

3 Segurança: gestão e resposta a desastres

A prevenção e proteção aos desastres naturais são essenciais para a segurança e resiliência das cidades inteligentes, especialmente em um contexto de mudanças climáticas e urbanização acelerada. Tecnologias como sensores IoT, sistemas de informações geográficas (SIG), radares meteorológicos, gêmeos digitais e sistemas de emissão de alertas permitem antecipar riscos, mitigar impactos e coordenar respostas eficazes.

3.1 Gestão de Riscos e Desastres

A Gestão de Riscos e Desastres pode ser definida como um processo permanente e contínuo que visa enfrentar os riscos presentes em um determinado local, ou seja, trata-se de ações que antecipem e reduzam a possibilidade de perdas e danos ou amenizem suas consequências[1].

A lei nº 12.608/12[2], que instituiu a Política Nacional de Proteção e Defesa Civil – PNPDEC, estabelece as ações de prevenção, mitigação, preparação, repostas e recuperação.

Figura 3.1 – Organização das ações segundo a Política Nacional de Proteção e Defesa Civil.

Fonte: PNPDEC[3].

Conhecendo os Riscos

Para se estar bem-preparado para a ocorrência de desastres é necessário, primeiramente, conhecer os riscos existentes em uma determinada localidade. A partir do mapeamento de riscos um gestor público terá condições de saber:

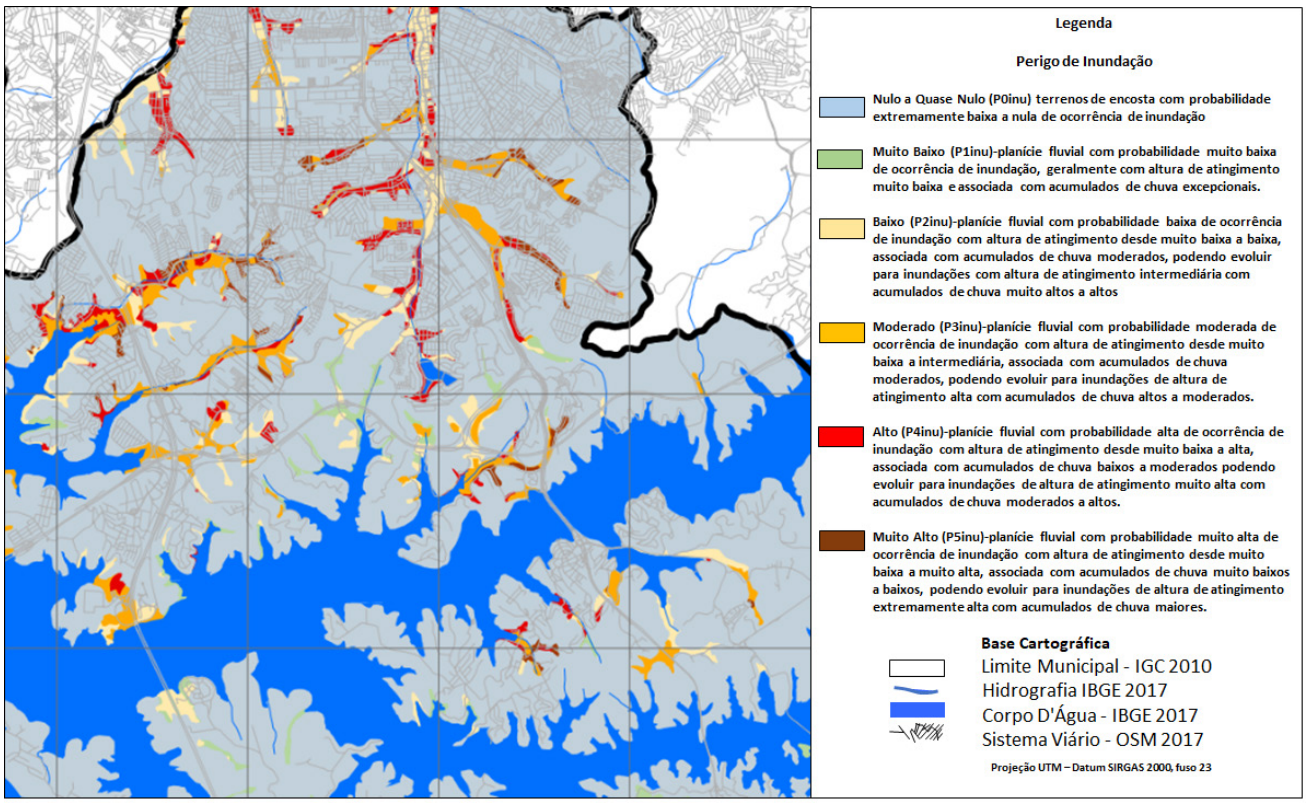
- A susceptibilidade de uma região à ocorrência de processos físicos (como uma inundação) que possam representar ameaças;
- As possibilidades de realizar uma ocupação urbana de forma segura em um determinado terreno;
- A determinação dos graus de riscos dos territórios. A PNPDEC -Política Nacional de Proteção e Defesa Civil (Lei n° 12.608/2012[2]) instrui sobre a necessidade desses mapeamentos, sob responsabilidade dos municípios.

O processo de mapeamento de riscos deve considerar, pelo menos, os seguintes elementos:

- Dados históricos, levantar os registros de desastres de uma localidade e seus pontos mais afetados;
- Reconhecimento das ameaças, reconhecer os riscos de um local é necessário para determinar as formas de monitoramento adequadas;
- Representação gráfica, apresentação espacial de forma facilitada das áreas de risco.

O mapeamento de riscos envolve a realização de análises por sensoriamento remoto e inspeções locais, que resulta na elaboração de cartas gráficas e deve contar sempre com a participação de técnicos da administração municipal e agentes da Defesa Civil[3] (ver Figura 3.2).

Figura 3.2 – Carta de perigo de inundações do município de São Bernardo do Campo[4]



Prevendo os Desastres

Ferramentas que sejam capazes de prever os desastres são de extrema importância para o gestor público, pois possibilitam o direcionamento das ações que devem ser tomadas para reduzir os riscos e mitigar os danos causados à população, meio ambiente e infraestrutura.

No Brasil, o Centro Nacional de Monitoramento e Alertas de Desastres Naturais do Ministérios da Ciência, Tecnologia e Inovações (CEMADEN/MCTI) desenvolveu o GeoRisk, um sistema que oferece previsões de risco de deslizamento de terras para diferentes regiões a partir da combinação de modelos meteorológicos, dados ambientais e uma base de dados de desastres.

Uma solução para previsão automatizada de ocorrência de inundações em áreas urbanas foi proposta por Barcelos[5].

Outra ferramenta que vem sem empregada é a de gêmeos digitais (*Digital Twins* em inglês): representações virtuais do mundo real, criadas para simular, monitorar e prever seu comportamento em diversas condições. Diversos estudos vendo sendo realizados na construção de modelos voltados para o gerenciamento de desastres, envolvendo terremotos[6,7], incêndios e vendavais[7].

Mitigando os Desastres

Mapear as áreas de risco e realizar simulações para prever e se preparar não terão efeito se não for realizado um monitoramento permanente das áreas de risco. O monitoramento permite ao gestor público receber, avaliar e responder à uma situação de risco e coordenar equipes de resgate na ocorrência de desastres.

Floriano e colegas[8] desenvolveram um sistema online para realizar o monitoramento de alagamentos a partir da informação dos níveis de corpos d'água. Já Fortes e colegas[9] desenvolveram um programa de monitoramento de encostas na BR-116.

O Governo do Estado de São Paulo conta com a Plataforma de Gestão de Riscos de Desastres Naturais, para situações que dependem de informações geológicas, e que faz parte do programa São Paulo Sempre Alerta.

Uma vez que se detecta a possibilidade de ocorrer um desastre, por exemplo, grande volume de chuva em um curto espaço de tempo, os órgãos públicos devem emitir alertas para que a população possa se proteger.

A Portaria Nº 3.027, de 4 de dezembro de 2020, define procedimentos para o envio de alertas à população sobre a possibilidade de ocorrência de desastres, em articulação com os órgãos e entidades estaduais, distritais e municipais de proteção e defesa civil, e para utilização do sistema Interface de Divulgação de Alertas Públicos para envio de alertas via mensagem de texto (SMS), televisão por assinatura ou plataforma de avisos públicos.

Os alertas devem ser emitidos em tempo hábil para que a população possa agir preventivamente e mitigar os riscos de desastres. Idealmente, ele deve atingir toda população que esteja no local de risco e para isso existem diversas formas de se propagar essa informação como, torres de alertas em regiões críticas, mensagens de alerta em celulares, mensagens de alertas em emissoras de rádio e televisão.

3.2 Orientação para Implementação de Gestão de Riscos e Desastres

A gestão de desastres envolve um ciclo contínuo de ações para antecipar e mitigar riscos com ênfase nos seguintes componentes:

- **Mapeamento de riscos:** elaborar Carta de Suscetibilidade, Carta Geotécnica de Aptidão à Urbanização e Carta de Risco, para embasar o planejamento urbano.
- **Simulações**: Usar gêmeos digitais para testar cenários de desastres e planejar respostas;
- **Monitoramento em tempo real:** utilizar redes de sensores conectados para detectar mudanças ambientais (por exemplo, níveis de rios, chuvas intensas) alimentando sistemas preditivos, como o GeoRisk do CEMADEN/MCTI (Centro Nacional de Monitoramento e Alertas de Desastres Naturais / Ministérios da Ciência, Tecnologia e Inovações);
- **Sistemas inteligentes de evacuação:** desenvolver rotas de fuga baseadas em dados em tempo real para orientar a população em áreas de risco, como encostas ou zonas inundáveis;
- **Sistemas de alerta em tempo real:** implementar plataformas que disseminem alertas rápidos via SMS (como o Defesa Civil Alerta), aplicativos e sirenes, garantindo que a população receba orientações preventivas.

Desastres naturais, como o causado pelas chuvas em 2023 no litoral norte do estado de São Paulo, causam perdas humanas, danos à infraestrutura e prejuízos econômicos. A gestão proativa é essencial para:

- Reduzir a vulnerabilidade de comunidades em áreas de risco, como encostas e margens de rios;
- Proteger infraestruturas críticas, como hospitais e vias de acesso;
- Alinhar municípios aos princípios de cidades inteligentes, promovendo resiliência e segurança.

A gestão de desastres requer colaboração entre:

- Gestores públicos, que coordenam a implementação de tecnologias e a articulação com a Defesa Civil;
- Equipes técnicas, envolve defesas civis estadual/federal, instituto públicos de pesquisa, como IPA (Instituto de Pesquisas Ambientais), IPT (Instituto de Pesquisas Tecnológicas do Estado de São Paulo) e Serviço Geológico do Brasil;
- População, que participa da realização de treinamentos e exercícios simulados de preparação para desastres.

As ações devem priorizar áreas de alto risco no estado, incluindo:

- Municípios costeiros, áreas de encosta e próximas a corpos d'água (por exemplo, represas, rios);
- Regiões metropolitanas e áreas de adensamento populacional;
- Rodovias críticas, com grande deslocamento populacional e de cargas.

A gestão de desastres deve ser contínua, com etapas específicas:

- **Pré-desastre**: de caráter preventivo**,** envolve mapeamento de riscos, instalação de sensores e sirenes;
- **Durante eventos**: monitoramento em tempo real, emissão de alertas e ativação de sistemas de evacuação durante temporais;
- **Pós-desastre:** recuperação, análise de impactos e atualização de modelos preditivos.

3.3 Tecnologias para Gestão de Riscos e Desastres

A seguir são apresentadas as diversas tecnologias que podem ser empregadas para gestão de riscos e desastres.

Sensores IoT

Sensores IoT são essenciais para um monitoramento constante das condições de locais críticos, como regiões próximas a encostas, corpos d'água e florestas com históricos de queimadas, possibilitando se antecipar a situações de risco com emissão de alertas, evacuação da população e preparo de equipes de resgate. Eles podem ser utilizados sozinhos ou em conjunto para medir os atributos de interesse, por exemplo:

- Piezômetro - detecção de pressão de água no solo;
- Inclinômetro - movimentações laterais e deformações de solo;
- Extensômetro - mudanças de tensão no solo;
- Acelerômetros – medição de vibrações e movimentos do solo;
- Pluviômetro - quantidade de chuva;
- Boias: medição de níveis de corpos d'água, como rios, lagos e represas;
- Detectores de fumaças;
- Anemômetros: velocidade e direção do vento.

Esses sensores precisam estar aptos a enviar e receber dados confiáveis e de forma ininterrupta para centrais de monitoramento das defesas civil estaduais/municipais, corpos de bombeiros e outras agências que possam agir em emergências. Isso significa que as fontes de energia devem garantir autonomia para operacionalização dos equipamentos, a transmissão de dados deve atingir todos os equipamentos e garantir redundância para evitar a perda de sinal (Tabela 3.1).

Tabela 3.1 – Características técnicas para os diversos tipos de sensores[10].

Fontes de energia	Baterias	Energia solar	Baterias combinadas com energia solar
Transmissão de dados	Ondas de rádio (ZigBee, wi-fi, Bluetooth, LoRa/LoRaWan)	Rede de celular (GSM, 4G, 5G)	Cabo
Topologia de rede	Estrela	Árvore	Mesh

Câmeras de Monitoramento

Câmeras de alta resolução para monitoramento automático de regiões críticas, integradas com sistemas de inteligência artificial para detecção automática de eventos e disparos de alarmes (níveis de corpos d'água, chuvas em aproximação, ocorrência de alagamentos em locais de grande movimentação de pessoas/veículos).

Radares e Satélites Meteorológicos

As informações coletadas por essas ferramentas permitem prever e antecipar a ocorrência de temporais, vendavais, granizos para tomadas de decisão por parte das autoridades.

Visando melhorar sua capacidade de previsão meteorológica, o Estado de São Paulo implantou o Centro Paulista de Radares e Alertas Meteorológicos (CePRAM), que permite maior capacidade técnica na emissão de boletins meteorológicos e alertas de chuvas e temporais mais precisos.

Sistemas de Informações Geográficas (SIG)

As informações coletadas em campo, pelos sensores, satélites e drones são integradas em softwares SIG (como os softwares livres QGIS e gvSIG) permitindo a elaboração de Carta de Suscetibilidade, Carta Geotécnica de Aptidão à Urbanização e Carta de Risco. A partir dessas cartas é possível fazer o planejamento da ocupação do solo. O mapeamento também permite a realização de modelagens geotécnicas para simular e prever o comportamento de áreas críticas e estipular as condições e limites de ocupação do solo de forma segura.

Uso de Veículos Aéreos não Tripulados (VANT)

Os VANT, popularmente chamados de drones, são equipamentos com capacidade de chegar em áreas de difícil acesso e cobrir uma grande área em curto espaço de tempo. Eles podem ser equipados com diversos tipos de sensores e câmeras, e auxiliar no monitoramento áreas atingidas por desastres permitindo e facilitando a coordenação das equipes de resgate e auxiliando na busca por vítimas[11,12]. Também pode ser utilizado para transportar cargas e funcionar como antenas para transmissão/repetição de sinal de internet/celular[12,13].

Os drones também vem sendo utilizados no combate a incêndios florestais no gerenciamento, monitoramento e detecção de focos de incêndio[14,15,16] e no seu combate[17,18].

Gêmeos Digitais

O uso de gêmeos digitais (*digital twins*) permite a criação de cenários virtuais realistas, baseados no mundo real, que possibilitam a realização de simulações seguras para previsão de danos causados por desastres e testar diferentes cenários de forma eficiente[19]. O advento das tecnologias envolvidas nas Cidades Inteligentes possibilita a aquisição de diversas informações, em tempo real, das condições da cidade, que alimentam os modelos de gêmeos digitais[20]. Essas informações podem ser geradas por drones/satélites (como mapeamento de áreas construídas ou naturais), sensores IoT, câmeras de vigilância/monitoramento, deslocamento populacional (dados de celulares); introduzidas em plataformas do tipo SIG e BIM; e analisadas usando redes neurais e inteligência artificial. A Tabela 3.2 apresenta alguns países que utilizam essa tecnologia.

Singapura desenvolveu um projeto de mapeamento virtual (*Virtual Singapore*) completo do país utilizando imagens aéreas e terrestres que pode ser usado pelo governo, indústria e universidades[21].

Diversas cidades no mundo vêm empregando estas ferramentas para o gerenciamento de desastres[19,22,23,24].

Tabela 1.2 – Exemplos de países que empregaram gêmeos digitais para gerenciamento de desastres.

Desastre/Tema	Local	Caso
Terremoto	Estados Unidos	Restauração pós-terremoto em Missouri, usando simulação baseada em eventos
Terremoto	China	Simulações de edifícios em Shangai e Pequim para verificar sua vulnerabilidade a terremotos
Incêndios	China	Simulação de incêndios em vilarejos após ocorrência de terremotos

EMISSÃO DE ALERTAS

A Portaria Nº 3.027, de 4 de dezembro de 2020 (Anexo A, Tabela A.1.1), define procedimentos para o envio de alertas à população sobre a possibilidade de ocorrência de desastres, em articulação com os órgãos e entidades estaduais, distritais e municipais de proteção e defesa civil, e para utilização do sistema Interface de Divulgação de Alertas Públicos para envio de alertas via mensagem de texto (SMS), televisão por assinatura ou plataforma de avisos públicos.

Os alertas devem ser emitidos em tempo hábil para que a população possa agir preventivamente e mitigar os riscos de desastres. Idealmente, ele deve atingir toda população que esteja no local de risco e para isso existem diversas formas de se propagar essa informação como, torres de alertas em regiões críticas, mensagens de alerta em celulares, mensagens de alertas em emissoras de rádio e televisão. No Estado de São Paulo existem algumas soluções já empregas pela Defesa Civil:

- **Defesa Civil Alerta**: sistema de envio de mensagens que utiliza a tecnologia de transmissão via telefonia celular é complementar às outras ferramentas de alertas de emergência disponíveis para prevenção e mitigação dos impactos causados por desastres, avisando e orientando as pessoas que estejam em localidades com risco iminente de alagamentos, enxurradas, deslizamentos de terra, vendavais, chuvas de granizo, dentre outros;
- **São Paulo Sempre Alerta:** Sistema de informação por SMS da Defesa Civil do Estado (40199), em que a população pode cadastrar o CEP de interesse e receber informações específicas do local. Também conta com canal público no *Whatsapp* para divulgação de informações;
- **Alertas em APP:** os aplicativos de celular são ótimas ferramentas para encaminhar alertas para a população (como alertas meteorológicos, níveis de rios, riscos de deslizamentos), bem como ser uma plataforma para população realizar a notificação de ocorrências de algum local/comunidade. No Estado de São Paulo a Defesa Civil encaminha alertas em alguns aplicativos utilizados por motoristas e entregadores, como Waze, iFood e 99[25].

A cidade de Blumenau, SC, conta com um aplicativo/sistema[26]; Niterói, RJ, conta com o aplicativo Alerta DCNit[27]. O Serviço Geológico do Brasil mantém o aplicativo Prevenção SGB, com indicações de riscos ao nível nacional[28].

- **Sirenes:** as sirenes são instaladas em locais de risco conhecidos sendo capazes de emitir alertas e alarmes. Seu acionamento pode ser feito à distância ou manualmente, por um agente da Defesa Civil ou alguma liderança local devidamente treinada. Um alerta é uma mensagem que prepara a população local para uma situação de perigo previsível. Já o alarme informa sobre a necessidade de evacuação do local e deslocamento para lugares seguros. No Estado de São Paulo, existem sirenes instaladas nos morros de cidades como São Sebastião[29], Guarujá[30] e Franco da Rocha[31] para aviso da população em casos de risco de deslizamentos.

3.4 Considerações sobre desastres naturais

A gestão de desastres naturais no contexto das cidades inteligentes, especialmente no estado de São Paulo, representa um desafio multidimensional que exige a integração de tecnologias avançadas, planejamento estratégico e colaboração intersetorial para promover resiliência urbana frente às mudanças climáticas e à urbanização acelerada[1].

Tecnologias como sensores IoT, sistemas de informações geográficas (GIS), gêmeos digitais, drones, câmeras de monitoramento e sistemas de alerta em tempo real têm se mostrado essenciais para antecipar, mitigar e responder a eventos como inundações, deslizamentos, vendavais e incêndios florestais[10,19].

Iniciativas locais, como o Centro Paulista de Radares e Alertas Meteorológicos (CePRAM) e o sistema São Paulo Sempre Alerta, demonstram o impacto dessas soluções na redução de vulnerabilidades e na proteção de vidas e infraestruturas críticas[5].

A Política Nacional de Proteção e Defesa Civil, PNPDEC, instituída pela Lei nº 12.608 de 2012[2] (Anexo A, Tabela A.1.1) reforça a responsabilidade municipal no mapeamento de riscos e na execução de ações contínuas de prevenção, mitigação, preparação, resposta e recuperação[1]. A metodologia 5W2H oferece um guia prático para estruturar essas iniciativas, apoiando a elaboração de cartas de susceptibilidade, como a de inundações de São Bernardo do Campo (Instituto Geológico, 2020), e a implantação de sistemas inteligentes de evacuação baseados em dados em tempo real integrados a GIS e gêmeos digitais[19]. O uso de gêmeos digitais, a exemplo do projeto Virtual Singapore, permite simular cenários de desastres, otimizando rotas de evacuação e estratégias de resposta, reduzindo custos e aumentando a eficiência[20,21].

O monitoramento contínuo, suportado por sensores como pluviômetros, piezômetros e boias, é crucial para antecipar riscos, enquanto sistemas de alerta via SMS, aplicativos como Prevenção SGB e sirenes em cidades como São Sebastião, Guarujá e Franco da Rocha garantem a disseminação rápida de informações à população[10,32]. Estudos como os de Floriano e colegas[8] e Fortes e colegas[9] destacam a eficácia de sistemas de monitoramento de alagamentos e encostas, respectivamente, enquanto o GeoRisk do CEMADEN (Centro Nacional de Monitoramento e Alertas de Desastres Naturais) exemplifica o potencial de modelos preditivos na gestão de riscos[5]. A integração de dados de drones e satélites em plataformas de informações geográficas fortalece o planejamento urbano seguro, como demonstrado em mapeamentos de áreas críticas[21].

O sucesso dessas estratégias, no entanto, depende de fatores como a capacitação contínua de agentes da Defesa Civil (Noções Básicas em Proteção e Defesa Civil, 2017), o engajamento comunitário por meio de aplicativos colaborativos[1], e parcerias com instituições como o CEMADEN[33] (Centro Nacional de Monitoramento e Alertas de Desastres Naturais) e universidades para o desenvolvimento de modelos preditivos[5]. A escalabilidade de tecnologias, como sensores alimentados por energia solar e redes LoRa, combinada com o financiamento federal previsto na PNPDEC, viabiliza a implantação em larga escala, especialmente em municípios com recursos limitados[1,10].

Em síntese, a adoção de tecnologias de cidades inteligentes na gestão de desastres alinha São Paulo aos padrões globais de resiliência urbana, como observado no caso de Singapura[20]. Ao integrar dados em tempo real, inteligência artificial e participação cidadã, o estado pode mitigar os impactos de desastres naturais, proteger infraestruturas críticas e fortalecer a confiança na gestão pública, promovendo cidades mais seguras, sustentáveis e preparadas para os desafios futuros [19,20].

Referências Bibliográficas

1. SULAIMAN, S. N.; NOGUEIRA, F. R.; CARVALHO, C. S.; COUTINHO, S. M. V.; LEITE, M. A. B.; MOURA, R. B. Perspectivas sobre a gestão de riscos e desastres. *In:* **GIRD+10:** caderno técnico de gestão integrada de riscos e desastres. 1 ed. Brasília, DF: Ministério do Desenvolvimento Regional: Secretaria Nacional de Proteção e Defesa Civil, 2021.

2. BRASIL. Lei nº 12.608, de 10 de abril de 2012. Institui a Política Nacional de Proteção e Defesa Civil - PNPDEC; dispõe sobre o Sistema Nacional de Proteção e Defesa Civil - SINPDEC e o Conselho Nacional de Proteção e Defesa Civil - CONPDEC; autoriza a criação de sistema de informações e monitoramento de desastres; altera as Leis nºs 12.340, de 1º de dezembro de 2010, 10.257, de 10 de julho de 2001, 6.766, de 19 de dezembro de 1979, 8.239, de 4 de outubro de 1991, e 9.394, de 20 de dezembro de 1996; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 11 abr. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12608.htm. Acesso em:23 abr. 2025.

3. MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL. **Consulta geral nas publicações, 2017.** Disponível em: https://www.gov.br/mdr/pt-br/centrais-de-conteudo/publicacoes/protecao-e-defesa-civil-sedec. Acesso em:3 mar. 2025.

4. INSTITUTO GEOLÓGICO. **Carta de perigo de inundações do município de São Bernardo do Campo.** São Paulo: Instituto Geológico, 2020.

5. BARCELOS, D. V. **Desenvolvimento de um modelo de data science para prevenção de enchentes**. 2023. 64 f. Dissertação (Mestrado) - Programa de Pós-Graduação em Gestão de Organizações Públicas, Universidade Federal de Santa Maria, Santa Maria, 2023.

6. LU, X.; LU, X.; GUAN, H.; XIE, L. **Application of earthquake-induced collapse analysis in design optimization of a super-tall building: Collapse analysis in design optimization of a supertall building.** The Structural Design of Tall and Special Buildings, v. 25, p. 926–946, 2016. https://doi.org/10.1002/tal.1291.

7. LU, X.; GU, D.; XU, Z.; XIONG, C.; TIAN, Y. CIM-**Powered Multi-Hazard Simulation Framework Covering both Individual Buildings and Urban Areas**. Sustainability**,** v. 12, n. 12, art. 5059, 2020. https://doi.org/10.3390/su12125059.

8. FLORIANO, D.; SCOZ, D.; MELO, D.; SEVEGNANI, J.; SANTOS, F. SIGMAOn –**Sistema de Informação Geográfica para Monitoramento de Alagamentos On-line**. *In*: WORKSHOP DE COMPUTAÇÃO APLICADA À GESTÃO DO MEIO AMBIENTE E RECURSOS NATURAIS (WCAMA), 5., 2014, Brasília. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2014. p. 63-72. https://sol.sbc.org.br/index.php/wcama/article/view/10913

9. FORTES, R. M.; UDDIN, W.; RESSUTTE, A. F. B.; FARIA, V. C.; KLINSKY, L. M. G. **Estudo de implantação de um programa de monitoramento de encostas na BR-116**. *In:* CONGRESSO BRASILEIRO DE RODOVIAS & CONCESSÕES, 9., 2015, Brasília. **Anais** [...]. São Paulo: ABCR, 2015. Disponível em: https://pt.slideshare.net/slideshow/estudo-de-implantao-de-um-programa-de-monitoramento-de-encostas-na-br-116/53942623. Acesso em: 3 mar. 2025.

10. MENDROT FILHO, A. S.; STRINGHINI, D. **Redes de sensores sem fio para monitoramento e detecção de deslizamentos de terra**. In: CONFERÊNCIA IBERO-AMERICANA, 2019. Atas [...]. [S.l.]: Single, 2019. p. 309–313. https://www.iadisportal.org/digital-library/redes-de-sensores-sem-fio-para-monitoramento-e-detec%C3%A7%C3%A3o-de-deslizamentos-de--terra-uma-revis%C3%A3o-sistem%C3%A1tica. Acesso em: 3 mar. 2025**.**

11. DEMIANE, F.; SHARAFEDDINE, S.; FARHAT, O. An optimized UAV trajectory planning for localization in disaster scenarios. **Computer Networks**, v. 179, art. 107378, 2020. https://doi.org/10.1016/j.comnet.2020.107378.

12. ZHOU, Z.; TANG, J.; FENG, W.; ZHAO, N.; YANG, Z.; WONG, K.-K. Optimized Routing Protocol Through Exploitation of Trajectory Knowledge for UAV Swarms. **IEEE Transactions on Vehicular Technology,** v. 73, p. 15499–15512, Oct. 2024. https://doi.org/10.1109/TVT.2024.340573.

13. WU, Q.; ZENG, Y.; ZHANG, R. Joint Trajectory and Communication Design for Multi-UAV Enabled Wireless Networks. **IEEE Transactions on Wireless Communications,** v. 17, p. 2109–2121, 2018. https://doi.org/10.1109/TWC.2017.2789293.

14. DUANGSUWAN, S.; KLUBSUWAN, K. Accuracy Assessment of Drone Real-Time Open Burning Imagery Detection for Early Wildfire Surveillance. **Forests,** v. 14, n. 9, p.1852, 2023. https://doi.org/10.3390/f14091852.

15. JONNALAGADDA, A. V.; HASHIM, H. A. SegNet: A segmented deep learning based Convolutional Neural Network approach for drones wildfire detection. **Remote Sensing Applications: Society and Environment,** v. 34, art. 101181, Apr. 2024. https://doi.org/10.1016/j.rsase.2024.101181.

16. BOROUJENI, S. P. H.; RAZI, A.; KHOSHDEL, S.; AFGHAH, F.; COEN, J. L.; O'NEILL, L.; FULE, P.; WATTS, A.; KOKOLAKIS, N.-M. T.; VAMVOUDAKIS, K. G. A comprehensive survey of research towards AI-enabled unmanned aerial systems in pre-, active-, and post-wildfire management. **Information Fusion,** v. 108, art. 102369, 2024. https://doi.org/10.1016/j.inffus.2024.102369..

17. AYDIN, B.; SELVI, E.; TAO, J.; STAREK, M. Use of Fire-Extinguishing Balls for a Conceptual System of Drone-Assisted Wildfire Fighting. **Drones,** v. 3, n. 1, p. 1-15, 2019. https://doi.org/10.3390/drones3010017.

18. AUSONIO, E.; BAGNERINI, P.; GHIO, M. Drone Swarms in Fire Suppression Activities: A Conceptual Framework. **Drones,** v. 5, n. 1, p. 1-22, 2021. https://doi.org/10.3390/drones5010017.

19. WANG, Y.; YUE, Q.; LU, X.; GU, D; XU, Z.; TIAN, Y.; ZHANG, S. Digital twin approach for enhancing urban resilience: A cycle between virtual space and the real world. **Resilient Cities and Structures,** v. 3, p. 34–45, 2024. https://doi.org/10.1016/j.rcns.2024.06.002.

20. FORD, D. N.; WOLF, C. M. Smart Cities with Digital Twin Systems for Disaster Management. **Journal of Management in Engineering,** v. 36, n. 4, art. 04020027, 2020. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000779.

21. SOON, K. H.; KHOO, V. H. S. Citygml modelling for singapore 3D national mapping. *In:* **International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences**. Melborne: ISPRS, 2017. v. XLII-4/W7, p. 37-42. https://doi.org/10.5194/isprs-archives-XLII-4-W7-37-2017.

22. GONG, J. **Mobile LiDAR Data Collection and Analysis for Post-Sandy Disaster Recovery**. Reston: ASCE, 2013. p. 677–684. https://doi.org/10.1061/9780784413029.085.

23. GOSAVI, A.; FRAIOLI, G.; SNEED, L. H.; TASKER, N. Discrete-Event-Based Simulation Model for Performance Evaluation of Post-Earthquake Restoration in a Smart City. **IEEE Transactions on Engineering Management**, v. 67, p. 582–592, 2020. https://doi.org/10.1109/TEM.2019.2927318.

24. ARIYACHANDRA, M. R. M. F.; WEDAWATTA, G. Digital Twin Smart Cities for Disaster Risk Management: A Review of Evolving Concepts. **Sustainability**, v. 15, n. 5, art. 11910, 2023. https://doi.org/10.3390/su151511910.

25. HENGUEL, R. P. Palestra. Ações de emergência no Estado de São Paulo: a tecnologia como aliada. *In*: **Ciclo ILP+IPT de Ciência Aplicada, Tecnologia e Inovação em Políticas Públicas 2025 - Ações de Emergência no Estado de São Paulo**: a Tecnologia como Aliada. São Paulo, 02 abr. 2025. Disponível em: https://www.youtube.com/watch?v=Zz0_PA6wfnk. Acesso em: 09 maio 2025.

26. ALERTABLU. **Sistema de monitoramento e alertas de Blumenau**. Disponível em: https://alertablu.blumenau.sc.gov.br/p/home. Acesso em: 09 maio 2025.

27. ALERTA DCNIT. **Aplicativo da Defesa Civil de Niterói.** Disponível em: https://niteroi.rj.gov.br/aplicativo-da-defesa-civil--de-niteroi-e-referencia-nacional/. Acesso em: 09 maio 2025.

28. SERVIÇO GEOLÓGICO DO BRASIL. **Aplicativo Prevenção SGB**. Disponível em: https://www.sgb.gov.br/w/aplicativo-indica-areas-de-risco-no-brasil-com-colaboracao-de-cidadaos. Acesso em: 09 maio 2025.

29. AGÊNCIA SP. **Tecnologia transforma prevenção de desastres em São Sebastião**. Disponível em: https://www.agenciasp.sp.gov.br/especiais/tecnologia-transforma-prevencao-desastres-sao-sebastiao/. Acesso em: 09 maio 2025.

30. GUARUJÁ (Município). **Defesa Civil faz siulação de novo sistema de sirenes para alerta de temporais.** Disponível em: https://www.guaruja.sp.gov.br/defesa-civil-faz-simulacao-de-novo-sistema-de-sirenes-para-alerta-de-temporais-na-quarta. Acesso em: 09 maio 2025.

31. FRANCO DA ROCHA (Município). **Inaugurada a sirene de alerta para temporais e deslizamentos em Franco da Rocha, 2024.** Disponível em: https://www.francodarocha.sp.gov.br/noticia/2024/02/28/inaugurada-a-sirene-de-alerta-para-temporais-e-deslizamentos-em-franco-da-rocha/. Acesso em: 09 maio 2025.

32. BRASIL. Portaria no 3.027, de 4 de dezembro de 2020. Define procedimentos para o envio de alertas à população sobre a possibilidade de ocorrência de desastres, em articulação com os órgãos e entidades estaduais, distritais e municipais de proteção e defesa civil, e para utilização do sistema Interface de Divulgação de Alertas Públicos para envio de alertas via mensagem de texto (SMS), televisão por assinatura ou plataforma de avisos públicos. **Diário Oficial da União,** Brasília, 07 dez. 2020. https://www.in.gov.br/en/web/dou/-/portaria-n-3.027-de-4-de-dezembro-de-2020-292327843. Acesso em: 23 abr. 2025.

33. CENTRO NACIONAL DE MONITORAMENTO E ALERTAS DE DESASTRES NATURAIS. **Consulta geral a homepage do Cemaden/ MCTI, 2025**. https://www.gov.br/cemaden/pt-br. Acesso em: 09 maio 2025.

4 Segurança: detecção e resposta a incêndios

Após apresentar os fundamentos da segurança em um contexto urbano inteligente, é necessário aprofundar o foco na segurança contra incêndio. Esse tipo de ocorrência, embora pontual, tem potencial devastador, especialmente em regiões densamente povoadas. A seguir, apresentam-se as estratégias específicas para prevenção, detecção e resposta a incêndios, com base em tecnologias emergentes e metodologias de gestão estruturada.

A implantação de sistemas digitais foi considerada essencial e com maior potencial de transformação em três áreas da segurança contra incêndio, a seguir indicadas e apresentadas visualmente na Figura 4.1.

- Detecção inteligente de incêndios com sensores, câmeras, drones integrados a uma central monitorada;
- Coordenação de resposta a sinistros em tempo real, com apoio de sistemas digitais;
- Base de dados de projetos de proteção contra incêndio em edificações, planos de emergência e incêndios ocorridos.

Figura 4.1 – Esquema visual dos sistemas digitais para segurança contra incêndio em cidades inteligentes

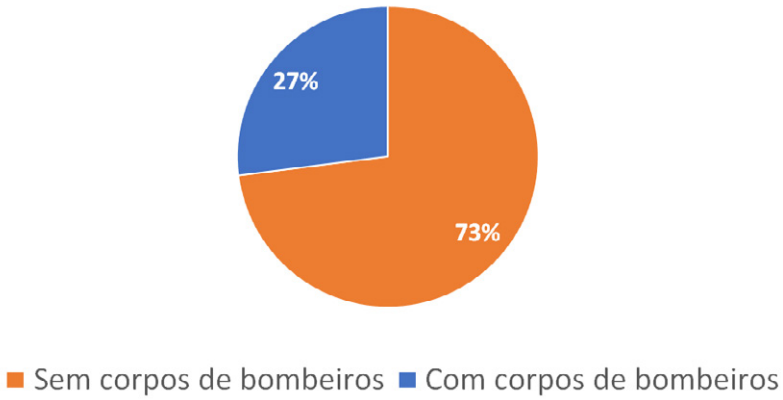
Fonte: Imagem gerada por ChatGPT em 18/04/2025

Essas áreas priorizam a detecção e a resposta rápida, fundamentais para evitar que pequenos focos de incêndio se transformem em grandes desastres, especialmente em regiões mais vulneráveis. Além disso, essas áreas se destacam por serem aquelas mais alinhadas ao potencial revolucionário das cidades inteligentes, aproveitando tecnologias como sensores, inteligência artificial (IA) e conectividade IoT. A detecção inteligente usa ferramentas modernas, como detectores baseados em redes neurais aplicados a câmeras urbanas inteligentes[1], para identificar problemas em minutos (até segundos), enquanto a coordenação em tempo real organiza respostas rápidas e eficazes com o apoio de sistemas digitais. A construção de uma base de dados também foi incluída por seu potencial de evolução com as tecnologias digitais e por oferecer ferramentas que podem ser importantes durante os incêndios, no combate, e após incêndios, em investigações e análises para aumento da segurança e melhor prevenção para futuros sinistros[2]. Juntas, essas áreas criam um sistema robusto e inovador para proteção do estado de forma eficiente.

4.1 Barreiras Tecnológicas e Operacionais na Segurança Contra Incêndio

O alinhamento entre inovação tecnológica e regulamentação local é essencial para tornar as cidades mais resilientes contra incêndios, protegendo vidas e patrimônios. A segurança contra incêndio é uma preocupação crescente em um mundo onde as cidades estão cada vez mais populosas e os riscos ambientais, como secas e ventos fortes, agravam os perigos. Com base em dados de 2018, no Estado de São Paulo essa questão ganha contornos ainda mais urgentes devido à distribuição desigual dos Corpos de Bombeiros: das 645 cidades, apenas 173 possuem Corpos de Bombeiros próprios, enquanto 472 dependem de apoio externo, muitas vezes vindo de longe[3]. Cerca de 73 % das cidades paulistas não contam com Corpos de Bombeiros próprios, conforme apresentado na Figura 4.2.

Figura 4.2 – Distribuição dos Corpos de Bombeiros no Estado de São Paulo[3]



Essa diferença cria um cenário de vulnerabilidade, especialmente em áreas rurais e cidades menores, onde a resposta a emergências pode chegar tarde demais. Em muitos casos, quando um incêndio ocorre, as equipes precisam vir de cidades vizinhas, enfrentando atrasos por causa de distância ou estradas precárias. Essa desigualdade expõe a necessidade urgente de estratégias que não dependam apenas da presença física de Corpos de Bombeiros em cada município e que possam acelerar a resposta deles.

Nesse contexto, soluções tecnológicas como sensores de fumaça conectados à nuvem, sistemas de notificação automatizada para equipes regionais e integração com centrais de dados estaduais podem representar uma revolução na capacidade de resposta, mesmo em áreas remotas. Incêndios representam uma ameaça séria à vida das pessoas e ao patrimônio, podendo causar perdas irreparáveis em poucos minutos se não forem controlados rapidamente.

Do mesmo modo que os demais temas afetos à segurança, a segurança contra incêndio depende da interposição de barreiras associadas a todas as possíveis fases de desenvolvimento do sinistro, de modo que o risco de sua evolução, até eventualmente atingir grandes proporções, seja contido.

A resiliência das cidades, característica precípua de uma cidade inteligente, sob o ponto de vista da segurança contra incêndio, deve ser entendida como a capacidade que deve ter para prevenir ocorrências e, quando os acidentes ocorrerem, minimizar seus efeitos, viabilizando, de maneira menos traumática possível, a continuidade das atividades na edificação afetada.

A abordagem da segurança contra incêndio, sob o ponto de vista sistêmico, pode ser entendida como um sistema de componentes em série, onde as barreiras compõem seus subsistemas. Nessa perspectiva, a falha de um subsistema, ou seja, de uma barreira, pode comprometer definitivamente a confiabilidade de todo o sistema.

Apesar de que, geralmente, o incêndio seja referido como um acidente, nem sempre seu início tem tal característica, visto que pode se iniciar a partir de uma ação deliberada, correspondendo a um ato criminoso (incendiarismo). Essa causa não é rara e ocorre mais frequentemente onde a vigilância das ações desenvolvidas por usuários nas edificações é incapaz de identificar intenções e coibir essas ações danosas. Entre as principais causas do incendiarismo encontra-se o vandalismo, apesar de que os incêndios criminosos podem ter intenções mais específicas, como vingança, ocultação de crimes, obtenção de indenizações securitárias, roubos e assassinatos. Quando isso acontece, nem sempre o foco de incêndio será único e a situação de desenvolvimento do incêndio pode ser mais crítica.

A menos que o incêndio se desenvolva a partir de um grande acidente imediatamente anterior, como uma explosão, possível em indústrias ou depósitos de grande risco, ou de uma ação criminosa maciça ou ainda que alcance edificações nas bordas das cidades, vindo com grande intensidade de áreas florestais, as barreiras propostas em uma boa abordagem da segurança contra incêndio devem ser capazes de conter o avanço do sinistro, a ponto das ações desenvolvidas pelo Corpo de Bombeiros, desde que se iniciem em tempo hábil, serem capazes de reduzir danos à propriedade e ao meio ambiente.

Note-se que o principal objetivo da segurança contra incêndio é garantir a incolumidade das pessoas, mas essa, rigorosamente, não depende do socorro externo no momento da emergência, visto que diante de um incêndio que se desenvolva e assuma o potencial de danos à vida, o plano de abandono previamente concebido e de conhecimento da população da edificação, deve ser imediatamente colocado em prática após o surgimento do incêndio, independentemente do apoio do Corpo de Bombeiros.

A quase totalidade dos municípios de menor porte (menor população) do Estado de São Paulo sequer conta com postos de Corpos de Bombeiros, definindo condições de apoio externo muito aquém do que qualquer situação de risco de incêndio requereria. Note-se que o Convênio estabelecido entre o Município e o Estado para implantação de postos de Corpos de Bombeiros requer a participação financeira do Município.

Apesar disso, as regras de segurança contra incêndio definidas na regulamentação estadual, emitidas pelo Corpo de Bombeiros, e a fiscalização de seu cumprimento, sob a responsabilidade do Corpo de Bombeiros, são obrigatórias. Tal obrigatoriedade se materializa na medida em que sejam exigidas, nos municípios, para a obtenção do Habite-se e da Licença de Funcionamento.

A fiscalização da segurança contra incêndio exercida pelo Corpo de Bombeiros se dá em dois momentos denominados Análise e Vistoria.

No primeiro momento, o processo de segurança contra incêndio apresentado ao Corpo de Bombeiros é analisado: busca-se saber se todas as exigências aplicadas às condições de risco, na qual a edificação se enquadra, estão sendo consideradas. Esse processo incorpora apenas plantas e cortes simplificados, definindo, mais propriamente, apenas um compromisso acerca do cumprimento das exigências contidas na regulamentação.

No segundo momento, o responsável pela construção ou seu proprietário, solicita a vistoria, cujo intuito é checar se os sistemas de proteção contra incêndio exigidos foram implantados. Essa checagem é visual e por amostragem; a avaliação positiva deste procedimento resulta na concessão do Auto de Vistoria do Corpo de Bombeiros - AVCB. Esse documento deve ser periodicamente renovado.

Sob todos os aspectos, à exceção do socorro externo para combate, a segurança contra incêndio de uma edificação independe da atuação do Corpo de Bombeiros. Apesar de esta afirmação parecer polêmica, de fato, não é. Ao contrário, vai de encontro ao que propõe o Corpo de Bombeiros no Capítulo VI do Decreto Estadual Nº 69.118, de 09 de dezembro de 2024 (Regulamento de Segurança Contra Incêndios das edificações e áreas de risco no Estado de São Paulo):

> Artigo 13 - Compete ao CBPMESP, nas vistorias técnicas de licenciamento ou de fiscalização, por meio de seus militares, a verificação, de forma visual e por amostragem, das medidas de segurança contra incêndio previstas para as edificações e áreas de risco, não se responsabilizando pela instalação, comissionamento, inspeção, teste, manutenção ou utilização indevida.
>
> Artigo 14 - Compete ao responsável técnico e ao responsável pela obra, baseados no princípio da boa-fé, adotar, dimensionar e instalar corretamente as medidas de segurança contra incêndio, conforme o disposto neste Regulamento e nas normas técnicas afins.
>
> Artigo 15 - Nas edificações e áreas de risco, com base no princípio da boa-fé, é de inteira responsabilidade do proprietário ou usuário, a qualquer título:
>
> > I - Utilizar a edificação de acordo com o uso para o qual foi projetada, nos termos da licença outorgada pelo CBPMESP;
> >
> > II - Realizar manutenção e testes periódicos das medidas de segurança contra incêndio existentes no local, atendendo às disposições das normas técnicas específicas tomadas como referência nas Instruções Técnicas estabelecidas neste Regulamento, com a devida emissão de relatórios comprobatórios;
> >
> > III - Efetuar, periodicamente, treinamento com os ocupantes do local, bem como manter atualizada a equipe de brigadistas e os planos de emergência;
> >
> > IV - Providenciar a adequação da edificação e das áreas de risco às exigências estabelecidas, nas condições do artigo 4º deste Regulamento;
> >
> > V- Providenciar e manter vigente a licença do Corpo de Bombeiros, exceto nos casos de dispensa previstos neste Regulamento e em normas afins.

Isto posto, fica claro que a administração municipal deve tomar a frente da questão da segurança contra incêndio nas edificações, atuando no município em diversas frentes que devem ter como objetivo final a adoção, para o tema Detecção e Resposta a Incêndios, de abordagem compatível com aquela que caracteriza as cidades inteligentes. Neste contexto, naturalmente, o Corpo de Bombeiros desempenhará um papel importante, desde que seja devidamente compatibilizado com essa abordagem. Apesar disso, não deverá ser independente da administração municipal, como tem sido atualmente.

É necessário ter-se como básico nas edificações de qualquer cidade inteligente, a adoção rigorosa da regulamentação de proteção contra incêndio, estabelecida pelo Corpo de Bombeiros estadual. Por rigorosa deve ser entendido o seguinte:

- Enquadramento correto nas categorias de risco previstas;
- Implantação de todos os sistemas de proteção contra incêndio previstos para o risco;
- Sistemas de proteção implantados a partir de projetos executivos que considerem a regulamentação e a normalização pertinentes;
- Comissionamento dos sistemas e disponibilização (para o proprietário da edificação ou responsável pelo seu uso) dos projetos como construído (*as build*) e de toda a documentação necessária para a operação e manutenção dos sistemas;
- Treinamento dos usuários para a operação dos sistemas;
- Capacitação dos responsáveis pelo uso das edificações para o gerenciamento da segurança contra incêndio;
- Definição de planos de abandono das edificações, a partir de simulação computacional de movimento de pessoas;
- Definição de plano de emergência contando com a participação ou, no mínimo, conhecimento do Corpo de Bombeiros, seguindo roteiro por ele estabelecido;
- Brigada de incêndio, periodicamente treinada;

- Brigada de incêndio contando com bombeiros profissionais civis nos casos de riscos mais severos, como dos locais de reunião de público, hospitais, edificações comerciais e escolas, todos a partir de determinada quantidade de ocupantes;
- Auto de Vistoria do Corpo de Bombeiros (AVCB) atualizado das edificações;
- Fiscalização ampla e aprofundada da abordagem e das características e operação dos sistemas de proteção contra incêndio implantados.

Ainda, é fundamental para atuar na área de segurança contra incêndio, considerando os preceitos aqui estabelecidos de cidade inteligente, que:

- Sejam fornecidas aos responsáveis pelo uso das edificações, informações periodicamente atualizadas sobre a evolução do plano de gerenciamento da segurança contra incêndio;
- Sejam fornecidas informações básicas à população a respeito das questões de segurança contra incêndio nas edificações;
- Seja aberto, por parte da administração municipal, um canal de denúncias para apurar desvios nas edificações capazes de comprometer a funcionalidade dos planos;
- Sejam definidas sanções a serem aplicadas aos proprietários ou responsáveis pelo uso no caso de serem apurados desvios capazes de comprometer a segurança contra incêndio.
- Seja realizada a apuração e o tratamento de dados de incêndio, considerando as regras definidas na norma *ABNT NBR 14023 – Registro de dados de ocorrências de incêndios e emergências*.

É importante destacar que a segurança contra incêndio no Estado de São Paulo vive um paradoxo. Apesar de avanços em regulamentações dos Corpos de Bombeiros e normas técnicas da ABNT, os sistemas instalados nas edificações ainda apresentam desempenho insatisfatório e confiabilidade duvidosa. Estudos realizados pelo IPT nos últimos anos apontam falhas graves em edificações que, mesmo legalmente regularizadas, apresentam sistemas que não funcionam a contento. Sistemas de detecção de fumaça, de sprinklers, de iluminação de emergência e de sinalização de emergência, dentre outros, quase que invariavelmente não atendem aos requisitos mínimos de projeto, instalação e manutenção. Ou seja, em muitos casos, os sistemas estão instalados, mas não têm confiabilidade satisfatória, gerando uma perigosa ilusão de segurança.

Há uma lógica na abordagem da segurança contra incêndio, ou seja, na composição das barreiras que retêm a evolução do incêndio que não está explicitada na regulamentação de segurança contra incêndio. Essa lógica consiste em definir barreiras que visam conter as fases sucessivas do avanço do incêndio e dos danos que podem provocar. Essas barreiras são compostas por conjuntos de medidas de segurança contra incêndio, como mostrado na Figura 4.3.

Figura 4.3 – Diagrama da lógica da segurança contra incêndio

Fonte: Autores, 2025

É importante frisar que a primeira barreira tem o sentido de prevenir o foco de incêndio e lida não apenas com a necessidade de conter ações criminosas de incendiarismo, mas também com aspectos como:

- Correto dimensionamento e execução de instalações de serviço e de processo;
- Manutenção dos equipamentos e instalações que podem provocar o início do incêndio;
- Leiautes e organização da produção voltados para a prevenção de incêndios;
- Sinalização de emergência;
- Correta estocagem e manipulação de materiais combustíveis, líquidos inflamáveis e de outros produtos perigosos;
- Conscientização do usuário da edificação para a prevenção do incêndio.

Diante disso, parte-se do reconhecimento das questões aqui expostas e propõe-se contribuições práticas que complementam a segurança contra incêndio com uso de tecnologias digitais inovadoras[4], que podem trazer grande impacto à área.

4.2 Detecção Inteligente de Incêndios

O objetivo da detecção inteligente é criar um sistema avançado para detectar incêndios rapidamente no Estado de São Paulo, utilizando sensores de fumaça e calor, câmeras térmicas com Inteligência Artificial (IA) e drones multirrotor, todos conectados a uma central monitorada via internet. A integração desses equipamentos busca identificar princípios de incêndio em tempo real, gerar alertas precisos e acelerar a resposta de equipes de emergência, especialmente em áreas urbanas densas, favelas e regiões rurais sem Corpos de Bombeiros. Inspirado em práticas de cidades inteligentes, como descrito por Érces e colegas[1] o sistema combina tecnologia e planejamento para salvar vidas e proteger patrimônios.

A adoção de detecção inteligente gera algumas vantagens para os munícipes em casos de incêndio:

- Redução do tempo de detecção de incêndios, de minutos para segundos, por exemplo os 8 segundos relatados por Érces e colegas[1] com uso de redes neurais;
- Aumento da precisão na localização e análise do foco, evitando atrasos em áreas remotas;
- Diminuição de alertas falsos com uso de inteligência artificial (IA), economizando recursos e mantendo a confiança no sistema;
- Agilidade na resposta das equipes de emergência, essencial em municípios sem Corpos de Bombeiros[3];
- Fornecimento de dados detalhados sobre o tipo e a severidade do sinistro, auxiliando na tomada de decisões.

Equipe Responsável

Uma equipe multidisciplinar é essencial para o sucesso da adoção de sistemas de detecção inteligente, conforme descrito a seguir:

- **Equipes de Tecnologia da Informação (TI**): configuram uma central monitorada, integram os sistemas digitais e garantem a conectividade via redes, como sugerido em *Recent Technology Advancements in Smart City Management*[5];
- **Engenheiros de segurança e especialistas em incêndios**: analisam mapas de risco e normas, como a instrução técnica IT-19/2025 do Corpo de Bombeiros do Estado de São Paulo[5], para escolher os locais ideais para sensores e câmeras;
- **Técnicos, eletricistas e instaladores**: realizam a montagem física dos equipamentos, obedecendo às normas da ABNT NBR 17240[6], que estabelece os requisitos para projeto, instalação, operação e manutenção de sistemas de detecção e alarme de incêndio;

- **Pilotos de drones**: capacitados por empresas ou instituições, operam os drones para vigilância aérea, cobrindo áreas de difícil acesso;
- **Bombeiros do Corpo de Bombeiros da Polícia Militar do Estado de São Paulo (CBPMESP):** elaboram planos de resposta a emergências, treinam as equipes e ajustam os protocolos com base em simulações e dados coletados, conforme instrução técnica IT-16/2025[7].

Implantação

A implantação de um sistema de detecção inteligente de incêndios envolve várias etapas:

- Instalação de sensores de fumaça e calor em pontos estratégicos, como prédios acima de 750 m², favelas (exemplo Paraisópolis) e áreas florestais (exemplo Serra da Cantareira), para monitoramento contínuo. Esses sensores detectam anomalias e enviam dados à central;
- Configuração de câmeras de vigilância térmica equipadas com IA para identificar movimento e calor, de preferência capazes de registrar imagens e integrar os sensores;
- Criação de bases de recarga para drones, equipadas com energia solar em áreas rurais, inspiradas em soluções sustentáveis[1];
- Montagem de centrais de monitoramento, que recebem, processam e analisam dados em tempo real, usando softwares de gestão como os descritos por Avazov[9];
- Integração total dos sensores, câmeras e drones à central, gerando alertas automáticos e fornecimento de informações adicionais (localização, tipo e gravidade do sinistro).

O processo de instalação e operação de detecção de incêndios pode seguir um procedimento padrão, descrito a seguir:

- **Fase 1 - Planejamento e Aquisição:** mapear áreas de risco, definir especificações técnicas e adquirir equipamentos, conforme Lei nº 14.133/2021 (Nova Lei de Licitações);
- **Fase 2 - Instalação de Sensores e Câmeras:** montagem física em cidades-piloto como São Paulo e Campinas, com prioridade para áreas vulneráveis;
- **Fase 3 - Configuração da Central:** instalar servidores e conectar os sistemas via IoT, testando a comunicação em tempo real;
- **Fase 4 – Treinamento:** capacitar 100 agentes em operação de drones, análise de dados e resposta a emergências;
- **Fase 5 - Testes e Ajustes:** simular cenários de incêndio com BIM e ajustar o sistema com base nos resultados.

Instalação

A instalação da detecção inteligente de incêndio pode ocorrer em todos os municípios de São Paulo, porém, sugere-se algumas prioridades, como:

- Cidades de grande porte e metrópoles, onde sensores e câmeras devem ser instalados em prédios, postes e áreas de alta densidade populacional;
- Áreas rurais e florestais, como a Serra da Cantareira, onde drones e sensores solares cobrem grandes extensões sem bombeiros locais;
- Centrais de monitoramento, localizadas em pontos estratégicos com infraestrutura tecnológica robusta (por exemplo, cidades de Sorocaba e São Paulo), protegidas e acessíveis para equipes de emergência.

Operação

o sistema de detecção de incêndio opera em etapas conectadas:

- Sensores, câmeras e drones coletam dados em tempo real de várias partes do estado, enviando informações para as centrais via redes IoT;
- As centrais, equipadas com softwares avançados, processam esses dados, geram alertas e respostas coordenadas, além de prever riscos com base em históricos[10];
- Bombeiros e equipes locais recebem informações por aplicativos ou rádios TETRA (*Terrestrial Trunked Radio*) rapidamente com base em mapas BIM (*Building Information Modeling*) e imagens de drones.

Tecnologias Envolvidas

O sistema de detecção de incêndio depende de tecnologias modernas, tais como:

- ***Blockchain***: garante a segurança dos dados e cria contratos inteligentes para manutenção, conforme [23];
- **Internet das coisas (IoT):** como redes 4G/5G em áreas urbanas e LoRaWAN em rurais para conectar equipamentos sem fio[23];
- **Desligamento Rápido:** ao detectar um incêndio, o sistema de segurança do prédio desativa automaticamente os sistemas elétricos de áreas críticas. Essa é uma medida de proteção essencial que, ao ser integrada aos sensores de incêndio (como detectores de fumaça e calor), ajuda a prevenir a propagação das chamas e a proteger vidas e bens[9];
- **Inteligência Artificial (IA):** filtra falsos positivos, analisa padrões em tempo real e detecta falhas nos sensores, como indicado por Érces e colegas[1];
- **Modelagem BIM (*Building Information Modeling*):** fornece modelos 3D dos edifícios com dados sobre sensores e rotas de evacuação[11];
- **Monitoramento por Vídeo:** câmeras térmicas identificam incêndios em tempo real, registram imagens e se integram aos sensores[8];
- **Plataformas de Gestão:** centros de comando coordenam respostas, comunicam equipes e analisam dados[12,13];
- **Satélites:** monitoram áreas abertas com aerofotogrametria;
- **Sensores:** detectam fumaça e calor continuamente, alertam sobre manutenção e geram dados preditivos[6];
- **Sistemas de Detecção:** reagem automaticamente ao fogo e registram eventos.

4.3 Resposta a Sinistros em Tempo Real

O atendimento a sinistros em tempo real busca conectar equipes de emergência às centrais de monitoramento para gerenciar e direcionar respostas a incêndios de forma rápida e eficiente sob uma coordenação definida. O sistema usa comunicação via internet e considera a capacidade das equipes, a urgência e a gravidade do sinistro, além da presença ou ausência de Corpos de Bombeiros nos municípios do estado. Inspirado em modelos como o desenvolvido pelo *Firescope* na California[12,13] e em práticas em cidades ao redor do mundo[1], o objetivo é salvar vidas e reduzir danos com uma coordenação precisa e em tempo real.

A implantação dos sistemas e tecnologia visando a coordenação rápida de respostas gera algumas vantagens para os munícipes, sendo duas apresentadas a seguir:

- Agilidade na resposta a sinistros para salvar vidas e minimizar danos materiais, crucial em um Estado com histórico de incêndios como os de 2024[14];
- Controle do uso de recursos humanos e materiais, direcionando equipes de forma inteligente para evitar desperdícios e garantir a eficiência, especialmente onde os recursos são escassos.

Equipe Responsável

Um grupo diversificado é essencial na coordenação de resposta a sinistros em tempo real:

- Equipes das centrais de monitoramento coordenam tudo, usando dados de detecção inteligente, análises de Inteligência Artificial (IA) e orientações de especialistas para organizar as respostas;
- Bombeiros do Corpo de Bombeiros da Polícia Militar do Estado de São Paulo (CBPMESP) lideram o combate ao fogo no local, cuidam da evacuação de pessoas em risco, conforme instrução técnica IT-16/2019[7];
- Equipes de emergência médica, como o SAMU (Serviço de Atendimento Móvel de Urgência), prestam socorro imediato às vítimas, trabalhando em conjunto com os bombeiros;
- A Polícia Militar auxilia no controle de acesso à área afetada, garantindo segurança e ordem, conforme práticas de resposta integrada[23].

Implantação

O plano de implantação de uma coordenação para atendimento a sinistros em tempo real envolve ações práticas para uma resposta eficaz:

- Organizar equipes de emergência, recursos e comunicação com base em dados atualizados e análises de especialistas especializados por IA garantindo que cada sinistro receba atenção certa;
- Estabelecer protocolos claros de comunicação entre bombeiros, médicos, polícias e centrais, evitando atrasos e confusões;
- Treinar as equipes para agir de forma rápida e coordenada, usando simulações realistas baseadas em sistemas como o BIM (*Building Information Modeling*)[11];
- Utilizar sistemas de geolocalização, como GPS (*Global Positioning System*), para orientar as equipes diretamente ao local de incêndio com precisão, especialmente em áreas sem bombeiros locais.

Os prazos de repostas quando da adoção da Coordenação de resposta em tempo real tem como padrão o que segue:

- Resposta inicial: até 5 minutos após a detecção de incêndio, com a central enviando alertas às equipes mais próximas, alinhadas às metas de eficiência de SPN-Based Dynamic Risk Modeling[10];
- Chegada ao local: Até 15 minutos após o alerta, dependendo da distância e da infraestrutura viária, com ajustes para áreas rurais onde os drones podem acelerar o processo.

A coordenação de resposta a sinistros em tempo real deve ser aplicada com prioridade em:

- Municípios e bases com equipes de emergência, como as cidades de São Paulo, Campinas e Sorocaba, onde bombeiros e outros profissionais já estão presentes;
- Centrais de monitoramento, instaladas em pontos seguros e tecnologicamente incluídos, como *hubs* regionais ou na capital, para coordenar as ações em tempo real.
- Áreas sem Corpos de Bombeiros (472 municípios[3]), onde a resposta depende de equipes regionais e tecnologias como drones e rádio TETRA (*Terrestrial Trunked Radio*).

Operação

O processo de resposta a sinistro em tempo real é direto e integrado e envolve, basicamente, o seguinte:

- Uma plataforma de comunicação em tempo real conecta as centrais às equipes em campo, permitindo a troca rápida de informações;
- Aplicativos móveis fornecem atualizações instantâneas (ex.: localização do sinistro, gravidade) e coordenadas às equipes, inspiradas em sistemas como o do *Japan Fire Service*[15];
- Sistemas de geolocalização (GPS - *Global Positioning System*) rastreiam e direcionam as equipes, garantindo que cheguem ao local exato sem demora, mesmo em áreas complexas como favelas ou florestas.

Tecnologias Envolvidas

As tecnologias envolvidas para sustentar o sistema de resposta a sinistros em tempo real são:

- ***Big Data* e *Analytics***: armazena dados de sinistros, faz análises preditivas e cria dashboards visuais para as centrais[23].
- **Internet das coisas (IoT)**: conecta sensores, câmeras e drones via 4G/5G, com rádio TETRA (*Terrestrial Trunked Radio*) como backup em áreas sem internet[13].
- **Inteligência Artificial (IA)**: prioriza chamados por severidade, filtra alertas falsos e analisa padrões em tempo real[9].
- **Modelagem BIM (*Building Information Modeling*)**: oferece mapas 3D de edificações para planejamento de acesso e combate ao fogo[11].
- **Plataformas de Gestão**: centros de comando organizam respostas, comunicam equipes e gerenciam incidentes[1].
- **Satélites e Informações Geográficas**: usam aerofotogrametria e GPS para direcionar drones e equipes em grandes áreas.

4.4 Base de Dados de Informações

Essa iniciativa cria uma base de dados robusta para registrar informações sobre incêndios passados, projetos de proteção contra incêndio e planos de emergência de edificações no Estado de São Paulo. O sistema utiliza tecnologias modernas para digitalizar e organizar esses dados, permitindo aprender com o passado, prever riscos futuros e facilitar a resposta aos sinistros. Inspirado em práticas como as dos Corpos de Bombeiros de Londres[16] e em estudos de *Big Data* para segurança[1], o projeto exige sistemas de digitalização, pessoal treinado e apoio estadual, especialmente para os municípios sem Corpos de Bombeiros[3].

A adoção da base de dados gera diversas vantagens, como:

- Aprendizado com dados históricos para identificar padrões e melhorar ações futuras, evitando repetição de erros[17];
- Dimensionamento dos investimentos em segurança contra incêndio com estimativas precisas de danos financeiros, ajudando a priorizar recursos;
- Facilidade para fiscalização do Corpo de Bombeiros da Polícia Militar do Estado de São Paulo (CBPMESP) com informações confiáveis em BIM (*Building Information Modeling*), agilizando vistorias e aprovações;
- Simplificação do acesso a dados de edificações e planos de emergência durante sinistros, acelerando a resposta das equipes.

Equipe Responsável

A equipe envolvida no desenvolvimento do projeto de base de dados de informações deve contar com os seguintes especialistas:

- **Engenheiros e arquitetos**: elaboram e revisam projetos de proteção contra incêndio, fornecendo dados em formato BIM (*Building Information Modeling*) com detalhes sobre sistemas de segurança[11];
- **Bombeiros do CBPMESP (Corpo de Bombeiros da Polícia Militar do Estado de são Paulo)**: relatados com registros de incêndios e planos de emergência, enriquecidos por dados de sensores, câmeras e drones;
- **Equipes de TI**: desenvolvem e mantêm uma base de dados, garantindo segurança e acessibilidade com tecnologias como blockchain[23];
- **Especialistas em segurança contra incêndio**: analisam os dados para identificar padrões, prever riscos e sugerir ações preventivas, apoiados por IA[10].

Implantação

O sistema de base de dados abrange várias ações práticas para a sua implantação:

- Registrar dados detalhados de incêndios ocorridos, como causas, impactos, investigações e lições aprendidas, utilizando informações de sensores, câmeras e drones para maiores precisões;
- Coletar e armazenar projetos de proteção contra incêndio de edificações, como sistemas de sprinklers e saídas de emergência, digitalizados em BIM (*Building Information Modeling*);
- Organizar planos de emergência detalhados para diferentes tipos de prédios (residenciais, comerciais, industriais), com rotas de evacuação e protocolos claros;
- Usar a base para prever riscos futuros e planear medidas preventivas, como reforço em áreas vulneráveis, com base em análises preditivas.

O desenvolvimento do sistema de base de dados pode seguir um prazo médio, conforme apresentado a seguir:

- **Criação inicial da base**: inclui digitalização de registros existentes e configuração do sistema em nuvem;
- **Atualizações regulares**: para adicionar novos projetos, planos e registros de incêndios, garantindo que a base esteja sempre atual[23].

Instalação

O sistema de base de dados deve ser implementado com prioridade em:

- Centrais de monitoramento, localizadas em pontos seguros e tecnologicamente instalados em cidades de grande porte e metrópoles para gerenciamento dos dados em tempo real;
- Servidores em nuvem, garantindo acesso remoto seguro para bombeiros e gestores em todo o estado, incluindo cidades pequenas[24].

Operação

O processo de base de dados deve ser estruturado e eficiente:

- Dados de incêndios são registrados a partir de investigações desenvolvidas, complementados por informações de sensores, câmeras e drones, criando um histórico rico e confiável;
- Projetos existentes e registros oficiais são obtidos, com incentivo para que a sociedade envie planos digitalizados, integrados via plataformas como o Via Fácil Bombeiros[18];
- Softwares de gestão organizam as informações, tornando-as acessíveis por meio de dashboards e relatórios, com IA analisando padrões e consultas de ações[9].

Tecnologias Envolvidas

A principais tecnologias modernas, que sustentam o sistema de base de dados de informação, são:

- ***Big Data e Analytics***: armazena grandes volumes de dados, faz análises preditivas e cria dashboards visuais para gestores[23];
- ***Blockchain***: garante a segurança e a integridade dos dados, evitando alterações não autorizadas[23];
- **Internet das coisas (IoT)**: permite acesso sem fio à base em nuvem por usuários autorizados, utilizando redes 4G/5G;
- **Inteligência Artificial (IA)**: interpreta dados, prevê riscos e estima custos futuros de segurança[10];
- **Modelagem da informação da construção (BIM - *Building Information Modeling*)**: fornece detalhes 3D sobre edificações, incluindo sensores e simulações de cenários[11];
- **Plataformas de Gestão**: analisam dados de segurança e disponibilizam informações em tempo real[16].

4.5 Tecnologias para Detecção e Resposta a Incêndios

Big Data e *Analytics*

O objetivo geral é processar grandes volumes de dados em larga escala, transformando informações brutas em percepções importantes para a segurança contra incêndios. Essa tecnologia é essencial para lidar com a complexidade dos dados gerados por sensores, câmeras e históricos de sinistros23. Os seguintes aspectos devem ser considerados para a implantação da tecnologia de detecção e resposta a incêndios:

- **Equipe necessária para implantação**: equipes de TI e cientistas de dados configuram os sistemas, gerenciam os servidores e desenvolvem modelos analíticos, enquanto especialistas em segurança contra incêndios interpretam os resultados para decisões práticas;
- **O que será feito**: a tecnologia processa dados em tempo real e históricos, oferecendo análises preditivas para antecipar riscos e dashboards para visualização clara das informações, como mapas de calor de áreas de risco;
- **Cronograma**: implantação inicial, por exemplo, em 6 meses, com atualizações contínuas à medida que novos dados são coletados;
- **Locais de implantação**: centrais de monitoramento em cidades de grande porte e metrópoles e servidores em nuvem acessíveis em todo o estado.
- **Como funciona e quais são as tecnologias de apoio**:
  - Armazenamento de Dados - Servidores locais e conexão em nuvem guardam grandes volumes de dados com segurança e escalabilidade.
  - Análise Preditiva - Computadores com softwares como SQL, Python (com bibliotecas, como *TensorFlow*) e SAS preveem tendências, como áreas propensas a incêndios, com base em históricos[9].
  - Dashboards de Visualização - Monitores grandes e ferramentas como Tableau ou Power BI exibem dados em tempo real, ajudando na tomada de decisões rápidas.

Blockchain

O objetivo geral é garantir a integridade e segurança dos dados, protegendo informações sensíveis contra alterações ou acessos não autorizados, uma prática crescente em cidades inteligentes, e garantir a transparência na gestão. As seguintes etapas devem ser consideradas para a implantação do sistema ou a da tecnologia:

- **Equipe responsável**: especialistas em segurança cibernética e equipes de TI implementam e gerenciam plataformas *blockchain*.
- **O que será feito**: criar um registro seguro e imutável para dados de detecção de incêndios e projetos de segurança, além de contratos inteligentes para manutenção automatizada.
- **Cronograma**: configuração, por exemplo, em 4 meses, com integração gradual aos sistemas existentes.
- **Locais de atuação**: servidores em Centrais de Monitoramento e Nuvens Seguras
- **Como funciona e quais são as tecnologias de apoio**:
  - Plataformas seguras - servidores com criptografia armazenam dados com alta proteção.
  - Contratos inteligentes (*smart contracts* - acordos digitais autoexecutáveis, armazenados e executados na *blockchain*) - Computadores com softwares como Ethereum criam acordos automáticos para manutenção de sensores, custos operacionais[23].

Internet das Coisas (IoT)

O objetivo geral é conectar dispositivos como sensores, câmeras e drones às centrais e equipes, permitindo a comunicação em tempo real, de forma rápida e confiável1. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe responsável necessária**: engenheiros de redes e técnicos de Tecnologia da Informação (TI) instalam e mantêm a infraestrutura de conectividade;
- **O que será feito**: por exemplo, estabelecer uma rede sem fio robusta para integrar todos os equipamentos do sistema de segurança contra incêndios;
- **Cronograma**: implantação, por exemplo, em 6 meses, com expansões conforme novas áreas são cobertas;
- **Locais de atuação**: por exemplo, cidades urbanas (com 4G/5G) e rurais (com LoRaWAN), conectando centros e bases de emergência;
- **Como funciona e quais são as tecnologias de apoio**:
  - Redes Sem Fio: Antenas LoRaWAN e Zigbee conectam sensores em áreas remotas, com gateways IoT gerenciando o tráfego[23];
  - Infraestrutura 4G/5G: Estações de rádio base (ERBs), fibra óptica, roteadores e switches fornecem alta velocidade em zonas urbanas.

Desligamento Rápido (*Rapid Shutdown* - RSD)

O objetivo geral é desativar sistemas elétricos instantâneos em edifícios críticos ao detectar incêndios, reduzindo riscos secundários como choques elétricos e propagação em algumas situações9. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe responsável**: engenheiros elétricos e técnicos instalam e integram os dispositivos às centrais;
- **O que será feito**: implementar sistemas automáticos de desligamento em prédios de alto risco, como hospitais e indústrias;
- **Cronograma**: instalação, por exemplo, em 3 meses por edifício, com prioridade para projeto pilotos;
- **Locais de Atuação**: edifícios críticos nas cidades;
- **Como funciona e quais são as tecnologias de apoio**:
  - Microinversores: equipamentos que desligam painéis solares automaticamente[19];
  - Caixas RSD: dispositivos que cortam energia em inversores elétricos;
  - Controladores de tensão: sensores e relés automáticos monitoram e reagem a anomalias, integrados às centrais.

Inteligência Artificial (IA)

O objetivo geral é analisar dados, prever riscos e automatizar respostas, aumentando a eficiência da segurança contra incêndio[10]. As seguintes etapas devem ser consideradas para a implantação da tecnologia:

- **Equipe responsável**: cientistas de dados e engenheiros de software desenvolvem e treinam os modelos de IA;
- **O que será feito**: usar IA para filtrar alertas, priorizar respostas e prever cenários de risco com base em dados em tempo real e histórico;
- **Cronograma**: desenvolvimento inicial, por exemplo, em 6 meses, com ajustes contínuos;
- **Locais de implantação**: centrais de monitoramento e servidores em nuvem processando dados em todo o estado.

- **Como funciona e quais são as tecnologias de apoio:**
  - Aprendizado De Máquina (*Machine Learning*) E Redes Neurais: Servidores Que Treinam Modelos Para Análise Preditiva;
  - Visão Computacional: Câmeras Térmicas E De Alta Resolução Com Detecção De Incêndio Embarcada[8] Ou Com Processamento Posterior Em Servidores.

Modelagem Bim (*Building Information Modeling*)

O objetivo geral é armazenar digitalmente projetos de edificações, incluindo sensores e simulações, provendo informações importantes para respostas a incêndios, fiscalização e bases de dados[11]. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe responsável:** arquitetos e engenheiros criam os modelos, enquanto as equipes de TI gerenciam os dados;
- **O que será feito:** digitalizar projetos com detalhes de segurança e usar simulações para respostas planejadas;
- **Cronograma:** digitalização inicial, por exemplo, em até 6 meses, com expansão contínua;
- **Locais de atuação:** centrais e servidores em nuvem, acessíveis para bombeiros e gestores;
- **Como funciona e quais são as tecnologias de apoio:**
  - Armazenamento: servidores em nuvem guardam modelos 3D;
  - Análise: computadores com softwares como Revit verificam e simulam cenários.

Monitoramento Inteligente por Vídeo

O objetivo geral é detectar incêndios visualmente e fornecer imagens para análise e resposta de forma confiável[9]. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe responsável:** técnicos instalam as câmeras, e equipes de TI processam os vídeos;
- **O que será feito:** monitorar áreas em tempo real com detecção automática de fogo;
- **Cronograma:** instalação, por exemplo, em 6 meses;
- **Locais de atuação:** áreas urbanas e rurais com alto risco;
- **Como funciona e quais são as tecnologias de apoio:**
  - Câmeras: modelos 4K e térmicas com IA embarcada[8], com ajuste automático de foco;
  - Análise de Vídeo: servidores com softwares avançados identificam padrões de incêndio.

Plataformas e Softwares de Gestão

O objetivo geral é centralizar a coordenação de respostas e integrar dados em tempo real para otimizar ações de emergência. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe Responsável:** equipes de TI desenvolvem e gerenciam os sistemas;
- **O Que Será Feito:** por exemplo, criar centros de comando e sistemas integrados para gerenciar incidentes;
- **Cronograma:** configuração, por exemplo, em 6 meses.;
- **Locais de Atuação:** centrais de monitoramento em *hubs* regionais;

- **Como funciona e quais são as tecnologias de apoio:**
  - Centros de Comando: monitores grandes e estações de trabalho exibem dados;
  - Gestão de Incidentes: servidores e tablets registram e acompanham ocorrências;
  - Comunicação: rádios TETRA (*Terrestrial Trunked Radio*) e smartphones conectam equipes.

Satélites e Informações Geográficas

O objetivo geral é monitorar áreas amplas e gerenciar a logística de resposta. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe Responsável:** engenheiros aeroespaciais e técnicos de TI processam os dados;
- **O que será feito:** por exemplo, usar imagens aéreas e GPS (*Global Positioning System*) para direcionar equipes e drones;
- **Cronograma:** integração, por exemplo, em 4 meses;
- **Locais de atuação**: áreas rurais e florestais, como Serra da Cantareira;
- Como funciona e quais são as tecnologias de apoio:
  - Aerofotogrametria: receptores de satélite (por exemplo, INPE – Instituto Nacional de Pesquisas Espaciais) fornece imagens;
  - Drones: equipados com câmeras térmicas[20];
  - GPS: celulares e dispositivos navegam com precisão.

Sensoriamento

O objetivo geral é monitorar em tempo real variáveis como temperatura e fumaça, garantindo detecção precoce e dados confiáveis. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe responsável:** técnicos instalando e mantendo os sensores;
- **O que será feito:** detectar anomalias e mapear riscos continuamente;
- **Cronograma:** instalação, por exemplo, em 6 meses;
- **Locais de atuação:** edifícios e áreas abertas de risco.
- **Como funciona e quais são as tecnologias de apoio:**
  - Sensores IoT: dispositivos de fumaça e calor conectados via gateways.
  - Mapeamento: softwares GIS em computadores criando mapas dinâmicos.

Sistemas de Detecção e Alarme

O objetivo geral é detectar e avisar sobre princípios de incêndio automaticamente. Os seguintes aspectos devem ser considerados para a implantação da tecnologia:

- **Equipe responsável:** engenheiros e técnicos instalam os sistemas;
- **O que será feito:** por exemplo, implementar alarmes e supressão em edifícios;
- **Cronograma:** instalação, por exemplo, em 6 meses por área prioritária;
- **Locais de atuação:** prédios residenciais, comerciais e industriais;

- **Como funciona e quais as tecnologias de apoio:**
  - Detectores e Alarmes: sensores de fumaça e sirenes conectados via wi-fi ou cabos.
  - Supressão: sprinklers com válvulas inteligentes[21].
  - Iluminação: luzes LED de emergência com baterias.

4.6 Sistemas Digitais para Segurança Contra Incêndio

Os sistemas digitais apresentam um grande potencial para a segurança contra incêndio. As três medidas priorizadas — detecção inteligente com sensores, câmeras e drones integrados a uma central monitorada; coordenação de resposta a sinistros em tempo real; e construção de bases de projetos de proteção contra incêndio, planos de emergência e incêndios ocorridos — formam um sistema integrado que maximiza a eficiência na gestão de incêndios.

A detecção inteligente identifica focos de incêndio com maior rapidez, e esses podem ser atendidos de forma coordenada, eficiente e integrada, com respostas mais ágeis, conectando equipes e recursos. A base de dados, registros de projetos de proteção, planos de emergência e histórico de sinistros, apoiam o combate ativo, investigações pós-incidente e a prevenção futura. Juntas, essas estratégias alavancam o potencial das cidades inteligentes, criando um modelo inovador para a segurança contra incêndio.

Apesar dos avanços propostos, desafios permanecem. A eficácia do modelo depende de infraestrutura tecnológica robusta, capacitação contínua das equipes e investimentos consistentes. Também é indispensável a atuação conjunta entre governos municipais, estaduais e o setor privado. Além disso, é necessário reforçar a fiscalização e o cumprimento das normas técnicas. Sistemas instalados com desempenho insatisfatório mostra a urgência de integrar tecnologia às barreiras tradicionais de segurança (prevenção, contenção e abandono)[9].

Em síntese, uma abordagem inovadora e integrada, que combina prevenção, resposta rápida e aprendizado contínuo, alinhada aos princípios das cidades inteligentes[22,24] deve ser a proposta. Mitigar os riscos de incêndio e fortalecer a resiliência urbana e rural, contribui para a proteção de vidas e patrimônios. Entretanto, é fundamental o alinhamento com regulamentações locais, o envolvimento da comunidade e a cooperação com o Corpo de Bombeiros da Polícia Militar do Estado de São Paulo (CBPMESP), para alcançar a referência em segurança contra incêndio no contexto das cidades inteligentes.

Referências Bibliográficas

1. ÉRCES, G.; RÁCZ, S.; VASS, G.; VARGA, F. Fire safety in smart cities in hungary with regard to urban planning. **IDRiM Journal**, v. 13, n. 2, P. 104-128, Dec. 2023. https://doi.org/10.5595/001c.91474.

2. ZHANG, T.; JIANG, Y.; ZHONG, R. Y. Fire Database and Cybersecurity. *In:* X. Huang, W.C. Tam (eds.). **Intelligent Building Fire Safety and Smart Firefighting.** Cham, Switzerland: Springer Nature, 2024. p. 259–280. https://doi.org/10.1007/978-3-031-48161-1_1.

3. GALLUZZI, T. C. **Éramos vinte – a história do corpo de bombeiros de São Paulo - We are twenty – the history of São Paulo fire department**. São Paulo: Gramani Editora, 2018.

4. SILVA, M. F.; MOLDERO, L. D. S.; TRINDADE, L. H.; BARBOSA, A. P. Cidades inteligentes e prevenção de desastres: transformando dados em estratégias resilientes. **Revista Aracê,** São José dos Pinhais, v. 6, n. 4, p. 18618-18631, 2024. https://doi.org/10.56238/arev6n4-444.

5. POLÍCIA MILITAR DO ESTADO DE SÃO PAULO. Corpo de Bombeiros. **Instrução técnica nº. 19/2025 - Sistema de detecção e alarme de incêndio.** São Paulo: Polícia Militar do Estado de São Paulo, 2025.

6. ABNT. **NBR 17240:** Sistemas de detecção e alarme de incêndio – Projeto, instalação, comissionamento e manutenção de sistemas de detecção e alarme de incêndio – Requisitos. Rio de Janeiro: ABNT, 2010.

7. POLÍCIA MILITAR DO ESTADO DE SÃO PAULO. Corpo de Bombeiros. **Instrução técnica nº. 16/2025 - Sistema de detecção e alarme de incêndio.** São Paulo: Polícia Militar do Estado de São Paulo, 2025.

8. HIKVISION. **Câmeras com detecção de incêndio**. 2024. Disponível em: https://www.hikvision.com/pt-br/products/Thermal-Products/Security-thermal-cameras/heatpro-series/?q=inc%C3%AAndio&pageNum=1&position=1&hiksearch=true&category=T%C3%A9rmico&subCategory=C%C3%A2meras+t%C3%A9rmicas+de+seguran%C3%A7a&series=S%C3%A9rie+HeatPro&checkedSubSeries=NONE. Acesso em: 22 abr. 2025.

9. AVAZOV, K.; MUKHIDDINOV, M.; MAKHMUDOV, F.; CHO, Y. I. **Fire Detection Method in Smart City Environments Using a Deep-Learning-Based Approach**. Electronics, v. 11, n. 1, art. 73, 2021. https://doi.org/10.3390/electronics11010073.

10. Hui, M.; Ni, F.; Liu, W.; Liu, J.; Chen, N.; Zhou, X. **SPN-Based Dynamic Risk Modeling of Fire Incidents in a Smart City**. Applied Sciences**,** v. 15, n. 5, art. 2701, 2025. https://doi.org/10.3390/app15052701.

11. SABBAGHZADEH, M.; SHEIKHKHOSHKAR, M.; TALEBI, S.; REZAZADEH, M.; MOGHADDAM, M. R.; KHANZADI, M. A **BIM-Based Solution for the Optimisation of Fire Safety Measures in the Building Design**. Sustainability**,** v. 14, n. 3, art. 1626, 2022. https://doi.org/10.3390/su14031626.

12. FIRESCOPE CALIFORNIA. **Managing Large Scale Incidents – Area Command ICS 420-1.3.** 2020. https://www.firescope.org/. Acesso em: 22 abr. 2025.

5 Segurança pública

A segurança pública em cidades é um desafio crescente e as tecnologias digitais oferecem soluções inovadoras para monitorar, prevenir, detectar, identificar e responder às ameaças (crimes e emergências), auxiliando gestores públicos na tomada de decisões e promovendo maior segurança e bem-estar para a sociedade[1].

As tecnologias digitais, além de permitirem monitorar áreas públicas, ajudando na resolução de crimes, também permitem estudos preditivos para evitar futuras ocorrências. A implantação dessas tecnologias requer planejamento, recursos humanos, e envolve custos com infraestrutura e equipamentos. A seleção criteriosa de tecnologias, aliada a um bom planejamento, potencializa a segurança urbana independentemente da dimensão da cidade.

Um exemplo prático do uso de tecnólogas digitais é o Programa Muralha Paulista, na cidade de São Paulo, que integra câmeras fixas, câmeras corporais e inteligência artificial para monitorar áreas e combater a criminalidade, mostrando como essas tecnologias funcionam em conjunto[20].

A Figura 5.1 exemplifica os principais sistemas digitais empregados em segurança pública em cidades inteligentes.

Figura 5.1 – Tecnologias digitais para segurança pública em cidades inteligentes

Fonte: Imagem gerada por Chatgpt em 25/04/2025.

Definir claramente quais tecnologias serão utilizadas é o primeiro passo para criar um sistema eficiente e adaptável às necessidades de cada cidade, desde pequenos municípios com recursos limitados até grandes centros urbanos com alta complexidade. A Tabela 5.1 elenca os principais sistemas de tecnologias digitais e suas aplicações.

Tabela 5.1 – Sistemas de tecnologias digitais aplicáveis à segurança pública em cidades inteligentes

SISTEMAS DE TECNOLOGIA DIGITAL	DESCRIÇÃO	APLICAÇÕES	EXEMPLO
Sistemas inteligentes de vigilância por vídeo	Câmeras com inteligência artificial (IA) para análise comportamental, reconhecimento facial e de placas veiculares.	Detectar suspeitos, rastrear veículos, monitorar espaços	Programa Muralha Paulista
Câmeras corporais	Dispositivos portáteis para policiais, com gravação de áudio, vídeo e metadados.	Coletar evidências, promover transparência	Polícia Militar do estado de São Paulo em operações urbanas
Sistemas de biometria	Identificação por características físicas ou comportamentais, como rosto, íris ou voz.	Localizar foragidos, controlar acessos	Sistema Automatizado de Identificação de Impressões Digitais presente em bases policiais
Vigilância com drones e robôs	Veículos aéreos e terrestres com sensores para monitoramento e operações de risco.	Monitorar eventos, busca e resgate	Drones usados no Carnaval de 2025 na cidade de São Paulo
Ambientes multissensoriais	Integração de sensores (vídeo, áudio, térmico e radar) para cobertura estratégica.	Cobertura estratégica	Sistemas em rodovias do estado de São Paulo

- ***Big Data* e análise dos dados com Inteligência artificial (IA)**

  Big Data na segurança pública refere-se ao uso de tecnologias avançadas para coleta, armazenamento, processamento e análise de grandes volumes de dados, visando apoiar a tomada de decisão nas áreas de prevenção, intervenção e investigação criminal em centros urbanos. Esta abordagem tecnológica vai muito além das análises estatísticas tradicionais, incorporando elementos de inteligência artificial, aprendizado de máquina e análise preditiva para transformar dados brutos em conhecimento acionável para as forças de segurança.

  Estes sistemas são frequentemente integrados a outras tecnologias emergentes como Internet das Coisas (IoT) e *Blockchain*, formando um conjunto de soluções que estão transformando o cenário da segurança urbana, possibilitando processar informações estruturadas e não estruturadas simultaneamente.

- **Sistema de posicionamento global (GPS)[28]**

  Receptores GPS rastreiam pessoas, veículos e ativos via satélite, transmitindo dados por redes celulares. Possibilita: localização de vítimas em desastres; rastreamento de veículos suspeitos; e coordenação de respostas em eventos.

- ***Blockchain* e sistemas de evidências digitais (DEMS)**

  Blockchain garante a integridade de dados, enquanto sistemas DEMS organizam evidências para uso judicial. Aplicações: proteção contra manipulação de vídeos e áudios; armazenamento seguro de evidências; conformidade com requisitos legais.

- **Computação de Bordo[29]**

  Processa dados diretamente em dispositivos (por exemplo, câmeras), reduzindo latência. Aplicações: análise imediata de vídeos para alertas; respostas rápidas em emergências; redução de carga em servidores centrais.

- **Centros de Comando e Controle (CCC)[27]**

  Unidades centralizadas integram dados de câmeras, sensores, GPS e IoT para monitoramento e coordenação. Aplicações: gestão de operações policiais em tempo real; coordenação de emergências (p. ex. desastres e eventos) visualização via georreferenciamento.

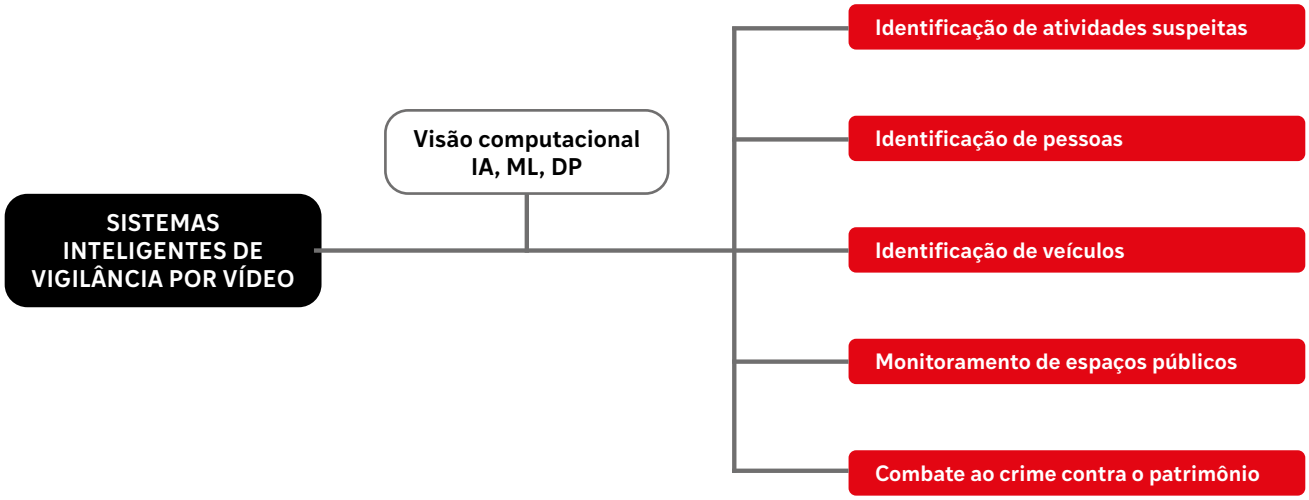
5.1 Sistemas Inteligentes de Vigilância por Vídeo

Os sistemas inteligentes de vigilância por vídeo têm como objetivo garantir a proteção da população urbana, combinando Inteligência Artificial (IA) e novas tecnologias digitais de forma coordenada para prevenir, detectar e responder a atos ilícitos de modo mais eficiente[2,3].

Esses sistemas realizam monitoramentos a partir das imagens capturadas dos vídeos de câmeras (fixas ou móveis) que são convertidas em fluxos de dados visuais digitalizados.

Os fluxos de dados são analisados por modelos de inteligência artificial (IA), por aprendizado de máquina (*machine learning*) e/ou por aprendizagem profunda (*deep learning*), treinados para identificar padrões específicos, como movimentações suspeitas, atitudes potencialmente criminosas e comportamentos anômalos, ou, ainda, características únicas, como o reconhecimento de uma pessoa pelo rosto ou veículos roubados pelo cruzamento dos dados entre a placa licenciada e bases de dados policiais (Figura 5.2).

Figura 5.2 – Resumo da adoção e aplicação das tecnologias de sistemas inteligentes de vigilância por vídeo para cidades inteligentes.



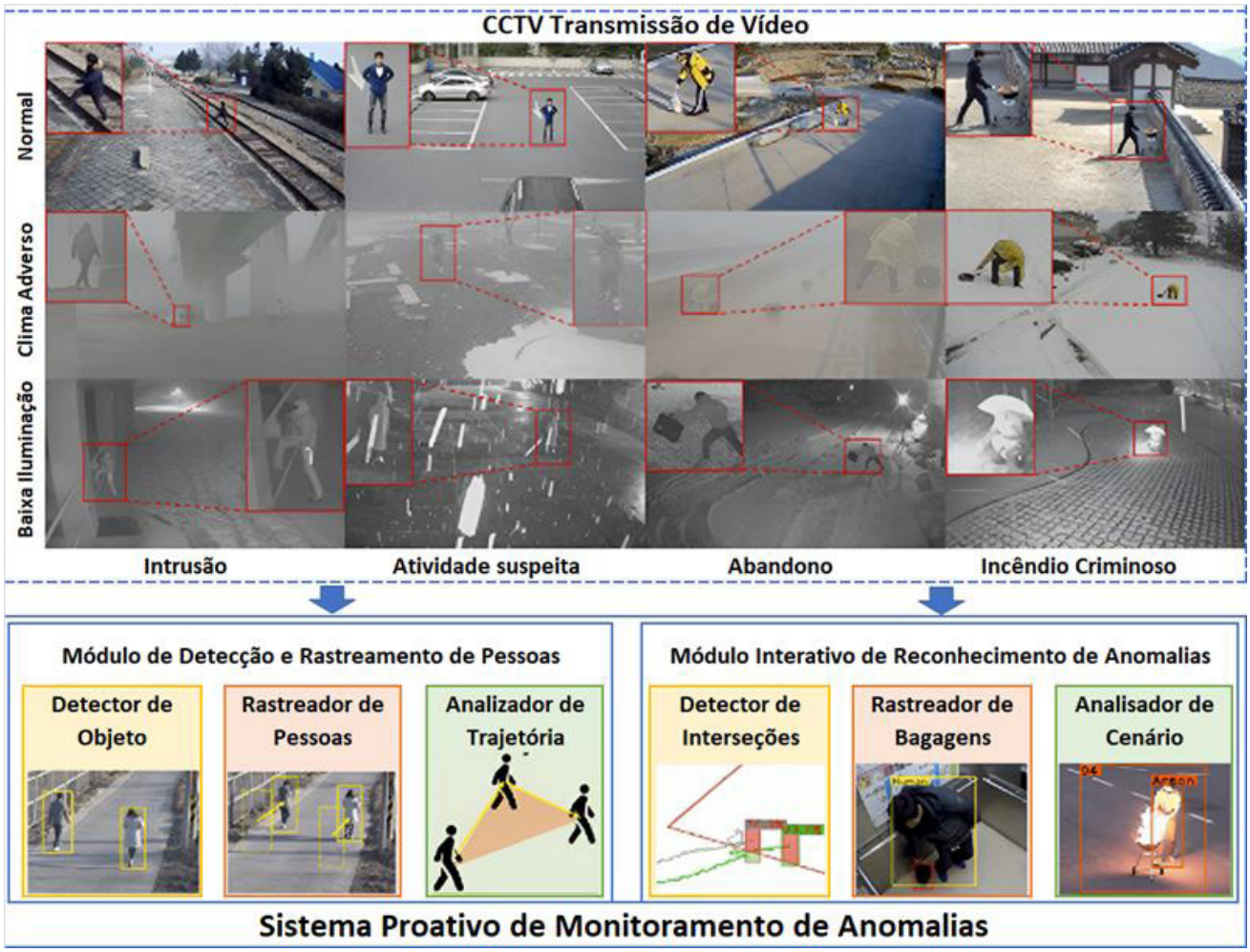
Fonte, Autores, 2025

Os sistemas inteligentes de vigilância são de grande ajuda nas questões indicadas a seguir.

- Atividades suspeitas

  Por meio da análise de padrões comportamentais anômalos é possível a identificação de atividades ou comportamentos suspeitos, assim como mapear trajetórias suspeitas de pessoas e veículos. Esta técnica ajuda a prever crimes e identificar reincidentes, assim como fornece detalhes para investigações e processos judiciais, como horários, locais e sequências de eventos. A Figura 5.3 mostra um exemplo da aplicação da solução tecnológica

Figura 5.3 – Exemplo de sistema de vigilância com câmera proativo com detecção e rastreamento de pessoas e objetos, em diferentes condições ambientais[6]



Também é possível utilizar esta tecnologia para o auxílio e acompanhamento de operações em campo, como perseguições policiais, coordenando ações táticas das equipes.

- Identificação de pessoas

  A identificação de pessoas é realizada ao comparar dados biométricos de imagens capturadas por câmeras e sensores com bases de dados policiais, possibilitando a localização contínua e em tempo real de pessoas desaparecidas, procuradas ou foragidas.

  A utilização da biometria permite o reconhecimento de características físicas ou comportamentais únicas, como impressões digitais, rostos, padrões de íris ou voz para identificação ou verificação de identidade por correspondência. Esse recurso é especialmente útil em locais com grande fluxo de pessoas, como aeroportos, rodoviárias, estações de metrô, eventos públicos ou locais de fronteira, onde criminosos podem tentar se misturar à multidão e se locomover para outras regiões.

- Identificação de veículos roubados

  Esta técnica integrada à de biometria, também permite efetuar a leitura e identificação automática de placas de veículos para rastreamento e controle.

  A identificação permite verificar veículos roubados, não licenciados ou envolvidos em atividades suspeitas ou ilícitas, através do reconhecimento automático de placas veiculares. Câmeras equipadas com inteligência artificial (IA) capturam e analisam as imagens das placas dos veículos convertendo-as em dados alfanuméricos e comparando-as com bases de dados da polícia e dos órgãos de fiscalização do trânsito de veículos terrestres. Um exemplo é mostrado na Figura 5.4.

Figura 5.4 – Exemplo da tela de um sistema de identificação de placas de veículos[5]

- Monitoramento de espaços públicos

  No monitoramento de espaços públicos de grande circulação, as câmeras são empregadas em vias urbanas (ruas, avenidas e rodovias) e locais de multidões, como praças, parques, centros comerciais e terminais de transportes públicos, fornecendo uma vigilância constante e permitindo a detecção imediata de incidentes, como furtos, assaltos e agressões.

  O uso de Inteligência Artificial (IA) permite que esses sistemas identifiquem indivíduos e atividades anômalas, como padrões comportamentais suspeitos, aglomerações incomuns e movimentações bruscas que possam indicar um crime em potencial ou em andamento, acionando automaticamente as forças de segurança para intervenção rápida.

- Combate ao crime contra o patrimônio

  Esses sistemas são utilizados para identificar ações de vandalismo, depredação, pichações e destruição de bens públicos e privados, assim como invasões.

  A Inteligência Artificial (IA) pode detectar padrões de comportamento relacionados a atos de vandalismo ou acessos não autorizados e notificar imediatamente os operadores de segurança, permitindo uma resposta mais ágil e a preservação do patrimônio. Além disso, a capacidade de armazenar e analisar imagens facilita a investigação e a responsabilização dos envolvidos, funcionando como um meio de dissuasão para futuros crimes.

A implantação de sistemas inteligentes de vigilância urbana aumenta a segurança pública nas cidades por meio da identificação automática de atividades suspeitas ou criminosas em tempo real. Esses sistemas combinam redes de sensores e câmeras (por exemplo, Internet das Coisas - IoT) com algoritmos de inteligência artificial (IA) para monitorar o ambiente urbano de forma abrangente e proativa[2,3].

Com o crescimento das áreas urbanas e o volume massivo de dados gerados (vídeo, áudio, entre outros), a IA surge para analisar automaticamente imagens de câmeras de segurança, sons capturados por microfones e outros sensores, detectando comportamentos anômalos ou ameaças e alertando as autoridades instantaneamente[3].

A integração de IA com esses sistemas pode prevenir crimes ao reconhecer situações de risco (por exemplo, identificar brigas, invasões ou disparos de armas de fogo) e permitir respostas rápidas das equipes de segurança[2,4]. Além disso, a análise preditiva de dados históricos de criminalidade permite antecipar crimes ou incidentes, orientando o policiamento para locais e horários de maior risco[2].

Esses sistemas apoiam-se na necessidade de elevar a capacidade de vigilância urbana frente à criminalidade, utilizando tecnologias modernas para superar limitações humanas e tornar as cidades mais seguras e bem monitoradas (reduzindo o tempo de reação e aumentando a dissuasão)[2]. Vale notar que, paralelamente aos benefícios, há consenso na literatura sobre a importância de considerar questões de privacidade, segurança de dados e vieses algorítmicos, implementando-se desde o início diretrizes éticas e legais para uso responsável da IA em segurança pública[3,34].

Requisitos para Implantação de Sistemas Inteligentes de Vigilância por Vídeos

Os pré-requisitos para implantação de sistemas inteligentes de vigilância por vídeos englobam infraestrutura de rede e computação adequadas, disponibilidade de dados e modelos de Inteligência Artificial (IA) validados, adesão a normas técnicas e de segurança e a preparação institucional para suportar o novo sistema[3,4]. Atender a esses pré-requisitos é condição essencial para que a implantação ocorra sem entraves e o sistema atinja o desempenho esperado com confiabilidade e em conformidade com as normas.

A transmissão de vídeo em tempo real e dados de múltiplos sensores demandam redes de banda larga robustas (fibra óptica, enlaces sem fio dedicados ou 5G) com baixa latência[3]. Se a cidade ainda não possui cobertura adequada, a atualização ou expansão da infraestrutura de telecomunicações torna-se um pré-requisito fundamental.

Também é preciso assegurar a disponibilidade de plataformas computacionais para processamento dos dados. Isso inclui servidores locais e unidade de processamento gráfico (GPU) ou aceleradores para rodar algoritmos de visão computacional, bem como acesso a serviços de *cloud computing* para tarefas de maior carga ou armazenamento em longo prazo[4].

Recomenda-se abordar as questões de privacidade desde a fase inicial do desenho do sistema ("*security and privacy by design*")[3,7]. Os mecanismos de proteção de dados pessoais e auditabilidade dos algoritmos devem ser pré-requisitos atendidos antes da ativação do sistema em ambiente real.

A operação de um sistema inteligente de vigilância urbana por vídeo não é trivial e envolve os pontos indicados a seguir.

Requer processos bem definidos e infraestrutura adequada de comando e controle

Em geral, as cidades implantam um Centro de Comando e Controle (CCC) ou salas de controle e operação 24 horas, onde convergem os fluxos de vídeo e alertas gerados pela IA.

No CCC operadores humanos monitoram múltiplas telas com imagens ao vivo de câmeras distribuídas pela cidade, enquanto softwares analíticos executam em segundo plano a detecção automática de eventos suspeitos[2]. Quando um algoritmo identifica uma possível ocorrência (por exemplo, uma pessoa portando arma, um aglomerado de pessoas não usual indicando briga ou um indivíduo invadindo área restrita) o sistema emite um alarme em tempo real para os operadores[2].

Esses alertas automáticos são imediatamente validados por um operador humano, evitando mobilizações indevidas por falsos alarmes[4]. Uma vez confirmada a veracidade, protocolos são acionados e viaturas próximas são notificadas via rádio, centrais são acionadas pelo 190 (em integração), ou são feitas comunicações diretas com equipes de pronta resposta e patrulha na área. Essa sinergia entre Inteligência Artificial (IA) e humano permite respostas em espaço de tempo menores, onde as análises automatizadas reduzem o tempo para localizar suspeitos ou veículos após um crime, em comparação à métodos tradicionais[5].

Requer que o sistema integre diversas fontes de dados em tempo real.

Além de câmeras de vídeo, sensores acústicos de detecção de tiros podem alertar sobre disparos em segundos, sinalizando automaticamente câmeras próximas para apontar para a direção do som. Quando um disparo é detectado por sensores, o sistema pode posicionar câmeras de vídeo PTZ (Pan-Tilt – Zoom) adjacentes para filmar o local exato do tiro[8]. Essas câmaras permitem o controle remoto de movimentos horizontais (pan), verticais (tilt) e zoom.

Da mesma forma, sistemas avançados podem acender iluminação pública inteligente ao detectar situações de violência (por exemplo, voz agressiva ou quebra de vidro) à noite, contribuindo para inibir a continuidade do ato. Toda essa coordenação automática é supervisionada pela central, onde os operadores têm visão global e podem intervir manualmente se necessário.

Requer garantir a continuidade do serviço.

Arquiteturas modernas empregam computação de borda e em nuvem de forma redundante: nós de borda (*edge nodes)* próximos às câmeras processam localmente os dados críticos, mas se algum nó falha, a nuvem assume suas tarefas para assegurar operação ininterrupta[2]. Essa redundância minimiza o tempo de inatividade (*downtime*) e garante que, mesmo diante de falhas de conexão ou equipamento, a vigilância permaneça ativa.

A operacionalização inclui rotinas de manutenção e atualização, as câmeras devem ser limpas e calibradas periodicamente, os algoritmos de Inteligência Artificial (IA) requerem retreinamento ou ajustes conforme mudanças nos padrões urbanos, e testes de segurança cibernética devem ser conduzidos para prevenir invasões ao sistema.

A equipe da Tecnologia de Informação (TI) monitora a saúde da rede e dos servidores, enquanto a equipe de segurança analisa relatórios gerados, como estatísticas de alertas por região, para retroalimentar estratégias de policiamento. A operação de um sistema inteligente de vigilância é um processo contínuo que combina monitoramento automatizado e intervenção humana, com protocolos claros de resposta e um ecossistema tecnológico resiliente para assegurar que quaisquer atividades suspeitas sejam detectadas e tratadas com máxima agilidade[5].

Requer políticas de armazenamento seguro de dados para evitar perda de evidências.

E importante também gerenciar a sobrecarga de informações, uma vez que a central pode receber milhares de fluxos e alarmes por dia. Portanto, painéis interativos (*dashboards*) e interfaces de prioridade devem classificar os alertas por grau de severidade. Ferramentas de análise de conteúdo de vídeo (*video analytics)* muitas vezes agrupam eventos relacionados e fornecem resumos (clipes dos momentos-chave) para facilitar a avaliação pelos analistas humanos[2].

Adicionalmente, é importante o engajamento das instituições responsáveis. A efetividade da vigilância inteligente depende de integração com as operações policiais, portanto protocolos de cooperação e treinamento conjunto devem estar acordados. Aspectos legais, como autorização para uso de câmeras em locais públicos ou compartilhamento de dados entre órgãos, precisam ser resolvidos previamente (por meio de convênios, decretos municipaise outros tipos de acordos).

Definição de Locais de Implantação de Sistemas de Vigilância Inteligente por Vídeos

Os locais de implantação de um sistema inteligente de vigilância por vídeos devem ser escolhidos com base em critérios objetivos de segurança, como concentração de crimes, fluxo populacional e ativos urbanos críticos, fundamentados em dados estatísticos e análise preditiva, garantindo que os recursos tecnológicos sejam alocados onde seu impacto na prevenção e repressão ao crime seja maior[3].

Usualmente são destacados para vigilância os centros comerciais e turísticos, regiões com grande circulação de pessoas (como praças, estações de transporte e terminais urbanos) e áreas com histórico de delitos (bairros com alta taxa de roubos ou locais com incidência de vandalismo). Vias de tráfego intenso e cruzamentos movimentados também recebem atenção, pois, além de crimes, são pontos onde ocorrem incidentes de trânsito e aglomerações.

A otimização de cobertura de câmeras em cidades aponta que o fluxo de tráfego é um dos principais critérios para selecionar rotas e posições de câmeras, pois ruas com maior movimentação estão mais expostas a acidentes e situações de risco, devendo ser monitoradas prioritariamente. Da mesma forma, locais como entradas de escolas, parques públicos e eventos de grande porte são críticos para a segurança e se beneficiam da detecção precoce de comportamentos anômalos (por exemplo, brigas e tumultos).

Infraestruturas sensíveis e estratégicas podem ser incluídas na cobertura, como os arredores de instalações governamentais, áreas portuárias, refinarias ou usinas, onde riscos de sabotagem ou terrorismo exigem vigilância reforçada[4].

A seleção dos locais também deve considerar, ainda, aspectos práticos, como a disponibilidade de pontos de fixação para câmeras (postes e edifícios altos), acesso à energia, e sinal de rede e locais com visibilidade ampla que minimizam pontos cegos. O posicionamento das câmeras pode ser determinado utilizando modelos em grafo da malha urbana para escolher posições que ofereçam o maior campo de visão possível com o menor número de câmeras.

Como complementação às câmeras fixas, pode-se empregar câmeras móveis ou drones em áreas de difícil acesso ou em operações especiais, ampliando temporariamente o alcance de vigilância conforme a necessidade[4].

Importante observar que a cobertura total e indiscriminada de todos os espaços urbanos não é viável nem desejável (por custos e privacidade). Assim, a implantação deve ser faseada e orientada por prioridades. Inicia-se pelos locais de maior risco e, conforme os recursos, expande-se o monitoramento para regiões adjacentes ou novos bairros, sempre mediante análise de dados criminais atualizada. Essa priorização dinâmica é apoiada por modelos preditivos que realocam recursos conforme surgem novos padrões de criminalidade em determinados locais[4].

Implantação de Sistema de Vigilância Inteligente por Vídeo

A implantação de sistema integrado de vigilância inteligente por vídeos deve seguir etapas bem definidas e orientação técnica rigorosa. A Figura 5.5 apresenta uma sugestão de etapas para implantação de sistema inteligente de vigilância por vídeo.

Figura 5.5 – Etapas para implantação de sistema inteligentes de vigilância por vídeo

Fonte: Autores, 2025

Para essas etapas tem-se:

- **Definição de objetivos:** os objetivos devem ser claros e não dar margem a dúvidas, por exemplo, reduzir determinado crime em certo local;
- **Levantamento de risco e locais críticos:** devem ser identificadas áreas de alta incidência criminal e eventos a serem monitorados (por exemplo, furtos e vandalismo), o que guiará a disposição dos sensores e câmeras[3];
- **Avaliação da infraestrutura existente:** verificação da existência de Tecnologia da Informação, como redes de fibra óptica, disponibilidade de 4G/5G e de energia elétrica e, se necessário, modernizar a infraestrutura para garantir alta confiabilidade e banda larga suficiente[3];

  Tecnologias de IoT e Inteligência Artificial (IA) aplicadas em cidades exigem redes robustas e estáveis para interligar milhares de dispositivos com baixa latência[3]. Assim, recomenda-se investir em conectividade 5G ou em malhas de comunicação dedicadas, assegurando que o grande volume de dados (vídeos em alta definição, por exemplo) trafeguem em tempo real sem perda. Em paralelo, devem-se adotar protocolos e padrões de comunicação para garantir interoperabilidade entre dispositivos de diferentes fabricantes;
- **Projeto piloto em escala reduzida**: consiste em instalar um conjunto inicial de câmeras inteligentes e sensores em um bairro ou região de teste, integrados a uma central de monitoramento equipada com os algoritmos de IA escolhidos;

- **Análise dos resultados do projeto piloto:** é essencial para realizar a calibração dos algoritmos de detecção, ajustando parâmetros para o contexto local e coletando dados para treinar ou refinar os modelos de reconhecimento, por exemplo, adaptando a detecção de comportamento suspeito às características culturais e ambientais da cidade[4,6];
- **Definição da solução:** escolha final da tecnologia e dos protocolos com base nos resultados do projeto piloto;
- **Expansão gradual do sistema para outras áreas prioritárias da cidade:** a partir dos resultados do projeto piloto.

A implantação de sistemas inteligentes de vigilância por vídeos deve ser acompanhada de um plano de treinamento para os agentes que utilizarão o sistema, garantindo que saibam operar as novas ferramentas e interpretar os alertas. A existência de Procedimentos Operacionais Padrão (POPs) ajudam nas respostas a eventos, como por exemplo: definir como os alertas serão verificados e quais ações imediatas devem ser tomadas (por exemplo, despacho de viatura e acionar equipes de pronta-resposta).

Por fim, a implantação de um sistema inteligente de vigilância urbana envolve: planejamento e infraestrutura adequados, uso de tecnologias interoperáveis e escaláveis, execução de projeto piloto com melhoria iterativa, treinamento de pessoal e estabelecimento de protocolos, além da integração antecipada de medidas de segurança e privacidade no desenho do sistema[3]

Equipe Responsável

A implantação de um sistema inteligente de vigilância por vídeo requer uma equipe multidisciplinar e colaboração interinstitucional, envolvendo órgãos de segurança pública (Guarda Municipal, Polícia Militar e Civil) atuando em conjunto com equipes técnicas de Tecnologia da Informação (TI) e especialistas em Inteligência Artificial (IA).

Também é possível estabelecer parcerias entre departamentos de polícia, universidades, autoridades municipais e empresas de tecnologia para desenvolver e operar plataformas avançadas de videomonitoramento[5]. Nesse modelo colaborativo, a polícia fornece a orientação de segurança e responde aos alertas, enquanto pesquisadores e engenheiros de dados auxiliam no aprimoramento dos algoritmos de IA e no tratamento dos dados coletados[3].

Parcerias sustentáveis entre forças de segurança e instituições de pesquisa podem incorporar práticas baseadas em evidências e avaliar continuamente a efetividade do sistema. A equipe responsável deve incluir gestores públicos, para assegurar a conformidade legal (por exemplo, respeito à privacidade e transparência) e especialistas em infraestrutura de rede e computação, para manter o funcionamento dos equipamentos de Internet das Coisas (IoT), redes 5G e servidores em nuvem.

Esse arranjo multidisciplinar aumenta a eficiência do sistema, pois combina conhecimento operacional de campo com expertise tecnológica[3,5].

Tecnologias Envolvidas

Os sistemas inteligentes de vigilância urbana por vídeo integram diversas tecnologias digitais, cujo uso conjunto viabiliza a detecção automática de crimes. A estrutura é formada por dispositivos IoT (Internet das Coisas) espalhados pela cidade, como as câmeras de segurança de alta resolução, microfones direcionais, sensores de movimento, detectores acústicos de disparos, entre outros.

Esses dispositivos coletam continuamente dados do ambiente urbano. Câmeras inteligentes, por exemplo, incorporam processadores e algoritmos embarcados capazes de identificar objetos ou pessoas nas imagens em tempo real, enviando informações (como presença de determinado veículo ou contagem de pedestres) para os níveis superiores do sistema[4]. Em complemento, sensores acústicos especializados podem reconhecer o som de tiros ou explosões e ativar alarmes instantaneamente[8], enquanto sensores ambientais (por exemplo, de iluminação e de temperatura) podem contribuir para análises contextuais. Todos esses dispositivos comunicam-se via redes sem fio ou cabeadas, frequentemente utilizando protocolos de IoT eficientes, compondo uma malha de coleta de dados ubíquos pela cidade.

No núcleo do sistema está a Inteligência Artificial (IA), sobretudo na forma de algoritmos de aprendizado de máquina (*machine learning*) e de aprendizagem profunda (*deep learning),* aplicados à visão computacional e à análise de séries temporais. A IA é responsável por interpretar os dados brutos captados pelos sensores, identificando padrões indicativos de anomalias ou delitos.

Em vídeos, utilizam-se técnicas de detecção de objetos para localizar pessoas, veículos ou outros itens de interesse em cada imagem individual. Em seguida, algoritmos de rastreamento (*tracking*) acompanham o movimento desses alvos através das câmeras[2]. Isso permite, por exemplo, seguir um suspeito que transita por diferentes câmeras ou rastrear a trajetória de um veículo em fuga.

Algoritmos de reconhecimento facial também podem ser empregados, comparando rostos capturados com bases de dados de procurados. Uma componente da IA nesses sistemas é a detecção de comportamentos anômalos ou ações suspeitas. Modelos de *Human Action Recognition* (HAR) e detecção de anomalias em vídeo aprendem sequências de movimento típicas (por exemplo, andar e correr) e disparam alertas quando identificam algo fora do comum, como alguém caindo e permanecendo imóvel (possível mal-súbito), uma briga com agressões físicas ou um objeto abandonado em local público.

Esses modelos baseados em redes neurais profundas conseguem captar sutilezas e realizar em segundos essas análises. Um sistema de vigilância inteligente detecta e rastreia objetos, reconhece faces, identifica anomalias e até prediz incidentes potenciais, enviando alarmes para monitoramento proativo e resposta rápida. Ou seja, além de identificar eventos em andamento, os algoritmos podem estimar riscos iminentes, como reconhecer uma aglomeração crescente e indicar possibilidade de tumulto, permitindo que a polícia atue preventivamente[2].

Para viabilizar o uso da IA distribuída, entram em cena duas tecnologias complementares: computação em nuvem (*cloud computing*) e computação de borda (*edge computing*).

A computação em nuvem (*cloud computing*) fornece poder de processamento escalável e centralizado. Grandes volumes de vídeos podem ser enviados para datacenters onde algoritmos realizam análises aprofundadas, como identificar novamente um suspeito em várias câmeras pela roupa[2]. Também na nuvem ficam frequentemente os sistemas de armazenamento de longo prazo e bancos de dados correlacionando diferentes fontes (p. ex. cadastro de veículos e histórico de ocorrências).

A computação de borda (*edge computing*) consiste em processar os dados próximo de onde são gerados, nos próprios dispositivos ou em servidores locais nas regiões monitoradas. Isso reduz a latência de decisões urgentes, como detectar um atropelamento e fechar um semáforo próximo, onde a decisão pode ser imediata e localmente. Além disso, alivia a carga da rede e da nuvem, onde somente eventos relevantes ou dados filtrados são enviados adiante, economizando banda e armazenamento[2].

Assim, os sistemas atuais combinam a computação de borda (*edge computing*) e computação em nuvem (*cloud computing)* de forma hierárquica. As câmeras inteligentes e nós de borda (*edge nodes)* fazem triagem inicial e respondem a eventos imediatos, enquanto a computação em nuvem consolida informações e executa algoritmos de alto custo ou abrangência global, como predições semanais de padrões criminais.

Outra tecnologia é a conectividade 5G, a quinta geração de telecomunicações móveis. O 5G oferece alta velocidade de transmissão e latências na ordem de poucos milissegundos, o que é essencial para aplicações de vídeo em tempo real com Inteligência Artificial (IA). Em redes 4G convencionais, transmitir dezenas de *streams* (sequência contínua de dados) em alta definição simultaneamente poderia gerar atrasos, já que o 5G suporta fluxos de vídeo 4K e comunicação quase instantânea entre sensores e central.

As capacidades de alta banda e baixa latência do 5G são um habilitador-chave para sensoriamento ubíquo em cidades inteligentes, tornando viável conectar massas de câmeras e dispositivos IoT espalhados pela área urbana. Além disso, o 5G possibilita a implantação de fatiamento de rede (*network slicing*), tecnologia que permite criar redes virtuais independentes e personalizadas sobre a mesma infraestrutura de rede, assim pode-se ter rede móvel configuradas especificamente para tráfego de segurança pública, garantindo qualidade de serviço mesmo em horários de pico.

Por fim, outras tecnologias complementares frequentemente integradas incluem: análise preditiva e *Big Data*, usando mineração de dados (*data mining*) e modelos estatísticos e aprendizado de máquina (*machine learning*) sobre grandes bases de dados criminais e urbanos para prever tendências e orientar ações futuras (o chamado *predictive policing*, em que algoritmos analisam histórico de ocorrências e variáveis socioeconômicas para indicar onde crimes têm maior probabilidade de ocorrer)[2,9].

O *blockchain* e computação confiável, explorados para garantir integridade e autenticidade dos vídeos e *logs do sistema* (arquivos que registram eventos e atividades ocorridas em um sistema operacional ou em um aplicativo específico), impedindo adulterações (por exemplo, registrando o *hash* de cada vídeo em uma *blockchain*).

As tecnologias de segurança cibernética avançadas, como sistemas de detecção de intrusão, autenticação multifatorial para operadores e criptografia ponta-a-ponta, protegem a infraestrutura de vigilância contra-ataques digitais. Portanto, o ecossistema tecnológico envolvido engloba dispositivos IoT diversos, IA (visão computacional e reconhecimento de padrões), computação em nuvem e de borda trabalhando em sinergia, redes 5G, além de ferramentas de análise preditiva e segurança cibernética, formando um sistema complexo e interconectado. Essa convergência de tecnologias permite que as cidades implementem vigilância proativa, com resposta automatizada e inteligente a eventos de segurança, algo impraticável com tecnologias isoladas ou legadas[2].

5.2 Câmeras Corporais (*Bodycams*)

As câmeras corporais são dispositivos portáteis usados por oficiais da força policial, fixados em uniformes, para capturar e registrar áudio e vídeo de interações da perspectiva do policial com o público.

As câmeras são ativadas manualmente ou automaticamente e os dados são transmitidos para as centrais de apoio tático. As interações gravadas e armazenadas incluem metadados (*timestamps* e localização por GPS) utilizados pelos sistemas de gestão das evidências digitais (*Digital Evidence Management Systems* - DEMS) da segurança pública.

As câmeras corporais (BEWs - *Body-Worn Cameras)* permitem a documentação fidedigna das interações entre agentes de segurança e cidadãos, mediante captura simultânea de vídeo de alta definição, áudio sincronizado e metadados (data-hora em UTC, GPS, identificador do dispositivo e do usuário). Os modelos atuais permitem gravação contínua e acionamento manual, sensorial (som e movimento) ou automatizado por inteligência artificial, integrando os registros a sistemas seguros de gestão de evidências digitais[11].

O objetivo principal de sua implantação na segurança pública urbana é aumentar a transparência e a responsabilização nas ações policiais, fornecendo um registro independente de abordagens, intervenções e incidentes. Além disso, as imagens captadas servem como evidência objetiva em investigações e processos judiciais, facilitando a apuração dos fatos e a resolução de denúncias contra policiais ou de alegações falsas contra cidadãos[10,17].

Aspectos da Aplicação de Câmaras Corporais

A definição dos contextos e operações urbanas prioritárias para uso de câmeras corporais deve considerar onde seu impacto potencial em transparência e accountability será mais benéfico. De modo geral, dá-se prioridade a funções de policiamento ostensivo e preventivo, em que há frequente contato direto com a população.

Assim, unidades de patrulha de rua (a pé ou motorizada) e policiamento de proximidade são candidatas iniciais, pois envolvem abordagens, fiscalizações de trânsito, atendimento a ocorrências diversas e outras interações cotidianas com cidadãos.

Outro contexto são as ações policiais em áreas de alta criminalidade ou de maior incidência de confrontos. Nesses locais, onde há maior risco de uso da força letal ou não letal, as câmeras atuam como importante ferramenta de registro de *como* se deram as intervenções.

No Brasil, têm-se direcionado câmeras inicialmente para batalhões e companhias com histórico elevado de confrontos e letalidade, exatamente para promover uma mudança de cultura e redução de violência policial nesses cenários críticos. Operações especiais planejadas – como cumprimento de mandados de busca e apreensão em áreas urbanas, blitz de trânsito em grande escala, policiamento de manifestações públicas e eventos com aglomeração – também são indicadas para uso das câmaras corporais, dadas as potenciais situações de conflito e necessidade de transparência.

De modo complementar, as câmeras corporais vêm sendo empregadas em policiamento de trânsito e fiscalização viária. Em abordagens de trânsito urbanas (como paradas em blitz ou verificação de documentos), a gravação protege tanto o agente quanto o cidadão de alegações infundadas (por exemplo, a câmera pode provar que não houve extorsão ou que o motorista estava apresentando comportamento suspeito).

Embora a maior parte das implantações foque no policiamento ostensivo, outras forças de segurança urbana também podem se beneficiar. Guardas municipais em metrópoles brasileiras, responsáveis pelo patrulhamento de parques, praças e proteção de patrimônios, têm avaliado o uso de câmaras corporais para registro de suas intervenções administrativas e apoio às polícias. Outro tipo de uso é pelos corpos de bombeiros durante atendimentos de resgate, para fins de documentação da cena, e por equipes de fiscalização civil, como agentes de imigração ou segurança privada.

Implantação das Câmaras Corporais

A implantação de um programa de câmeras corporais deve ser cuidadosamente planejada, seguindo etapas e boas práticas amplamente recomendadas por órgãos técnicos e estudos de caso (Figura 5.6).

Figura 5.6 – Fluxograma resumido das etapas de implantação das câmeras corporais

Inicialmente na fase de planejamento, é indicada a criação de um grupo de trabalho multidisciplinar dentro do órgão de segurança, englobando comandos operacionais, setor jurídico, tecnologia da informação, corregedoria e, se possível, representantes da comunidade e de órgãos de controle externo[10]. Esse grupo elabora um plano de implantação que define os objetivos do projeto, o escopo e levanta requisitos técnicos e orçamentários.

A seguir, desenvolve-se uma normatização clara sobre o uso das câmeras. Essa normatização geralmente toma forma em políticas ou portarias internas que detalham quando os agentes devem ativar a câmera, em quais tipos de ocorrência seu uso é obrigatório, e exceções, além de procedimentos para armazenamento, guarda e acesso às imagens[10].

Outro aspecto que deve ser salientado é a necessidade de treinamento extensivo dos policiais antes do uso efetivo das câmeras em serviço[6,7]. Os agentes devem ser capacitados não apenas no manuseio técnico do dispositivo, mas também informados sobre as implicações legais do registro audiovisual, boas práticas de postura ao gravar (por exemplo, anunciar quando possível que a interação está sendo filmada) e as penalidades por descumprimento das diretrizes (como esquecer de acionar a câmera sem justificativa).

Na fase de aquisição das câmaras, é fundamental seguir as normas de compras públicas e, preferencialmente, especificações técnicas padronizadas. O *National Institute of Justice* (NIJ) fornece subsídios sobre as características dos diversos modelos disponíveis e auxiliam na elaboração de termos de referência adequados. Critérios de avaliação devem incluir não apenas o custo unitário das câmeras, mas também capacidades técnicas (resolução de vídeo, autonomia de bateria e robustez), funcionalidades adicionais (como pré-gravação em *buffer* e marcação de eventos) e integração com sistemas existentes[10].

Após a aquisição e distribuição dos dispositivos, recomenda-se estabelecer um período de teste operacional e melhoria de procedimentos, no qual o uso das câmeras é monitorado de perto e eventuais ajustes nas políticas são realizados com agilidade.

Outro ponto da implantação é a comunicação e engajamento das partes interessadas. É importante informar claramente o efetivo policial sobre os objetivos do programa – enfatizando seu caráter de proteção tanto para o cidadão quanto para o agente – a fim de obter aceitação interna e minimizar resistências corporativas[6]. Da mesma forma, deve-se comunicar à sociedade sobre a novidade, explicando como as câmeras funcionarão e de que forma contribuirão para a melhoria da segurança pública, o que favorece a legitimidade pública do programa[6].

A orientação para implantação de câmaras corporais engloba a definição de métricas de avaliação e processos de revisão. É recomendável que se acompanhem indicadores como número de usos da força, número de reclamações contra policiais e taxa de conformidade no acionamento das câmeras, comparando períodos antes e depois da adoção. Os dados coletados permitem avaliar o impacto da iniciativa e realizar ajustes informados.

Operação com Câmaras Corporais

Na prática diária, o uso das câmeras corporais segue protocolos específicos para garantir que a operação policial seja documentada de forma contínua e segura sem comprometer a efetividade do agente. As etapas podem ser resumidas em pré-turno, durante o turno e pós-turno.

Antes de iniciar o turno, o policial verifica se sua câmera está devidamente acoplada ao uniforme (normalmente na altura do tórax e em suporte próprio) e se o equipamento está funcionando – bateria carregada, lente limpa e armazenamento disponível[10]. Algumas instituições adotam a padronização de que a câmera permaneça no modo *stand-by* (em espera) durante todo o turno, cabendo ao agente apenas acionar o *record* (gravar) efetivo no momento oportuno, enquanto outras definem janelas de gravação predefinidas.

Durante as missões, a orientação é de que o agente ative a gravação assim que iniciar uma interação policial que envolva contato com cidadãos ou entrada em uma cena de ocorrência. Uma vez iniciada, a gravação normalmente deve prosseguir ininterruptamente até a conclusão do atendimento ou da ação policial, salvo exceções previstas (por exemplo, em conversas estratégicas entre policiais ou quando a continuidade da gravação se torna inviável por segurança). Essa continuidade garante a captura de todo o encadeamento dos fatos, evitando lacunas que possam levantar dúvidas[7].

Posteriormente, esse material pode ser analisado quadro a quadro para esclarecer, por exemplo, a dinâmica de um confronto. Em alguns modelos mais avançados, as câmeras corporais podem contar com estabilização de imagem ou resolução alta que, mesmo em movimento, permitem identificar elementos relevantes.

Ao término da ação ou turno de serviço, ocorre a operacionalização do pós-gravação. Os dados coletados são transferidos de forma segura para o sistema de armazenamento central[10]. Uma vez no servidor, os vídeos recebem marcações de data, horário, identificador do policial e outras informações de identificação e rastreamento, ficando disponíveis para consulta autorizada. Procedimentos de cadeia de custódia entram em vigor aqui: cada acesso, cópia ou extração de trecho deve ser identificado, garantindo a rastreabilidade de quem acessou o quê. Se uma gravação for relevante para um inquérito, ela será vinculada ao respectivo processo, obedecendo às normas de preservação de evidências.

A operacionalização das câmeras corporais envolve procedimentos desde o acionamento correto nas diversas situações (patrulhamento, perseguição ou buscas) até a retirada segura dos dados e seu encaminhamento para uso apropriado. Quando tais procedimentos são seguidos rigorosamente, obtém-se um registro contínuo e confiável das ações policiais, o que aprimora tanto a *accountability* (pela possibilidade de auditoria) quanto à eficácia judicial das provas colhidas, integrando-se de maneira fluida à rotina dos agentes[10]. O Quadro 5.2 aponta requisitos técnicos gerais para as câmeras corporais.

Quadro 5.2 – Requisitos técnicos gerais e de infraestrutura referentes as câmara corporais

Requisitos	
Técnicos Gerais	■ Conformidade do hardware ■ Módulo criptográfico certificado ■ Integridade de evidência ■ Controle de acesso lógico ■ Sincronização temporal de alta precisão ■ Interoperabilidade de metadados ■ Formatos abertos ■ Mitigação de viés de perspectiva
Técnicos de infraestrutura	■ Largura de banda mínima de descarregamento ■ Gestão de segurança da informação ■ Gerenciamento centralizado de evidências ■ Residência e proteção de dados sensíveis ■ Ambiente físico controlado ■ Arquitetura de logs centralizados ■ Continuidade de serviço ■ Escalabilidade contratual

Equipe Responsável

Em geral, a instituição policial ou de segurança pública que implanta a tecnologia assume a coordenação central do programa[10,12,13]. Dentro da corporação, costuma-se designar uma unidade gestora específica ou um *coordenador do programa de câmaras corporais,* incumbido de elaborar procedimentos operacionais padrão, assegurar o treinamento dos usuários e monitorar a conformidade ao protocolo de uso (por exemplo, verificar se os agentes ativam as câmeras conforme exigido).

No nível operacional, os próprios agentes de segurança (policiais militares, guardas municipais ou patrulheiros) são responsáveis por portar e acionar as câmeras durante o serviço, seguindo as diretrizes estabelecidas. Seus supervisores imediatos devem orientá-los e fiscalizar o uso correto dos dispositivos, realizando revisões periódicas das gravações para fins de auditoria de procedimentos e identificação de necessidades de melhoria ou condutas inadequadas.

A manutenção técnica e a gestão do armazenamento dos vídeos geralmente ficam a cargo do setor de Tecnologia da Informação (TI) ou de comunicação da corporação policial. Essa equipe cuida da infraestrutura de armazenamento de dados (servidores locais ou nuvem) e garante que os vídeos sejam transferidos de modo seguro das câmeras para os repositórios ao fim de cada turno. Também é responsabilidade da TI assegurar a atualização dos softwares relacionados, a integridade dos arquivos (com mecanismos contra adulteração) e o funcionamento adequado dos equipamentos (baterias carregadas e câmera em bom estado)[10].

A análise dos dados captados pode envolver diferentes atores conforme a finalidade. Para fins de persecução penal, as imagens podem ser encaminhadas a peritos ou analistas de inteligência para extração de evidências específicas ou diretamente compartilhadas com o Ministério Público, que as avaliará na instrução de processos criminais.

Em atividades de monitoramento e pesquisa, unidades de estatística ou observatórios de segurança podem analisar conjuntos de vídeos para extrair indicadores operacionais visando aprimoramento gerencial.

Tecnologias Envolvidas

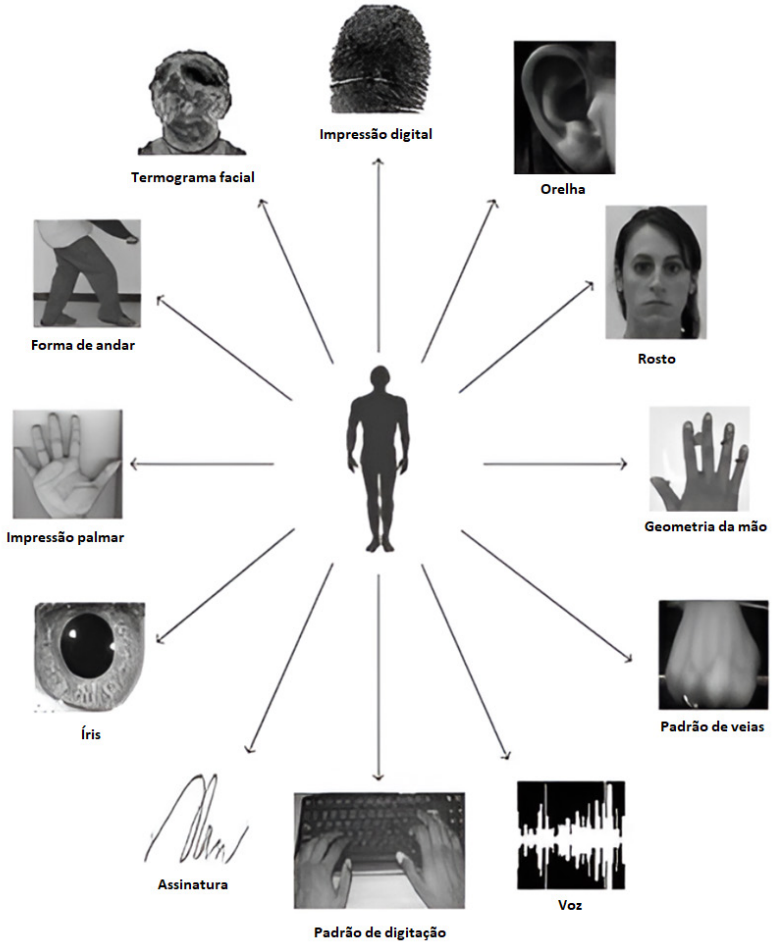
A seguir, estão elencadas tecnologias envolvidas no caso das Câmeras Corporais:

- Sensores óticos e módulos de captura;
- Processamento embarcado e criptografia de borda;
- Sincronização temporal e padronização de metadados;
- Arquiteturas de computação de borda;
- Inteligência artificial de vídeo;
- Detecção de violência;
- Identificação de armas;
- Anomalias em multidões;
- Resumo automático;
- Inteligência artificial de áudio;
- Preservação de privacidade e redação automática;
- Proveniência de evidência e blockchain;
- Gestão de evidência digital (DEMS);
- Mitigação de viés algorítmico e governança;
- Padrões emergentes e pesquisa continuada.

5.3 Sistemas de Identificação Biométrica

Os sistemas de biometria utilizam características físicas e comportamentais únicas, como impressões digitais, rostos, padrões de íris ou voz, para identificação e verificação da identidade de pessoas (Figura 5.7). Sensores e câmeras capturam dados biométricos, processados pelo sistema, para extrair características que são comparadas à bancos de dados para correspondência (por exemplo, *Automated Fingerprint Identification Systems* – AFIS).

Figura 5.7– Exemplos de biometrias que podem ser usadas para autenticar um indivíduo[2]



A biometria contribui para a vinculação da identificação de pessoas com evidências de cenas de crimes, restrições de deslocamentos ou acessos não autorizados, como prevenir entrada em áreas sensíveis a pessoal autorizado ou saída ilegal por fronteiras, e proporciona a busca sistematizada automática acelerando correspondências.

No caso de veículos, sistemas de reconhecimento automático de placas (ANPR, *Automatic Number Plate Recognition*) monitoram o tráfego e sinalizam veículos roubados ou em situação irregular, agilizando a recuperação de veículos e a prisão de suspeitos em fuga. Essas tecnologias, integradas a bases de dados policiais, oferecem um ganho estratégico no combate ao crime, pois ampliam a capacidade do Estado em identificar e localizar rapidamente alvos de interesse com precisão técnica superior à identificação humana convencional.

O sistema de identificação biométrica consiste em permitir a identificação única, inequívoca e célere de pessoas de interesse para a segurança pública, mediante captura, extração e comparação automatizada de dados biométricos com bases de referência, em conformidade com *ISO/IEC 19794-2 – Information Technology- Biometric data interchange formats. Part 2: Finger minutiae data*, referente a padrões de intercâmbio e *ISO/IEC 30107-3 - Information Technology- Biometric presentation attack detection. Part 3: Testing and reporting* referente à detecção de ataques.

O processo de identificação por biometria envolve três camadas: sensores (coleta), mecanismo de correspondência (motor biométrico) e camada de aplicação (integração com registros criminais, cadastros civis ou lista de procurados). A justificativa decorre das vantagens operacionais de confiabilidade, escalabilidade e interoperabilidade, evidenciadas no Radar Tecnológico da ANPD (Autoridade nacional de Proteção de Dados), nos estudos da Agencia das Nações Unidas sobre drogas e Crimes (UNODC – *United Nation Office on Drugs and Crime*) e no programa ABIS (Sistema Automatizado de Identificação Biométrica) da Polícia Federal, que preveem cobertura superior a 200 milhões de perfis e redução do tempo de identificação de horas para segundos.

Implantação da Tecnologia de Identificação Biométrica

A implantação dessa tecnologia envolve, principalmente, as etapas indicadas na Figura 5.8 e explicadas a seguir.

Figura 5.8 - Etapas de implantação das câmeras corporais.

Fonte: Autores, 2025

Análise de Viabilidade e Planejamento

Inicia-se com um estudo detalhado das necessidades e do contexto local, define-se o escopo do projeto (quais modalidades biométricas serão usadas – por exemplo, reconhecimento facial em câmeras urbanas, impressões digitais móveis, entre outras), e os objetivos específicos (captura de foragidos, identificação em abordagens, controle de acesso a áreas sensíveis, entre outras) com os indicadores de sucesso esperados. Concomitantemente ao planejamento técnico, deve-se verificar o arcabouço jurídico que permitirá a operação do sistema. Isso envolve obter eventuais autorizações legais, pareceres de órgãos de controle e estabelecer acordos de cooperação entre instituições. É recomendável criar um comitê gestor do projeto, com participação de autoridades policiais, representantes jurídicos e especialistas técnicos, para acompanhar a implantação e a tomada de decisões estratégicas. Esse comitê define políticas de uso (com quem pode acessar o sistema e em que circunstâncias), protocolos de atuação em caso de alertas e diretrizes de transparência e prestação de contas.

Aquisição e Desenvolvimento

Com base no estudo de viabilidade, inicia-se o processo de seleção ou contratação da tecnologia. As boas práticas recomendam buscar soluções consolidadas e compatíveis com padrões internacionais, garantindo interoperabilidade e desempenho. Para reconhecimento digital, é importante aderir a padrões, como os da série *ISO/IEC 19794 –Information technology – Biometric data interchange fromats,* que tem diversas normas referentes à aplicação da biometria, e do Departamento Federal de Investigação dos Estados Unidos (FBI- *Federal Bureau of Investigation*), permitindo que no futuro diferentes sistemas "conversem". Nas licitações, devem-se exigir testes de acurácia e laudos de desempenho dos algoritmos

(muitos países utilizam os relatórios do NIST – *National Institute of Standards and Technology* – que avaliam diversos algoritmos de reconhecimento facial e de digitais). Também é crucial prever cláusulas de transferência de conhecimento e treinamento: o fornecedor deve treinar os operadores e técnicos do órgão público. Durante essa etapa, é recomendável conduzir projetos-piloto em pequena escala para validar a tecnologia no cenário real antes do pleno funcionamento. Esses pilotos permitem ajustar configurações – por exemplo, sensibilidades do software para reduzir alarmes falsos – e identificar desafios operacionais (como iluminação inadequada em certos pontos de instalação de câmeras).

Implantação Gradual e Avaliação Contínua

Inicialmente, instala-se a infraestrutura nos locais prioritários e coloca-se o sistema em operação assistida. Nessa fase inicial, mantém-se uma atenção especial às métricas de desempenho: taxa de identificação correta, incidência de falsos positivos (identificações incorretas) e falsos negativos (pessoas não reconhecidas). Boas práticas sugerem que, se o sistema apresentar altas taxas de falso positivo ou negativo, ajustes sejam feitos antes da expansão, pois acurácia baixa pode comprometer a confiabilidade e legitimidade do programa. Deve haver um protocolo para que todo alerta de identificação passe por confirmação manual por um operador treinado, minimizando riscos de erros e constrangimentos indevidos a cidadãos inocentes. Ao longo da implantação, auditorias independentes podem avaliar se os usos estão de acordo com as finalidades previstas e se medidas de segurança da informação são satisfatórias.

Treinamento

A capacitação de policiais e agentes incluem orientações técnicas (uso de dispositivos de captura e consulta ao banco de dados móvel) e treinamento jurídico e ético, enfatizando os limites legais e o respeito à privacidade.

Operação Assistida

Uma vez implementado, o sistema deve operar inicialmente sob supervisão intensiva do comitê gestor. Reuniões periódicas analisam relatórios de desempenho e incidentes. Se forem constatados problemas, ações corretivas são tomadas – seja ajuste técnico ou realocação de equipamento.

Definição de Locais para Implementação da Tecnologia Biométrica

Definir onde implementar primeiro os sistemas biométricos é crucial para obter o máximo impacto na segurança pública. Os locais prioritários geralmente são escolhidos com base em critérios de índices de criminalidade, fluxo de pessoas e/ou veículos e criticidade estratégica. Pode-se considerar as seguintes áreas como prioritárias:

- **Áreas de Grande Circulação e Eventos:** locais com alta concentração de pessoas e acesso ao público, como centros comerciais, praças centrais, estações de metrô e trem e terminais rodoviários, são locais naturais para câmeras com reconhecimento facial. Nesses locais, é inviável para policiais checarem manualmente cada rosto, mas o sistema automatizado pode varrer multidões e apontar alvos de interesse em tempo real, aumentando a capacidade de vigilância sem expandir o efetivo policial;
- **Entradas, Saídas e Vias Estruturantes da Cidade:** para veículos, a prioridade costuma ser instalar leitores automáticos de placas nas principais vias de acesso e rotas com outras cidades, como rodovias, avenidas expressas e fronteiras municipais. Isso cria uma espécie de "cerco eletrônico", permitindo identificar carros roubados ou envolvidos em delitos assim que entrarem ou saírem do perímetro urbano;
- **Zonas de Alta Criminalidade (*Hotspots*):** outra abordagem é direcionar as primeiras unidades para bairros ou regiões com elevados índices de criminalidade violenta ou tráfico de drogas – os chamados *hotspots*. Assim, instalar câmeras inteligentes em cruzamentos de bairros críticos, ou levar dispositivos biométricos para operações policiais frequentes nesses locais, podem trazer resultados rápidos;

- **Instalações Sensíveis e Pontos de Interesse Estratégico**: proteger infraestrutura crítica e autoridades, como prédios governamentais, fóruns, aeroportos, estádios e fronteiras como prioritários. Esses são espaços onde um controle de identidade rigoroso previne ameaças graves (por exemplo, terrorismo e crime organizado);
- **Unidades Móveis e Patrulhas**: dotar de viaturas de patrulha com equipamentos biométricos (tablets integrados a câmeras ou leitores de digitais portáteis) é uma forma de priorização baseada em atividade. Assim, a tecnologia acompanha as equipes policiais em abordagens por toda a cidade, em vez de ficar restrita a um ponto.

Aspectos Relacionados à Operação da Tecnologia Biométrica

No cotidiano da segurança pública, a operacionalização dos sistemas biométricos ocorre de forma integrada às abordagens e procedimentos já realizados pelos agentes – porém agilizando e dando suporte objetivo nas decisões (Figura 5.9).

Figura 5.9 – Fluxo operacional típico da tecnologia

Fonte: Autores, 2025

Alguns cenários práticos de uso durante ações de verificação de identidades de pessoas e veículos são apresentados a seguir:

- **Abordagem a pedestres ou suspeitos:** com o sistema biométrico, o policial utiliza um dispositivo móvel de identificação biométrica (um leitor portátil de digitais ou um aplicativo com câmera) para verificar instantaneamente a identidade. Se a pessoa forneceu nome falso ou um documento adulterado, o sistema revelará sua identidade real, exibindo na tela do agente o nome verdadeiro, foto cadastrada e eventuais alertas (como mandados de prisão ou registro de pessoa desaparecida);
- **Verificação de veículos em movimento:** no caso de veículos, a operacionalização prática se dá tanto de forma fixa quanto móvel. Em pontos fixos (câmeras de monitoramento urbano ou radares inteligentes), o sistema *Reconhecimento Automático de Placas* (ANPR-*Automatic Number Plate Recognition*) lê automaticamente as placas de todos os veículos que passam e consulta, em fração de segundos, o banco de dados nacional de veículos. Se identificar uma placa inserida no sistema gerará um alerta imediato. Esse alerta pode ser exibido na central de monitoramento e diretamente para as viaturas próximas;
- **Reconhecimento facial em tempo real no campo:** o uso de câmeras acopladas a uniformes ou óculos, ou mesmo smartphones, para reconhecimento facial durante patrulhamentos. Assim, um policial poderia apontar a câmera portátil para um indivíduo que julgue suspeito (ou vários em sequência, ao caminhar numa área movimentada) e aguardar que o sistema retorne indicação de *match* se aquele rosto corresponder a alguém procurado;
- **Central de Comando e Controle:** em todas as situações acima, uma central de operações geralmente acompanha a movimentação em tempo real. Essa central conta com policiais ou analistas que monitoram os alertas entrando pelo sistema biométrico. Os centros integrados de monitoramento comunicam-se em tempo real com as viaturas e agentes, inclusive com localização geográfica dos alvos. Na prática, cria-se um fluxo contínuo de informação: as câmeras e dispositivos capturam os dados, o sistema identifica e gera alertas, o centro valida e coordena, e as equipes móveis executam a abordagem ou intervenção.

Como pré-requisito para operação é necessário dispor de uma infraestrutura de Tecnologia da Informação (TI) com servidores de alta capacidade de processamento (dada a carga de comparar milhares ou milhões de *templates* biométricos em segundos), armazenamento suficiente para os bancos de dados biométricos (imagens e *templates* de digitais, rostos, entre outros) e links de comunicação de dados velozes e seguros para conectar postos de coleta (câmeras e dispositivos móveis) ao sistema central.

Além disso, devem estar disponíveis dispositivos de captura de qualidade, ou seja, câmeras com resolução adequada e posicionamento correto (no caso de reconhecimento facial, câmeras HD ou superiores, instaladas em ângulos que capturam frontalmente os rostos), *kits* (conjunto) de coleta de digitais (*livescans* ou leitores portáteis homologados) e eventualmente scanners de íris se essa modalidade for usada. Esses dispositivos precisam ser calibrados e testados nas condições locais (luminosidade e clima – por exemplo, câmeras externas devem ter carcaça resistente e funcionar à noite com iluminação infravermelha).

Outro pré-requisito técnico é a existência de bases de dados de referência confiáveis. O sistema só "reconhece" alguém se há um registro prévio. Logo, é fundamental que o órgão já possua (ou possa integrar) bases de identificação civil ou criminal – como o cadastro de impressões digitais do instituto de identificação civil, o acervo de fotos de fichas policiais, o Registro Nacional de Condutores Habilitados (RENACH) e Registro Nacional de Veículos Automotores (RENAVAM) para as placas de veículos.

O software de biometria deve seguir padrões para poder receber e enviar dados a outros sistemas[33] (por exemplo, consulta ao banco de procurados da Interpol). A aderência a padrões garante também que, se for necessário trocar de fornecedor futuramente, os dados biométricos coletados poderão ser reutilizados no novo sistema, assegurando a sustentabilidade tecnológica.

Equipe Responsável

A implantação bem-sucedida de sistemas biométricos exige uma equipe multidisciplinar devidamente capacitada para gerir, operar e manter a infraestrutura, bem como para analisar os dados gerados. Em geral, a gestão fica a cargo de um órgão de segurança pública (por exemplo, a Secretaria de Segurança Pública estadual ou departamento de polícia responsável) que designa um núcleo ou divisão específica para o sistema. Essa equipe de gestão cuida do planejamento estratégico, da política de uso e do cumprimento de normas e protocolos.

Na operação diária, estão incluídos profissionais técnicos e policiais especializados: por exemplo, peritos em identificação (como os papiloscopistas, especializados em identificação por impressões digitais) e analistas de reconhecimento facial. Esses profissionais realizam o cadastramento de dados biométricos, monitoram as correspondências (*matches*) e validam manualmente eventuais alertas do sistema, garantindo que decisões críticas (como uma abordagem ou prisão) sejam tomadas com base em dados confirmados.

As equipes contam com analistas de inteligência que exploram os dados cruzados (por exemplo, correlacionando identidades confirmadas com mandados de prisão, antecedentes ou redes criminosas), extraindo informações estratégicas para investigações.

Tecnologias Envolvidas

O funcionamento dessas soluções envolve diferentes tecnologias integradas. Utilizam-se câmeras e scanners ópticos de alta resolução para captura de imagens e dados detalhados. A conectividade 5G, combinada com processamento em borda (*edge computing*), permite que parte das análises seja feita rapidamente, antes mesmo de os dados chegarem aos servidores centrais.

Os sistemas de aprendizado de máquina, especialmente aqueles baseados em redes neurais convolucionais (CNN - *Convolutional Neural Networks*), são treinados com bases de dados balanceadas, garantindo mais precisão na detecção de situações relevantes. Em alguns casos, empregam-se módulos de análise com luz estruturada e termografia para auxiliar em investigações e procedimentos administrativos disciplinares.

Para proteger a integridade das informações, utilizam-se infraestruturas de chave pública (PKI) para autenticação de dispositivos e, quando necessário, *blockchain* ou outros mecanismos que criam trilhas de auditoria imutáveis. A comunicação entre sistemas é feita por APIs padronizadas (RESTful – *Representational State Transfer*), o que facilita a integração entre diferentes plataformas.

Por fim, técnicas de *big data analytics* permitem identificar padrões criminais e apoiar decisões estratégicas. Toda a avaliação de segurança deve seguir critérios e metodologias utilizadas em testes forenses, garantindo a confiabilidade dos resultados.

A seguir, destacam-se as principais tecnologias envolvidas para a identificação de pessoas, identificação de veículos e sistemas de armazenamento e cruzamento de dados.

Para Identificação de Pessoas

- Reconhecimento facial: tecnologia que analisa a imagem do rosto de uma pessoa e extrai características únicas (distâncias entre olhos, formato do nariz, mandíbula, entre outras), gerando um *template* digital para comparação.
- Impressões digitais (AFIS/ABIS- Sistema Automatizado de Identificação de Impressões Digitais/ Sistema Automatizado de Identificação Biométrica): tecnologia biométrica que se refere a sistemas automatizados de identificação de digitais. Eles digitalizam as impressões e extraem minúcias (padrões de terminações e bifurcações de linhas) e comparam com base de dados. Para segurança pública, a digital tem papel duplo: identificação civil ou criminal de pessoas vivas (por exemplo, confirmar a identidade de um suspeito) e identificação de vestígios e vítimas nos locais de crime (por exemplo, elucidando autoria).
- Reconhecimento de íris: consiste na identificação pelo padrão de detalhes da íris, que é único para cada indivíduo.
- Outras biométricas humanas: outras técnicas que podem aparecer incluem reconhecimento de voz (útil sobretudo em interceptações ou atendimento de emergência –por exemplo, identificar pelo timbre se uma chamada ao 190 foi feita por determinada pessoa reincidente em trotes, ou comparar voz de sequestradores em gravações) e reconhecimento de marcha e porte físico (a forma de andar, usada para identificar indivíduos mesmo quando o rosto não está visível).

Para Identificação de Veículos

- Reconhecimento automático de placas: câmeras especiais ou comuns com software específico capturam a imagem da placa e um algoritmo de Reconhecimento Óptico de Caracteres (OCR – *Optical Character Recognition*) extrai a sequência alfanumérica. Esse dado é confrontado automaticamente com bases, como o do DENATRAN/RENAVAM (Departamento nacional de Trânsito/Registro Nacional de Veículos Automotores), e listas de interesse policial (veículos roubados, clonados ou envolvidos em crimes).
- Identificação por características do veículo: complementar ao reconhecimento automático de placas, sistemas modernos empregam algoritmos de visão computacional para identificar marca, modelo e cor do veículo capturadas pela câmera. Isso é útil especialmente se a placa estiver encoberta ou em caso de veículos com “dublês” (mesma placa em carros de modelo diferente). Através de redes neurais treinadas com milhares de imagens, o software pode apontar: “veículo do alerta é da “marca X”, “modelo Y” e “cor Z”, ano aproximado “XYZW”. Assim, mesmo que a placa não seja lida, a polícia tem uma descrição para buscar. Alguns projetos classificam também características como presença de bagageiro, adesivos, avarias – que ajudam na identificação visual.

Sistemas de armazenamento e cruzamento de dados

As tecnologias citadas nos itens anteriores alimentam e consultam bases de dados integradas. O coração de um sistema biométrico de segurança é o conjunto de bases, cruzamento e correlação (*matching*). Alguns componentes importantes:

- Banco de Dados Biométrico Central: armazena os *templates* e dados brutos (impressões digitais escaneadas, fotos de rosto e eventualmente íris). Esses bancos precisam de redundância (backup em tempo real) e altas medidas de segurança. É essencial a criptografia dos *templates* e controles rígidos de acesso;
- Base(s) de pessoas de interesse (*Watchlists*): para uso eficiente de reconhecimento facial e outras características, normalmente configurando-se listas restritas de interesse: por exemplo, lista de indivíduos procurados pela justiça, lista de presos foragidos, lista de desaparecidos, entre outras. Essas listas são extraídas do banco central, mas funcionam como filtros: as câmeras faciais urbanas não precisam comparar cada rosto com milhões de cidadãos sem pendências – isso seria ineficiente e invasivo. Em vez disso, comparam com uma lista de pessoas na *watchlist*;
- Integração com bases externas: além do banco biométrico em si, o poder do sistema reside em cruzar informações de diferentes fontes. Por exemplo, ao identificar uma pessoa, o sistema pode puxar automaticamente seus antecedentes criminais de outro banco de dados e apresentar ao policial um resumo. Ou, ao detectar um veículo, já trazer dados do proprietário, endereço registrado e possíveis relação com crimes (por exemplo, o proprietário tem passagem por tráfico);
- Ferramentas analíticas e *Data Mining* (mineração de dados): com a massa de dados coletada (logs de onde cada pessoa foi vista, placas capturadas com horas e locais), os sistemas frequentemente incluem módulos de análise para a produção de inteligência.

5.4 Vigilância Baseada em Veículos Aéreos não Tripulados (VANTs)

A vigilância baseada em VANTs equipados com câmeras e sensores oferece consciência situacional, auxiliando operações de monitoramento, busca, resgaste ou perseguições, reduzindo riscos humanos. As informações obtidas dessas imagens estendem o alcance dos policiais, fornecendo informações em tempo real ou realizando tarefas de alto risco humano, como o monitoramento de espaços públicos com grandes multidões, investigação de cenas contaminadas e desativação de bombas.

A utilização de drones embarcados com câmeras de alta resolução e sensores térmicos aumentam a capacidade de monitoramento aéreo e terrestre em tempo real. As câmeras de alta resolução proporcionam imagens nítidas e detalhadas, essenciais para o monitoramento visual durante patrulhas, eventos críticos ou situações de risco. Ela pode ser usada para capturar imagens de grande alcance, como em áreas de grande fluxo de pessoas ou regiões extensas, permitindo o reconhecimento de indivíduos, veículos e atividades suspeitas.

Essas câmeras podem ser integradas com software de reconhecimento de padrões, como sistemas biométricos para reconhecimento facial ou leitura de placas, permitindo a identificação rápida de pessoas ou veículos procurados.

Os sensores térmicos equipados nos drones permitem a detecção de calor, o que torna o monitoramento efetivo em condições de baixa visibilidade, como períodos noturnos ou em áreas com obstrução visual, como densas florestas ou áreas urbanas com grande volume de edifícios.

Sensores térmicos são particularmente valiosos para identificar movimentações suspeitas, como pessoas em fuga ou veículos estacionados fora do horário usual, sendo capazes de detectar fontes de calor mesmo em ambientes escuros ou cobertos por fumaça.

Implantação da Tecnologia de VANTs

Primeiramente, desenvolve-se um plano de implantação detalhado, que inclua procedimentos operacionais padrão (POP) para uso dos Veículos Aéreos não Tripulados (VANTs) em diferentes cenários (patrulhamento, ocorrências em andamento, resgate, entre outros).

Esses procedimentos definem quando e como acionar um drone, altitudes e áreas de voo permitidas em ambiente urbano, regras de engajamento (se o drone apenas observa ou pode intervir de outras formas, como uso de alto-falante) e protocolos de comunicação com as equipes terrestres.

Convém que o órgão interessado em implementar drones consulte a assessoria jurídica e as normativas pertinentes, elaborando um protocolo de adequação legal. Também é recomendável dialogar com órgãos de controle e a comunidade, a fim de gerar transparência e legitimação do projeto[7].

A orientação técnica da implantação envolve escolher os equipamentos e sistemas adequados às necessidades. Deve-se realizar um estudo de viabilidade técnica, considerando quais tipos de drones melhor atendem às missões urbanas previstas (multirrotores costumam ser mais ágeis em perímetros urbanos confinados, enquanto modelos de asa fixa cobrem áreas maiores em patrulha de fronteiras urbanas ou zonas rurais próximas).

Definir os sensores e cargas úteis apropriados também é crucial. Por exemplo, para operações noturnas e busca de pessoas, câmeras termográficas são indispensáveis; para monitoramento de multidões em eventos, câmeras de zoom óptico poderoso e estabilização são preferíveis.

A implantação deve prever a integração dessas plataformas com os sistemas de TI existentes – idealmente, o *feed* de vídeo do drone deve ser acessível em tempo real no Centro de Operações da corporação, podendo ser gravado nos servidores para análise posterior. Assim, uma orientação é investir também em infraestrutura de recepção de dados e armazenamento seguro das imagens, alinhado às políticas de segurança da informação e à Lei Geral de Proteção de Dados (no caso de gravações que incluam pessoas identificáveis).

Aspectos Sobre a Prioridade de Aplicação de VANTs

Para maximizar o impacto positivo dos Veículos Aéreos não Tripulados (VANTs), é necessário definir locais e contextos prioritários para sua utilização na segurança pública urbana. Em termos geográficos, a adoção inicial costuma focar grandes centros urbanos e áreas com maiores índices de criminalidade, onde a cobertura aérea contínua pode coibir delitos e acelerar a resposta policial.

Por exemplo, regiões metropolitanas densas e periferias com altos indicadores de violência são candidatas iniciais, já que drones podem sobrevoar bairros de difícil patrulhamento contínuo, monitorando vias estreitas, vielas ou áreas de risco inacessíveis a viaturas. Esse olhar do alto, mesmo que remoto, amplifica a presença do Estado em locais onde infratores tradicionalmente se valem do conhecimento do terreno para escapar da polícia.

Um caso típico são comunidades ou favelas com infraestrutura labiríntica: drones têm sido utilizados para mapear rotas de fuga e vigiar acessos, reduzindo a vantagem de criminosos que antes tiravam proveito da dificuldade de navegação urbana para as viaturas.

Além das áreas de patrulhamento rotineiro, grandes eventos públicos e situações de aglomeração despontam como cenários chave para a implementação de drones. Em eventos de grande porte – como festivais, eventos esportivos ou manifestações – os drones servem como "olhos adicionais" das forças de segurança, cobrindo extensões que demandariam dezenas de câmeras fixas ou patrulhas a pé.

Com a visão panorâmica de uma praça de shows ou de um protesto, os comandantes conseguem identificar aglomerações anormais, focos de tumulto ou emergências médicas precocemente, direcionando efetivo para esses pontos antes que a situação fuja do controle.

Portanto, estádios, sambódromos, vias públicas em datas festivas e outros locais de concentração temporária de público são locais de implantação altamente recomendados para drones, em apoio às equipes no solo e às câmeras de circuito fechado (CFTV- *Closed-Circuit Television*) já instaladas nesses ambientes. Inclusive, órgãos de defesa civil também se beneficiam: em eventos ao ar livre, drones auxiliam na identificação de riscos estruturais, rotas de evacuação obstruídas ou focos de incêndio, integrando a segurança pública e a proteção civil.

Outro eixo de implantação são as operações especiais e fiscalizações urbanas. Drones podem ser úteis em missões de inteligência e investigação, operando de forma discreta para observação de suspeitos e levantamento prévio de locais de operações policiais.

Da mesma forma, em operações de repressão ao tráfico de drogas em áreas urbanas complexas, os drones proveem vigilância superior, acompanhando deslocamentos de suspeitos por becos ou telhados e guiando as guarnições em terra.

Locais como bairros com bocas de fumo ativas, "cracolândias", ou entornos de escolas em áreas vulneráveis têm sido foco desse tipo de fiscalização aérea, onde o drone atua como plataforma de vigilância silenciosa para coletar provas em vídeo e direcionar ações policiais sem alertar os criminosos.

Cabe mencionar também a aplicação em fiscalização ambiental urbana: guardas municipais e polícias ambientais das cidades podem utilizar os Veículos Aéreos não Tripulados (VANTs) para monitorar áreas de preservação invadidas, loteamentos irregulares, depósitos clandestinos de lixo e outros ilícitos ambientais urbanos, dada a facilidade de cobrir terrenos amplos e detectar mudanças no uso do solo a partir das imagens aéreas. Assim, parques urbanos, zonas de manancial, encostas e terrenos baldios extensos são locais em que a implantação de drones trouxe melhorias na fiscalização contínua.

No contexto brasileiro, muitos estados e municípios já implementaram projetos de drones na segurança urbana, oferecendo estudos de caso valiosos. A variedade geográfica desses casos confirma que a tecnologia se adapta a diferentes realidades locais – desde metrópoles, como São Paulo e Rio de Janeiro, até estados da região Norte, onde drones auxiliam tanto nas capitais quanto em municípios menores no entorno, especialmente no combate a crimes ambientais e fronteiriços.

A estratégia de locais de implantação deve ser escalonada: iniciar em áreas-piloto (por exemplo, em determinada zona urbana crítica) e gradualmente expandir para outras regiões conforme os resultados e aprendizados. Locais centrais (centros comerciais e áreas turísticas) podem ser contemplados em fases seguintes, assim como integração com projetos de Cidade Inteligente, nos quais drones operam em sinergia com câmeras inteligentes, sensores de tiro e outras tecnologias para cobrir a malha urbana.

Operação da Tecnologia de VANT

A fase de operação ou operacionalização trata de como os drones serão efetivamente usados no dia a dia das ações de segurança pública. Uma vez implementados e entregues à equipe responsável, é preciso integrá-los aos fluxos operacionais de forma coerente.

Em operações rotineiras de policiamento ostensivo, os drones podem atuar como patrulha aérea permanente em áreas pré-determinadas ou de maneira orientada por inteligência, sendo acionados para sobrevoar locais em horários de maior incidência criminal conforme análise preditiva. Essa capacidade do drone de relatar é útil para avaliar a gravidade e natureza do evento. No contexto de operações planejadas (como cumprimento de mandados, *blitz* ou incursões em áreas conflagradas), a operacionalização dos Veículos Aéreos não Tripulados (VANTs) envolve etapa prévia de preparação. Os drones podem realizar sobrevoos de reconhecimento antes do início da operação, mapeando o terreno e identificando possíveis ameaças ou alvos. As informações coletadas – número de indivíduos presentes, existências de rotas de fuga e a presença de obstáculos – contribuem para o início dos trabalhos da equipe, aumentando a consciência situacional dos policiais que entrarão em ação.

Os drones são operados remotamente ou de forma autônoma, dependendo da configuração. A operação remota envolve o controle do veículo por um operador em tempo real, enquanto o funcionamento autônomo é baseado em algoritmos predefinidos ou em resposta a comandos específicos do Centro de Comando e Controle (CCC).

A integração dos sensores e das câmeras permite a coleta contínua de imagens e dados durante as missões de patrulhamento, sendo enviados ao CCC para análise. Os drones possuem autonomia de voo variada, podendo cobrir grandes áreas sem necessidade de intervenção humana constante.

Antes de lançar um programa de drones na segurança pública, é imprescindível atender pré-requisitos que englobam aspectos legais, institucionais, técnicos e operacionais, delineados a seguir:

- **Adequação legal e normativa**: O órgão deve assegurar que o emprego de veículos aéreos não tripulados (VANTs) esteja em conformidade com as normas aeronáuticas e de privacidade vigentes. No âmbito aeronáutico, isso significa observar as regulamentações da ANAC (Agência Nacional de Aviação Civil) e do DECEA (Departamento de Controle do Espaço Aéreo) para operação de drones – incluindo registro das aeronaves, classificações de risco conforme peso/emprego, respeito a altitudes máximas e distâncias de pessoas e obtenção de autorizações de voo no espaço aéreo urbano quando aplicável;
- **Aprovação institucional e políticas internas**: é necessário que a alta administração do órgão de segurança pública aprove e patrocine formalmente o programa de drones. Isso inclui designar por escrito a unidade responsável, alocar orçamento e recursos humanos, e expedir normativas internas (portarias ou diretrizes) detalhando a utilização. Uma política interna deve contemplar objetivos do uso (finalidades permitidas, como monitoramento, resgate, entre outros), limites (por exemplo, vedação de uso de drones para vigiar manifestações pacíficas sem indicação de crime, resguardando direitos constitucionais), procedimentos de autorização de missões e responsabilidades de cada cargo;
- **Infraestrutura e recursos materiais**: inclui instalações seguras para armazenamento dos VANTs (um local para guarda dos equipamentos, baterias e peças sobressalentes, preferencialmente climatizado e com acesso controlado), e uma estação de controle adequada, como uma sala de monitoramento com monitores de vídeo, computadores com softwares de controle de voo e análise de imagens, links de comunicação dedicados e energia redundante;

  Caso a operação dos drones envolva deslocamentos pelo território (por exemplo, uso em áreas rurais ou em diversos bairros), será necessário veículo apropriado para transportá-los, possivelmente uma viatura adaptada como unidade móvel de drones equipada com antenas de reforço de sinal e espaço para um operador trabalhar.
- **Planejamento de segurança e mitigação de riscos**: por se tratar de equipamento aéreo, é preciso realizar um planejamento de gerenciamento de risco da operação de drones. Isso envolve avaliar riscos potenciais (queda do drone por falha, interferência em aeronaves tripuladas, uso indevido, ataque cibernético ao sistema de controle, entre outros) e definir medidas mitigadoras. Por exemplo, se o drone for operar sobre vias públicas, uma mitigação é manter altura mínima segura e ter área livre para queda em caso de emergência (o Departamento de Controle do Espaço Aéreo, DECEA, prevê isso em suas normativas).

O órgão deve possuir um seguro ou fundo de cobertura para eventuais danos causados por acidentes com drones, conforme exigido pela ANAC (Agência Nacional de Aviação Civil) para certos tipos de operação. Também deve ser previsto as redundâncias de comunicação (ter frequências alternativas ou link de celular para comando do drone caso haja interferência no link principal) e procedimentos de emergência por escrito (como proceder se um drone apresentar falha de motor – alguns modelos executam retorno automático ao ponto de decolagem, mas o operador deve estar preparado para contingências).

Equipe Responsável

A implantação bem-sucedida de drones na segurança pública requer a definição clara da equipe responsável pela gestão e operação dos Veículos Aéreos não Tripulados (VANTs). Recomenda-se a criação (ou designação) de uma unidade especializada dentro do órgão de segurança para concentrar essa responsabilidade, por exemplo, a Polícia Militar do Paraná centralizou a fiscalização e doutrina de uso de drones em seu Batalhão de Operações Aéreas (BPMOA), o que assegurou padronização de procedimentos e ações mais seguras e eficientes[16]. A composição da equipe é multidisciplinar, sendo necessários pilotos remotos certificados, devidamente treinados conforme as normas da autoridade de aviação civil. A legislação brasileira já exige que operadores de drones de segurança pública sejam capacitados e credenciados[7], garantindo conhecimento técnico e de segurança de voo.

Juntamente a esses pilotos, costuma-se designar observadores de voo (*spotters*) quando necessário, que auxiliam na manutenção do contato visual e na observação do espaço aéreo ao redor, aumentando a segurança das operações. Outro profissional são os analistas de inteligência ou imagem, responsáveis

por monitorar em tempo real as transmissões de vídeo dos drones e interpretar as informações para repassá-las às equipes táticas ou aos centros de comando. Esses analistas convertem dados brutos (imagens aéreas) em orientações úteis – por exemplo, identificando movimentações suspeitas, locais de risco ou pessoas desaparecidas avistadas na filmagem.

Por fim, faz-se necessária a formação continuada dessa equipe. A tecnologia de VANTs evolui rapidamente, de modo que treinamentos periódicos, simulados de missão e atualização sobre novas funcionalidades (como novos modos de voo autônomo ou análise de dados) devem ser fornecidos aos integrantes.

Tecnologias Envolvidas

A execução de operações com drones na segurança urbana apoia-se em um conjunto de tecnologias[24], englobando tanto os equipamentos aéreos em si quanto os sistemas de apoio e de processamento de dados. Dentre as principais tecnologias envolvidas, pode-se citar as que seguem.

Plataformas de VANT (hardware aéreo)

São as aeronaves remotamente pilotadas propriamente ditas. Na segurança urbana, predominam os drones de múltiplos rotores (multirrotores), especialmente quadricópteros ou hexacópteros, devido à sua capacidade de pairar e manobrar em espaços confinados. Esses drones típicos podem decolar e pousar verticalmente em áreas reduzidas (até mesmo do topo de viaturas) e oferecem boa estabilidade para filmagens.

Em algumas aplicações específicas, utilizam-se VANTs de asa fixa (semelhantes a pequenos aviões) ou modelos híbridos, que possuem maior autonomia de voo e alcance – úteis para vigilância de extensas áreas periurbanas ou rurais (patrulhamento de rodovias, por exemplo).

Os VANTs modernos são construídos com materiais compostos leves e resistentes e trazem incorporadas tecnologias como GPS de alta precisão para navegação e manutenção de posição. Muitos dispõem de sistemas de estabilização e piloto automático avançados, que permitem ao drone pairar parado mesmo sob ação de vento ou realizar rotas predefinidas de forma autônoma. Tais avanços resultaram em drones com voos mais longos e maior alcance de missão, consolidando-os como ferramentas essenciais em diversos setores, inclusive segurança[18].

Sensores e cargas úteis embarcadas

A eficácia dos drones na segurança pública provém em grande medida de seus sensores de bordo, responsáveis por coletar informações do ambiente. O principal sensor é a câmera de vídeo de alta resolução, geralmente no espectro visível, montada em um gimbal (suporte estabilizado) que permite obter imagens nítidas mesmo com movimento. Essas câmeras podem dar zoom óptico e muitas gravam em resolução HD ou 4K, garantindo detalhes suficientes para identificar pessoas, placas de veículos e outros elementos importantes. Além das câmeras diurnas, uma tecnologia crucial são as câmeras termográficas (infravermelho), capazes de detectar assinaturas de calor de corpos e objetos. Elas permitem vigilância noturna e localização de indivíduos escondidos ou camuflados em vegetação densa ou à noite, pois captam o calor emitido pelo corpo humano.

Outros sensores que podem compor as cargas úteis incluem

Câmeras em espectro infravermelho próximo (úteis para identificar vestígios, como sangue, em cenas de crime), scanner a laser (para mapear em 3D terrenos ou estruturas desabadas, apoiando planejamento de resgate) e alto-falantes ou sirenes (para difusão de avisos sonoros à população ou intimar suspeitos a se renderem). Alguns drones destinados à polícia podem carregar pequenos lançadores de agentes não letais (spray de pimenta, por exemplo) ou dispositivos de iluminação (holofotes para iluminar um local à noite).

Sistemas de comunicação e transmissão

Para que as imagens e comandos fluam entre o drone e a equipe, entra em cena a tecnologia de comunicação sem fio. Os drones utilizam enlaces de rádio para telemetria e controle – tipicamente em frequências dedicadas ou, em sistemas mais avançados, via redes. A tecnologia de transmissão de vídeo em tempo real (*downlink*) é crucial. Os drones empregam protocolos digitais que enviam vídeo quase sem latência para o operador a quilômetros de distância.

Também é relevante a questão de comunicação entre os membros da equipe de drone e as equipes em solo: aqui emprega-se a rede de rádio digital da polícia ou bombeiros, integrando o piloto no despacho normal, ou aplicativos seguros de comunicação em dispositivos móveis para troca de informações e imagens.

Software de controle, gestão e análise

Há softwares de controle de voo instalados nos computadores ou tablets dos pilotos, oferecendo interfaces com mapas, telemetria (posição GPS, altitude, bateria, entre outras informações) e até rotas automatizadas. Tecnologias de piloto automático permitem que o operador defina pontos de interesse ou trajetória pré-programada e o drone voe autonomamente por eles – recurso útil para vigilância de rotina (por exemplo, sobrevoar perímetro de um parque diariamente às 18h).

Ferramentas de análise de vídeo baseada em IA já começam a ser utilizadas com algoritmos capazes de detectar comportamentos suspeitos em tempo real, identificar automaticamente um veículo ou pessoa específica nas imagens ou até acoplar reconhecimento facial. Há outros softwares que, por exemplo, podem identificar placas de veículos procurados ao sobrevoar estacionamentos ou contar automaticamente a quantidade de pessoas em uma praça para detectar aglomerações anômalas.

Outra tecnologia de software envolvida é a de geoprocessamento e mapeamento: imagens capturadas pelos drones podem ser processadas para gerar ortomosaicos (mapas aéreos atualizados) de uma cena de crime ou desastre, auxiliando na perícia ou no planejamento de resgastes.

Aplicativos de realidade aumentada também começam a surgir, permitindo que agentes em campo, via óculos ou tablets, vejam em tempo real a posição do drone e os pontos de interesse que ele destaca (por exemplo, o drone marca virtualmente onde está um suspeito escondido e o agente vê essa marcação sobreposta ao cenário real através do dispositivo).

Tecnologias de suporte e sustentação

Estações meteorológicas portáteis ou aplicativos de meteorologia são usados para consultar em tempo real as condições do vento e clima, já que rajadas de vento forte, chuva ou outras condições podem impedir ou limitar voos (drones têm parâmetros específicos de tolerância meteorológica).

Tecnologias de rastreamento de tráfego aéreo também são integradas com o receptor dos drones ou a coordenação via sistemas do DECEA - Departamento de Controle do Espaço Aéreo – para assegurar que o drone não conflite com aeronaves tripuladas, especialmente próximas a aeroportos.

Outro exemplo de tecnologia é o uso de inteligência artificial embarcada. Alguns drones avançados possuem chips de AI a bordo que lhes dão autonomia para desviar de obstáculos automaticamente, seguir alvos marcados pelo operador ou retornar para casa ao detectar bateria baixa. Essas funcionalidades derivam de algoritmos de visão computacional e aprendizado de máquina incorporados no firmware das aeronaves.

5.5 Ambientes Multissensoriais

O monitoramento por multissensores consiste na utilização integrada de diversos tipos de dispositivos de coleta de dados para vigilância, análise e resposta em ambientes urbanos.

Essa abordagem ultrapassa os sistemas tradicionais de monitoramento, incorporando múltiplas camadas de sensores que captam diferentes dimensões da realidade urbana.

Os principais componentes desse sistema são apresentados na Tabela 5.2.

Tabela 5.2 – Principais componentes em ambientes multissensoriais

COMPONENTE	FINALIDADE
Câmeras de vigilância	Formam a espinha dorsal do sistema, fornecendo imagens em tempo real de áreas monitoradas.
Sensores de áudio	Microfones capazes de detectar sons específicos como disparos de armas, explosões, gritos ou quebra de vidros, acionando alertas em tempo real.
Sensores térmicos	Câmeras infravermelhas que captam assinaturas de calor, permitindo vigilância em condições de baixa visibilidade e detecção de pessoas ou veículos em áreas restritas.
Radares	Utilizados para monitorar velocidade, fluxo e presença de veículos, ou detectar movimentos em áreas amplas, mesmo em condições climáticas adversas.
Sistemas biométricos	Tecnologias de reconhecimento facial, digital ou comportamental que auxiliam na identificação de pessoas em espaços públicos.
Sensores ambientais	Monitoram qualidade do ar, níveis de ruído, radiação e outros parâmetros que podem indicar situações de risco.

Sistemas de multissensores representam uma aplicação concreta do conceito de cidades inteligentes, que utilizam Tecnologias de Informação e Comunicação (TICs) como agentes de transformação no meio urbano. Estas tecnologias proporcionam dados em tempo real que, quando processados de forma integrada, permitem respostas mais eficientes.

A principal motivação para implantação de sistemas multissensoriais é o combate efetivo à criminalidade urbana. Estes sistemas permitem:

- **Detecção precoce de atividades suspeitas:** A combinação de diferentes sensores aumenta significativamente a capacidade de identificar comportamentos anômalos antes que crimes ocorram;
- **Resposta mais rápida a ocorrências:** A integração com centrais de comando permite o acionamento imediato das forças de segurança mais próximas;
- **Maior cobertura territorial:** A diversidade de sensores permite monitorar áreas mais amplas e com diferentes características;
- **Evidências de melhor qualidade:** Múltiplas fontes de dados fornecem evidências mais robustas para investigações e processos judiciais.

Além do enfrentamento à criminalidade, os sistemas multissensoriais podem ser essenciais para:

- **Monitoramento de infraestruturas críticas:** Prevenção de acidentes e sabotagens em instalações estratégicas;
- **Segurança em grandes eventos:** Monitoramento de multidões e detecção precoce de situações de risco.

Na aplicação de ambientes multissensoriais, há áreas prioritárias e infraestrutura críticas.

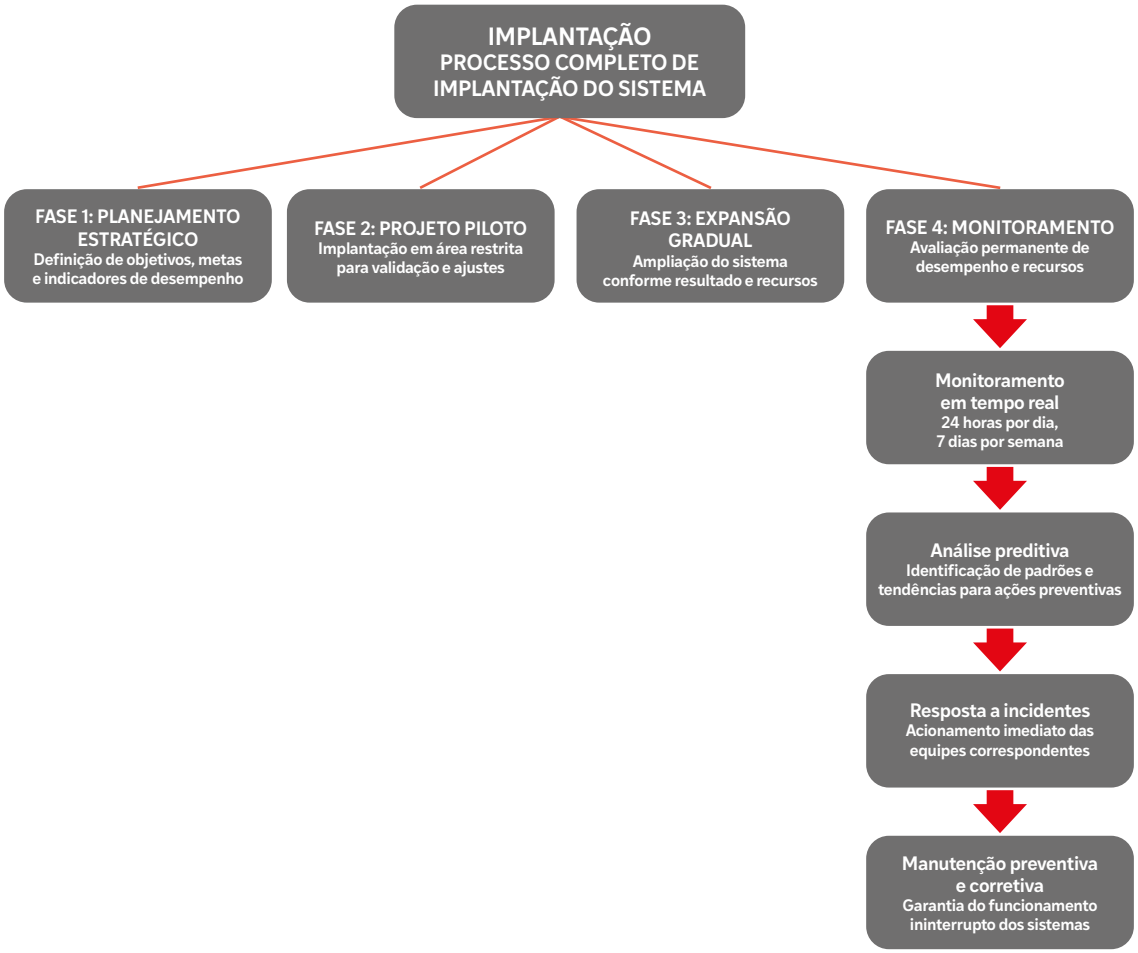
- **Áreas prioritárias**
  - Áreas com maior incidência criminal: baseando-se em estatísticas e mapeamento de crimes;
  - Centros urbanos e comerciais: locais com grande circulação de pessoas e atividade econômica;
  - Vias públicas estratégicas: principais avenidas, rotas de fuga e corredores de transporte;
  - Entornos de escolas e hospitais: garantindo segurança em áreas sensíveis.
- **Infraestruturas críticas**
  - Estações de tratamento de água e esgoto: proteção de serviços essenciais;
  - Terminais de transporte público: rodoviárias, estações de metrô e aeroportos;
  - Prédios públicos: sedes administrativas, tribunais e outros edifícios governamentais.

Implantação de Ambientes Multissensoriais

As fases de implantação da tecnologia estão descritas abaixo e visualizadas na Figura 5.10.

- **Fase 1 - Planejamento estratégico:** definição de objetivos, metas e indicadores de desempenho.
- **Fase 2 - Projeto Piloto:** implantação em área restrita para validação e ajustes.
- **Fase 3 - Expansão gradual:** ampliação do sistema conforme resultados e disponibilidade de recursos.
- **Fase 4 - Monitoramento contínuo e avaliação permanente do desempenho e adequação do sistema**:
  - Monitoramento em tempo real: 24 horas por dia, 7 dias por semana;
  - Análise preditiva: identificação de padrões e tendências para ações preventivas;
  - Resposta a incidentes: acionamento imediato das equipes correspondentes;
  - Manutenção preventiva e corretiva: garantia do funcionamento ininterrupto dos sistemas.

Figura 5.10 – Organograma da implantação de ambientes multissensoriais



Fonte: Autores, 2025

A implantação de ambientes multissensoriais deve considerar o que segue.

Infraestrutura Tecnológica

- Rede de sensores: instalação estratégica dos diversos tipos de sensores pela cidade.
- Rede de comunicação: estrutura robusta para transmissão de dados em tempo real.
- Central de processamento: servidores e sistemas para armazenamento e análise de dados.
- Software de integração: plataformas que unificam informações de diferentes fontes.

Gestão de Dados e Informações

- Coleta e agregação: captura e organização de dados dos diferentes sensores.
- Processamento em nuvem: utilização de computação em nuvem para análise de grandes volumes de dados, similar ao que acontece com imagens de sensoriamento remoto.
- Análise em tempo real: identificação imediata de situações que exigem intervenção.
- Armazenamento seguro: proteção dos dados contra acessos não autorizados, considerando aspectos de segurança cibernética.

Aspectos Legais e Éticos

- Conformidade com legislação: respeito às leis de proteção de dados e privacidade.
- Protocolos de uso: definição clara de quem pode acessar os dados e em quais situações.
- Transparência: informação à população sobre a existência e finalidade dos sistemas.
- Auditoria independente: verificação periódica do uso adequado das tecnologias.

Equipe Responsável

Os principais atores incluem: polícia militar, responsável pelo policiamento ostensivo e resposta imediata a ocorrências, polícia civil, utiliza dados dos sensores para investigações, e guarda municipal, atuação local e específica em áreas de responsabilidade municipal.

Os gestores públicos e técnicos geralmente são as secretarias de segurança pública, responsáveis pelo planejamento e coordenação das equipes técnicas, profissionais de TI, analistas de dados e especialistas em segurança, e operadores, profissionais que monitoram os sistemas em tempo real.

A participação social, como a comunidade, beneficiária direta e participante ativa através de canais de comunicação com o sistema, empresas de tecnologias, fornecendo equipamentos e sistemas e realizando as manutenções, e instituições acadêmicas, com pesquisa e desenvolvimento de melhorias e novas soluções.

5.6 Considerações sobre o uso de Tecnologias digitais

A integração de tecnologias digitais nos sistemas de segurança pública representa uma oportunidade transformadora para os municípios do Estado de São Paulo, permitindo que enfrentem os complexos desafios da urbanização, do aumento da criminalidade e do gerenciamento de emergências com eficiência e precisão sem precedentes. Tecnologias como videovigilância inteligente, câmeras corporais, biometria, drones, ambientes multissensoriais, análise de dados impulsionada por Tecnologia da Informação (IA), Centros de Comando e Controle (CCCs), Sistema de Posicionamento Global (GPS), *blockchain* e computação de borda (*edge computing)* não são apenas ferramentas, mas pilares de um ecossistema moderno de cidades inteligentes. Essas soluções, como demonstrado pelo Programa Muralha Paulista – que reduziu crimes nas rodovias em 15% por meio de sistemas integrados de câmeras e IA[20] – oferecem benefícios tangíveis na prevenção de crimes, resposta rápida e coleta de evidências, alinhando-se com as tendências globais em segurança urbana[19].

No entanto, a adoção bem-sucedida dessas tecnologias depende da superação de desafios críticos. Primeiro, são essenciais investimentos em infraestrutura, especialmente em redes de alta velocidade (5G e fibra óptica) e sistemas seguros de armazenamento de dados, para suportar o processamento e transmissão de dados em tempo real. O treinamento contínuo de forças policiais, operadores técnicos e analistas de dados é vital para garantir o uso eficaz de ferramentas avançadas, como IA e biometria.

A conformidade legal permanece como um pilar fundamental da implantação, especialmente o cumprimento da Lei Geral de Proteção de Dados (LGPD)[30], que exige medidas rigorosas de proteção de dados para informações biométricas e de vigilância. Regulamentações como o Decreto nº 10.777/2021 (Ver Anexo A, Tabela A.1.1) e a Lei n° 12.965/2014 (Ver Anexo A, Tabela A.1.1) reforçam a importância de alinhar o uso da tecnologia com padrões éticos e legais para manter a confiança pública[31,32]. O uso de *blockchain* para integridade de

provas, testado pela Secretaria de Segurança Pública do Estado de São Paulo (SSP-SP), exemplifica como a conformidade pode aumentar a confiabilidade judicial[22]. Além disso, a transparência, facilitada por câmeras corporais, contribui para a redução de reclamações contra policiais, fortalecendo a confiança da comunidade[21].

No futuro, a convergência entre Inteligência Artificial (IA), *Big Data* e Internet das Coisas (IoT) promete elevar a segurança urbana a novos patamares, permitindo polícia preditiva e alocação dinâmica de recursos[26]. No entanto, esse futuro exige investimento contínuo em cibersegurança para proteger contra violações de dados e garantir a resiliência dos sistemas, além de avaliação constante para adaptar as tecnologias a ameaças em evolução[27]. Drones e sistemas multissensoriais podem reduzir incidentes em rodovias, destacando o potencial de soluções escaláveis em diversos contextos[22,25].

Iniciativas bem-sucedidas, como o Muralha Paulista, são exemplos de que os municípios de São Paulo podem transformar a segurança pública em um alicerce do desenvolvimento urbano. O caminho a seguir exige colaboração entre formuladores de políticas, forças de segurança, tecnólogos e cidadãos para garantir que os avanços tecnológicos se traduzam em comunidades equitativas, seguras e sustentáveis.

Referências Bibliográficas

1. RISTVEJ, J.; LACINÁK, M.; ONDREJKA, R. **On Smart City and Safe City Concepts**. **Mobile** Networks and Applications, v. 25, 836–845, Feb. 2020. https://doi.org/10.1007/s11036-020-01524-4.

2. MYAGMAR-OCHIR, Y.; KIM, W. **A survey of video surveillance systems in smart city**. Electronics, v. 12, n. 17, art.3567, 2023. https://doi.org/10.3390/electronics1217356.

3. ALAHI, M. E. E. *et al.* **Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: Recent advancements and future trends**. Sensors, v. 23, n. 11, art. 5206, 2023. https://doi.org/10.3390/s23115206.

4. SANTAMARIA, A. F.; RAIMONDO, P.; TROPEA, M.; RANGO, F.; AIELLO, C. **An IoT surveillance system based on a decentralised architecture**. Sensors, v. 19, n. 6, art. 1469, 2019. https://doi.org/10.3390/s19061469.

5. SONGTHAI, M.; YANYONG, S.; KONGHUAYROB, P.; SAENGMANEE, P.; KAITWANIDVILAI, S. **Smart police systems: Enhancing urban safety through AI-powered surveillance and edge computing**. 2025. (Preprints). https://doi.org/10.20944/preprints202502.1171.v1.

6. JEON, H.; KIM, H.; KIM, D.; KIM, J. **PASS-CCTV: Proactive Anomaly surveillance system for CCTV footage analysis in adverse environmental conditions**. Expert Systems with Applications International Journal, v. 254, n. C, 2024. https://doi.org/10.1016/j.eswa.2024.124391.

7. DICKENS, C.; BOYNTON, P.; RHEE, S. **Principles for designed-in security and privacy for smart cities**. *In:* SCOPE 2019 WORKSHOP INTERNATIONAL SCIENCE OF SMART CITY OPERATIONS AND PLATFORMS ENGINEERING, 4., Montreal, 2019. Proceedings [...]. New York: ACM, 2019.

8. MARES, D. **Problem-oriented guides for police response guide series nº 14 gunshot detection reducing gunfire through acoustic technology**. [*S.l.*]: Bureau of Justice Assistance, 2022. **https://bja.ojp.gov/**

9. CUTLER, M. **Development of predictive policing technology and justification for use**. Ann Arbor: University of Michigan, 2024.

10. HUNG, V.; BABIN, S.; COBERLY, J. **A primer on body worn camera technologies.** Howard: Johns Hopkins University, Applied Physics Laboratory, 201.

11. HUNG, V.; BABIN, S.; COBERLY, J. **A market survey on body worn camera technologies**. Howard: Johns Hopkins University, Applied Physics Laboratory, 2013.

12. INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE. **Body-worn cameras**. Alexandria, VA: IACP, 2019).

13. MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Portaria nº 648/2024. **Estabelece diretrizes sobre o uso de câmeras corporais pelos órgãos de segurança pública**. Brasília: MJSP, 2024.

14. VELTMEIJER, E.; FRANKEN, M.; GERRITSEN, C. Real-time violence detection and localization through subgroup analysis. **Multimedia Tools and Applications,** v. 84, p. 3793-3807, May 2024. https://doi.org/10.1007/s11042-024-19144-5.

15. RAVI, S.; CLIMENT-PÉREZ, P.; FLOREZ-REVUELTA, F. A review on visual privacy preservation techniques for active and assisted living. **Multimedia Tools and Applications**, v. 83 14715–14755 July 2024. https://doi.org/10.1007/s11042-023-15775-.

16. MARTY, O. L. Uso de aeronaves remotamente pilotadas pela inteligência policial militar no combate aos crimes violentos contra o patrimônio. **Revista de Ciências Policiais**, v. 42, 2022

17. LIMA, R. S. **As câmeras corporais na Polícia Militar do Estado de São Paulo**: processo de implementação e impacto nas mortes de adolescentes. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. 40 p.

18. RIGO, R. G. **Desenvolvimento de sistema de monitoramento do estado de carga de baterias para uso em drones.** TCC (Graduação) - Universidade de Caxias do Sul, 2022. Disponível em: https://repositorio.ucs.br/xmlui/handle/11338/11152. Acesso em: 10 de abril de 2025

19. Zhenfeng; CAI, Jiajun; WANG, Zhongyuan. **Smart monitoring cameras driven intelligent processing to big surveillance video data.** IEEE Transactions on Big Data, v. 4, n. 1, p. 105-116, 2017.

20. SÃO PAULO (Estado). **Programa muralha paulista**. 2024. Disponível em: https://www.ssp.sp.gov.br/muralha-paulista. Acesso em: 21 fev. 2025.

21. MASKALY, Jon et al. **The effects of body-worn cameras (BWCs) on police and citizen outcomes: A state-of-the-art review**. Policing: An International Journal of Police Strategies & Management, v. 40, n. 4, p. 672-688, 2017.

22. SÃO PAULO (Estado). **Relatório anual de segurança** pública. 2023. Disponível em: https://www.ssp.sp.gov.br/estatistica/relatorios. Acesso em: Acesso em: 21 fev. 2025.

23. JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. (Ed.). Handbook of biometrics. Springer Science & Business Media, 2007.

24. AL-DOSARI, Khalifa; FETAIS, Noora. **A new shift in implementing unmanned aerial vehicles (UAVs) in the safety and security of smart cities: a systematic literature review**. Safety, v. 9, n. 3, p. 64, 2023.

25. ATREY, Pradeep K.; EL SADDIK, Abdulmotaleb. **Confidence evolution in multimedia systems. IEEE Transactions on Multimedia**, v. 10, n. 7, p. 1288-1298, 2008.

26. OMAROV, Batyrkhan et al. **State-of-the-art violence detection techniques in video surveillance security systems: a systematic review**. PeerJ Computer Science, v. 8, p. e920, 2022.

27. AUTERO, Anniina; DE MORAES BATISTA SIMAO, Marcela; KARPPI, Ilari. **Smart Urban Safety and Security: Interdisciplinary Perspectives**. Springer Nature, 2025.

28. KAPLAN, Elliott D.; HEGARTY, Christopher (Ed.). **Understanding GPS/GNSS: principles and applications**. Artech house, 2017.

29. ZHANG, Qingyang et al. **Edge video analytics for public safety: A review. Proceedings of the IEEE**, v. 107, n. 8, p. 1675-1696, 2019.

30. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, **Diário Oficial da União,** Brasília, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 09 de abr. 2025

31. CEBRIAN, Fabiana SP Faraco et al. B**iometria e reconhecimento facial**. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-anpd-1.pdf. Acesso em: 02/04/2025

32. BRASIL. Decreto n° 10.777, de 24 de agosto de 2021. Institui a Política Nacional de Inteligência de Segurança Pública. **Diário Oficial da União**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10777.htm. Acesso em 14 abr. 2025.

33. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União,** Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 abr. 2025.

34. SÃO PAULO (Estado). **Governo de SP entrega sirene em áreas de risco na Grande SP.** (2023). Disponível em: https://www.agenciasp.sp.gov.br/governo-de-sp-entrega-sirene-em-areas-de-risco-na-grande-sp/. Acesso em 28 abr. 2025.

6 Segurança: Iluminação inteligente

A iluminação pública sempre desempenhou um papel fundamental na organização das cidades, inicialmente voltada à promoção da mobilidade noturna e à ampliação da sensação de segurança nos espaços urbanos. No entanto, com os avanços tecnológicos recentes e o crescimento do conceito de cidades inteligentes, esse serviço essencial vem adquirindo novas funcionalidades estratégicas.

Em sua forma mais moderna, a iluminação pública deixa de ser apenas um sistema de iluminação e passa a integrar uma rede urbana inteligente e multifuncional, capaz de interagir com sensores, câmeras, transmissores de dados, pontos de wi-fi e dispositivos para monitoramento ambiental. Segundo a *International Energy Agency*[1], a substituição de lâmpadas convencionais por LEDs, combinada à automação de sistemas de controle, pode reduzir o consumo de energia em até 50%, além de permitir respostas mais rápidas a falhas e maior durabilidade da infraestrutura. É importante considerar nesta conjuntura os requisitos técnicos e procedimentos da Portaria Inmetro nº 62, de 17 de fevereiro de 2022 (Ver Anexo A, Tabela A.1.1), que trata da certificação de luminárias para iluminação pública viária com tecnologia LED, para assegurar que os equipamentos atendam aos critérios mínimos de desempenho, durabilidade, segurança elétrica e eficiência energética.

A relação entre iluminação urbana e segurança pública é amplamente respaldada por estudos nacionais e internacionais. Pesquisas realizadas pelo *Urban Labs* da Universidade de Chicago[2] demonstraram que a melhoria da iluminação em bairros vulneráveis pode reduzir significativamente a criminalidade, com quedas de até 36% em crimes violentos em regiões onde postes com LED foram instalados. Essa redução se dá tanto pelo aumento da visibilidade, que inibe ações criminosas, quanto pela maior ocupação dos espaços públicos por moradores.

Além disso, a teoria das "janelas quebradas"[3] argumenta que ambientes urbanos negligenciados — incluindo aqueles com iluminação precária — favorecem a desordem e incentivam comportamentos antissociais. Assim, investir em iluminação pública de qualidade é também investir na valorização e cuidado com o espaço urbano, promovendo o senso de pertencimento e vigilância natural pelas comunidades.

No contexto de cidades inteligentes, a iluminação pública torna-se ainda mais estratégica. De acordo com a *International Telecommunication Union*[4], cidades inteligentes devem utilizar tecnologias digitais para melhorar a qualidade de vida, otimizar a operação dos serviços urbanos e garantir sustentabilidade para as gerações futuras. A iluminação, ao ser conectada a sensores e plataformas de dados, transforma-se em um elemento ativo dessa inteligência urbana, contribuindo não apenas para a segurança, mas também para o gerenciamento ambiental, mobilidade e conectividade cidadã. É nesse contexto que o Ato Anatel nº 17087, de 19 de dezembro de 2022 (Ver Anexo A, Tabela A.1.1), ganha importância, pois ele estabelece os requisitos técnicos para a certificação e homologação de dispositivos com funcionalidades

de telecomunicação — como rádios LoRa, NB-IoT, wi-fi e módulos 5G integrados aos postes inteligentes — garantindo que não causem interferência em outros sistemas e estejam em conformidade com as faixas de frequência regulamentadas.

Portanto, a modernização da iluminação pública não deve ser tratada apenas como uma medida de infraestrutura, mas como uma ferramenta transversal de gestão urbana inteligente, com impacto direto na segurança, na eficiência dos serviços públicos e na qualidade de vida das populações urbanas.

A segurança viária é um componente essencial da mobilidade urbana sustentável e está intrinsecamente ligada à qualidade da infraestrutura urbana, incluindo a iluminação pública. A iluminação adequada das vias públicas não apenas facilita a visibilidade para condutores, ciclistas e pedestres, mas também desempenha um papel crucial na prevenção de acidentes de trânsito.

Estudos indicam que melhorias na iluminação pública podem levar a uma redução significativa nos acidentes de trânsito, especialmente durante o período noturno. A implementação de sistemas de iluminação inteligente, que ajustam automaticamente a intensidade luminosa com base nas condições ambientais e no fluxo de tráfego, contribui para uma maior segurança nas vias, reduzindo pontos cegos e melhorando a percepção de obstáculos[5].

Além disso, a integração de tecnologias como sensores de movimento e câmeras de monitoramento permite uma resposta mais rápida a incidentes e uma gestão mais eficiente do tráfego. Esses sistemas podem detectar a presença de pedestres e ciclistas, ajustando a iluminação para garantir sua visibilidade e segurança[4].

A cidade de São José dos Campos tem se destacado na implementação de soluções de iluminação pública inteligente, visando não apenas a eficiência energética, mas também a segurança viária. Projetos locais incluem a instalação de postes equipados com sensores e sistemas de controle remoto, permitindo ajustes em tempo real da iluminação conforme a necessidade[6]. É nesse cenário que a Portaria Inmetro nº 601, de 14 de dezembro de 2023 (Ver Anexo A, Tabela A.1.1), se torna fundamental, pois ela define os critérios de avaliação da conformidade para sistemas de telegestão aplicáveis à iluminação pública, com foco em interoperabilidade, segurança cibernética e confiabilidade do sistema.

Portanto, a modernização da iluminação pública, incorporando tecnologias inteligentes, é fundamental para promover um ambiente urbano mais seguro e acessível para todos os usuários das vias, especialmente os mais vulneráveis, como ciclistas e pedestres.

A rede de postes de iluminação pública inteligente representa um ativo estratégico com enorme potencial de integração de múltiplas funcionalidades urbanas. Além das já mencionadas aplicações voltadas à segurança urbana, como sensores de presença, botões de pânico e câmeras integradas, novas soluções vêm sendo incorporadas ao ecossistema urbano digital para ampliar a eficiência, sustentabilidade e inteligência das cidades.

Entre essas possibilidades, destacam-se:

- **Postes de Iluminação Inteligente com Sensores Integrados**: equipados com sensores de movimento, luminosidade, temperatura e som, permitem adaptação em tempo real da iluminação e coleta de dados ambientais urbanos;
- **Câmeras de Monitoramento Integradas à Iluminação:** as câmeras acopladas aos postes possibilitam videomonitoramento de vias públicas, inibindo delitos e auxiliando ações de segurança e fiscalização;
- **Iluminação Responsiva por Presença**: a luz se intensifica automaticamente ao detectar a presença de pessoas ou veículos, economizando energia em horários de pouco movimento;
- **Iluminação com Botão de Pânico Integrado**: postes equipados com botões de emergência permitem que cidadãos acionem rapidamente serviços de segurança em situações de risco;
- **Análise de Dados e Inteligência Artificial (IA)**: aplicada à Iluminação Pública Algoritmos de IA processam dados em tempo real para otimizar o uso da iluminação, prever falhas e propor ajustes automáticos baseados em padrões de uso;

- **Postes Multiuso com wi-fi, Iluminação e Comunicação de Emergência:** além da função de iluminação, servem como pontos de acesso à internet e de comunicação direta com serviços de emergência;
- **Geolocalização e Mapeamento de Iluminação Deficiente:** utilizam sistemas de georreferenciamento para identificar e monitorar áreas com falhas ou necessidade de reforço na iluminação, otimizando manutenções;
- **Estacionamento Inteligente:** sensores nos postes detectam e informam em tempo real a ocupação de vagas públicas, facilitando a busca por estacionamento e reduzindo congestionamentos;
- **Gestão de Resíduos com Sensores**: lixeiras inteligentes conectadas à rede dos postes monitoram o volume de resíduos e informam a necessidade de coleta, otimizando rotas e recursos;
- **Estacionamento inteligente:** sensores instalados em vagas públicas permitem a detecção em tempo real de disponibilidade, reduzindo o tempo de busca por estacionamento e contribuindo para a fluidez do tráfego[7];
- **Gestão inteligente de resíduos sólidos:** sensores em lixeiras monitoram os níveis de ocupação, otimizando rotas de coleta e evitando transbordamentos, o que aumenta a eficiência operacional e a limpeza urbana[8];
- **Monitoramento da saúde estrutural:** postes e dispositivos conectados podem ser equipados com sensores que avaliam vibrações e tensões em edifícios, pontes e monumentos históricos, auxiliando na detecção precoce de riscos[9];
- **Qualidade do ar e condições ambientais:** sensores ambientais acoplados à infraestrutura de iluminação monitoram índices de poluição, temperatura, umidade e ruído, fornecendo dados fundamentais para políticas públicas e alerta à população[10];
- **Gestão adaptativa do tráfego:** por meio de dados de sensores e câmeras, a iluminação pública pode colaborar com o gerenciamento em tempo real do tráfego, sinalizando rotas alternativas e ajudando a mitigar congestionamentos[11];
- **Cibersegurança e resiliência digital:** à medida que mais dados trafegam pela rede urbana, torna-se essencial incorporar protocolos de segurança digital robustos que protejam tanto a integridade dos dados quanto o funcionamento das infraestruturas críticas[12];
- **Previsão de tráfego com Inteligência Artificial (IA):** modelos preditivos com base em IA podem antecipar picos de fluxo e adaptar a intensidade da iluminação para maior segurança e menor consumo de energia[13];
- **Postes com estações de recarga para veículos elétricos:** alguns projetos já integram infraestrutura de iluminação e carregamento de veículos, ampliando a funcionalidade do mobiliário urbano e incentivando a mobilidade sustentável[14];
- **Avaliação de confiabilidade dos sensores e dispositivos físicos:** o monitoramento contínuo dos próprios sistemas de iluminação permite identificar falhas, otimizar manutenções e reduzir custos operacionais[5];
- **Integração com sistemas de gerenciamento urbano centralizado:** a interligação dos postes inteligentes com centros de comando urbanos viabiliza respostas mais rápidas e decisões baseadas em dados, fortalecendo a governança urbana[15];
- **Uso de energia renovável:** postes alimentados por energia solar ou eólica contribuem para a neutralidade de carbono e demonstram o compromisso das cidades com a sustentabilidade[6].

Este capítulo do Caderno Técnico Segurança abordará diretamente os sete primeiros itens elencados no parágrafo anterior. A Figura 6.1 mostra o esquema dos sistemas para iluminação no que diz respeito a segurança.

Figura 6.1 – Esquema visual dos sistemas digitais para iluminação em cidades inteligentes

(Fonte: Imagem gerada por Chatgpt em 18/04/2025).

6.1 Postes de Iluminação Inteligente com Sensores Integrados

Os postes de iluminação inteligente são estruturas multifuncionais equipadas com sensores e conectividade via Internet das Coisas (IoT). Seu principal diferencial é operar de forma autônoma e integrada ao ambiente urbano, contribuindo para a segurança, eficiência energética e gestão inteligente da cidade[16].

Esses postes podem incluir:

- Sensores de movimento, que ajustam a iluminação conforme a presença de pessoas ou veículos, economizando energia e aumentando a segurança;
- Sensores ambientais, que monitoram temperatura, umidade, ruído e qualidade do ar, gerando dados úteis para políticas de saúde e meio ambiente;
- Câmeras com inteligência artificial, que fazem vigilância em tempo real e emitem alertas automáticos;
- Conectividade remota, por redes como wi-fi, 5G, LoRa, Zigbee ou NB-IoT, permitindo controle à distância via plataformas na nuvem;
- Análise de dados e manutenção preditiva, que detectam falhas e otimizam o consumo com apoio de algoritmos inteligentes.

A adoção dessa tecnologia traz benefícios significativos para os municípios:

- Economia de energia de até 70%, com o uso de LEDs e sensores inteligentes[1];
- Redução da criminalidade, com iluminação responsiva e monitoramento contínuo[17];
- Manutenção automatizada, com alertas de falhas em tempo real, reduzindo custos operacionais;
- Geração de dados urbanos, essenciais para o planejamento baseado em evidências;
- Integração com outros serviços públicos, como mobilidade, segurança e meio ambiente.

A instalação de postes inteligentes é estratégica para a transformação digital dos municípios. Além de reduzir custos e melhorar a segurança, transforma a iluminação pública em um ponto de coleta e análise de dados, fundamental para a construção de cidades mais inteligentes, seguras e eficientes.

Equipe Responsável

Khemakhem e Krichen[16] destacam a importância do engajamento de intervenientes para superar desafios técnicos e regulatórios. No Brasil, a Resolução Normativa ANEEL nº 414/2010 atribui aos municípios a responsabilidade pela iluminação pública, enquanto a LGPD regula a proteção de dados.

A adoção de postes inteligentes envolve diferentes agentes públicos e privados. O papel principal cabe às prefeituras municipais, que devem coordenar o planejamento urbano, garantir o alinhamento com planos diretores e mobilizar recursos por meio de políticas públicas, editais ou parcerias. Para isso, é essencial o envolvimento das equipes técnicas responsáveis pela infraestrutura urbana e mobilidade, incluindo órgãos de trânsito como as Companhias de Engenharia de Tráfego (CETs), a fim de assegurar a integração funcional dos sistemas com a malha urbana existente.

Concessionárias de energia elétrica e operadores de iluminação pública também têm papel fundamental, especialmente quando atuam sob regime de concessão, pois detêm a infraestrutura básica e o know-how técnico necessário para a gestão do sistema. Já empresas especializadas em tecnologia urbana e energia podem participar por meio de Parcerias Público-Privadas (PPPs), contratos de performance energética (EPC - *Engineering, Procurement, and Construction*) realizados por empresas de serviço de energia (ESCOs - *Energy Services Company*) ou concessões administrativas.

A colaboração entre esses atores é essencial para o sucesso da iniciativa, sobretudo em municípios que buscam soluções integradas e sustentáveis. Khemakhem e Krichen[16] destacam a importância do engajamento de todos os intervenientes para superar desafios técnicos e regulatórios. No Brasil, a Resolução Normativa ANEEL nº 414/2010[18] atribui aos municípios a responsabilidade pela iluminação pública, enquanto a Lei Geral de Proteção de Dados (LGPD) regula o tratamento e a segurança das informações coletadas.

Onde a Tecnologia Deve ser Aplicada com Prioridade

A implantação de postes inteligentes deve ser orientada por critérios técnicos e estratégicos, com prioridade para áreas que apresentam alta circulação de pessoas e veículos, histórico elevado de criminalidade ou relevância social. Exemplos incluem: centros comerciais, corredores de transporte público, proximidades de escolas e hospitais, parques urbanos, vias expressas, e zonas com menor cobertura de policiamento comunitário. Essas regiões podem funcionar como áreas-piloto, onde os impactos da tecnologia são rapidamente percebidos e mensurados, facilitando a aceitação pública e o planejamento da expansão para outras áreas do município.

Implantação de Iluminação Inteligente com Sensores Integrados

Postes de iluminação inteligente com sensores integrados são uma solução estratégica para cidades inteligentes, promovendo segurança pública, eficiência energética e gestão urbana avançada. Equipados com tecnologias como IoT, sensores de movimento e conectividade 5G, esses postes permitem monitoramento em tempo real, iluminação responsiva e coleta de dados para combater a criminalidade e otimizar recursos.

A Tabela 6.1 detalha o processo de implantação, servindo como guia para gestores municipais e profissionais de segurança.

Tabela 6.1 – Etapas para Implantação de Postes Inteligentes com Sensores

Etapa	Ação
1. Planejamento	Mapeamento de áreas críticas com base em índices de criminalidade, tráfego e iluminação deficiente. Coleta de dados sobre malha viária, perfil populacional e vulnerabilidades urbanas, com consulta comunitária.
2. Seleção de Fornecedores	Elaboração de edital com especificações técnicas (luminárias LED, sensores IoT, durabilidade). Contratação via licitação pública ou parceria público-privada, priorizando fornecedores com expertise em segurança urbana.
3. Instalação	Substituição gradual de postes tradicionais por modelos inteligentes com sensores integrados. Garantia de cabeamento elétrico seguro e testes de funcionalidade para cobertura luminosa e detecção de eventos.
4. Integração	Conexão dos postes a plataformas de gestão urbana e centros de comando (C4). Configuração de sistemas para monitoramento em tempo real, geração de alertas e análise de dados (ex.: padrões de movimento).
5. Treinamento	Capacitação de equipes municipais em operação, manutenção e análise de dados gerados pelos sensores. Treinamento em resposta a alertas e uso de dashboards para tomada de decisão.
6. Monitoramento	Supervisão contínua do desempenho dos postes, com ajustes operacionais baseados em dados coletados. Rotinas de manutenção preventiva, atualização de firmware e suporte técnico com SLA definido.

Tecnologias Envolvidas

Os postes inteligentes são estruturas multifuncionais equipadas com sensores diversos e conectividade por Internet das Coisas (IoT). Seu diferencial está na capacidade de operar de forma autônoma e interativa com o ambiente urbano. Os componentes típicos são:

- Sensores de movimento: ativam a iluminação conforme o fluxo de pessoas e veículos, promovendo economia de energia e segurança adaptativa;
- Sensores ambientais: medem temperatura, umidade, níveis de ruído e poluição do ar, fornecendo dados valiosos para a saúde pública e gestão ambiental;
- Câmeras de vigilância com Inteligência Artificial (IA): realizam monitoramento em tempo real e podem acionar alertas automáticos;
- Conectividade remota: protocolos como LoRa, NB-IoT, Zigbee, wi-fi e 5G permitem controle e monitoramento centralizado por plataformas SCADA ou em nuvem[22];
- Análise de dados e manutenção preditiva: diagnóstico de falhas e consumo em tempo real, com base em algoritmos inteligentes.

6.2 Câmeras de Monitoramento Integradas à Iluminação

As cidades inteligentes demandam soluções que aproveitem a infraestrutura existente de forma eficiente e inteligente. A instalação de câmeras de vigilância diretamente em postes de iluminação pública é uma dessas soluções, combinando segurança, conectividade e economia de recursos.

Essa integração permite o uso compartilhado de energia e redes de comunicação já presentes nos postes, otimizando custos de instalação e manutenção. Além disso, amplia a vigilância urbana e contribui para a prevenção da criminalidade com monitoramento contínuo e em tempo real.

De acordo com a IFSEC Global[20], a presença dessas câmeras permite não apenas a detecção rápida de ocorrências, mas também uma atuação preditiva por parte das forças de segurança. Quando integradas a sensores e sistemas de comunicação, tornam-se ferramentas robustas para a gestão da segurança pública.

Em resumo, as câmeras integradas à iluminação representam uma solução estratégica para modernizar a vigilância urbana, elevar a percepção de segurança da população e fortalecer a capacidade de resposta dos municípios, tudo isso com uso otimizado da infraestrutura já instalada.

Os fatores principais que justificam o uso de câmeras de monitoramento integradas à iluminação são:

- **Reforço à segurança pública**: a presença de câmeras inibe práticas criminosas e facilita a resolução de ocorrências[21];
- **Eficiência de custos**: aproveitamento da infraestrutura de postes reduz os gastos com implantação[20];
- **Resposta rápida**: monitoramento em tempo real permite agir com agilidade diante de emergências;
- **Inteligência urbana**: geração de dados visuais que alimentam algoritmos de segurança e planejamento urbano[22].

Equipe Responsável

- Prefeituras municipais;
- Secretarias de Segurança Pública;
- Empresas de segurança eletrônica;
- Concessionárias de iluminação pública;
- Parceiros privados em modelos de concessão ou parcerias público-privadas (PPPs).

Onde a Tecnologia Deve ser Aplicada com Prioridade

- Áreas com altos índices de criminalidade;
- Estações de transporte público;
- Proximidades de escolas, hospitais e centros comerciais;
- Parques e zonas com grande fluxo de pessoas.

Implantação de Câmeras de Monitoramento Integradas à Iluminação

Em cidades inteligentes, a segurança pública ganha força com tecnologias que unem inovação e eficiência. A integração de câmeras de monitoramento a luminárias LED equipadas com sensores IoT transforma a gestão urbana, combinando vigilância em tempo real com iluminação responsiva. Essa solução reduz índices de criminalidade, melhora a visibilidade noturna e promove sustentabilidade energética.

A Tabela 6.2 apresenta uma sugestão de etapas para a implantação desse sistema, oferecendo um guia prático para gestores e profissionais de segurança.

Tabela 6.2– Etapas para a implantação de sistema de iluminação e vigilância integrados

Etapa	Ação
1. Levantamento	Mapeamento de áreas prioritárias com base em índices de criminalidade, tráfego e baixa iluminação. Análise de vulnerabilidades (pontos cegos, áreas escuras) com consulta a dados policiais e comunitários.
2. Projeto Técnico	Escolha Venha Escolha de luminárias LED com câmeras integradas, sensores IoT, conectividade (*Wi-Fi*/5G) e IA embarcada para reconhecimento facial ou detecção de movimento. Definição de redes, armazenamento em nuvem e sistemas de controle adaptativo (por exemplo, dimerização por presença).
3. Licitação ou PPP	Desenvolvimento de edital detalhando requisitos técnicos (resolução de câmeras, eficiência luminosa, durabilidade). Seleção de fornecedores via licitação ou parceria público-privada, priorizando experiência em segurança urbana.
4. Instalação	Fixação de postes com luminárias e câmeras, garantindo integração elétrica segura e alinhamento para cobertura otimizada (luz e vídeo). Testes de funcionalidade para iluminação responsiva a e captura de imagens em tempo real.
5. Integração	Conexão com Sistema de Comando e Controle C4 (comando, controle, comunicações, computação), plataformas de gestão de vídeo e sistemas de alerta. Configuração de dashboards para monitoramento em tempo real e análise de dados (por exemplo, identificação de padrões criminais).
6. Manutenção	Estabelecimento de rotinas de inspeção para limpeza de lentes e luminárias, atualização de firmware e verificação de conectividade. Suporte técnico contínuo para falhas de hardware ou software, com acordo de nível de serviço definido.

Tecnologia Envolvidas

O sistema consiste na instalação de câmeras de alta definição (Full HD ou superior) diretamente nos postes de iluminação pública. Essas câmeras operam com alimentação elétrica fornecida pelo próprio poste e conexão via redes de fibra ótica, 4G, 5G ou redes *mesh* de comunicação sem fio. As principais tecnologias envolvidas incluem:

- Câmeras de alta definição (Full HD ou superior), com operação contínua ou acionamento por sensores de presença;
- Visão noturna infravermelha *(night vision infrared)* ou imagem térmica, para captação em ambientes de baixa luminosidade;
- Inteligência artificial embarcada, com funcionalidades como reconhecimento de placas (LPR –*License Plate Recognition)*, detecção facial e análise de comportamento;
- Armazenamento local (*edge computing*) ou transmissão remota por fibra ótica, rádio, 4G/5G;
- Integração com Centros de Comando e Controle (CCCs) e serviços de emergência (190, SAMU-Serviço de Atendimento Móvel de Urgência), agilizando respostas a incidentes.

6.3 Iluminação Responsiva por Presença

A iluminação pública responsiva ajusta automaticamente a intensidade da luz conforme a presença de pedestres, ciclistas ou veículos. Essa solução inteligente melhora a segurança urbana, reduz o consumo de energia e diminui os custos operacionais.

O sistema é composto por sensores de presença (como infravermelho, ultrassônico ou micro-ondas), luminárias LED com capacidade de variação de intensidade (dimerização), conectividade remota (LoRaWAN, rede mesh, 4G/5G) e uma plataforma de gestão inteligente.

Ao detectar movimento, os sensores acionam as luminárias, criando um “caminho de luz” que acompanha o deslocamento das pessoas ou veículos em tempo real. Além de promover conforto e segurança, esse modelo pode ser integrado a outros serviços urbanos, como videomonitoramento ou gestão de tráfego.

A iluminação responsiva representa uma evolução no uso da infraestrutura urbana, unindo tecnologia, sustentabilidade e bem-estar social.

Vale ressaltar que, para garantir a conformidade e a qualidade do serviço, o sistema de iluminação responsiva deve atender aos requisitos estabelecidos pela nova norma ABNT NBR 5101- Iluminação viária — Procedimentos (Anexo A, Tabela A.2.1), que define os critérios e as condições para a implementação de iluminação pública viária. A norma proporciona diretrizes importantes para o planejamento, projeto e execução de sistemas de iluminação, assegurando a eficiência, segurança e sustentabilidade da infraestrutura.

A iluminação responsiva oferece diversos benefícios que justificam sua adoção por municípios. As principais estão elencadas abaixo:

- Eficiência energética significativa**,** com redução de até 70% a 80% no consumo, segundo estudos da IEA[5] e do projeto de Roterdã[23];
- Aumento da sensação de segurança**,** uma vez que áreas escuras se iluminam automaticamente na presença de pessoas[24];

Equipe Responsável

A responsabilidade pode ser compartilhada entre:

- Secretarias municipais de iluminação pública;
- Concessionárias de energia elétrica e operadores de iluminação urbana;
- Empresas integradoras de tecnologias urbanas, especializadas em sensores e controle remoto;
- Parceiros privados por meio de modelos de concessão ou parcerias público-privadas (PPPs).

Onde a Tecnologia Deve ser Aplicada Com Prioridade

A iluminação responsiva é especialmente recomendada para:

- Ciclovias, parques e calçadões com baixo movimento noturno;
- Avenidas e ruas com tráfego reduzido;
- Entornos de escolas, hospitais, praças e passagens públicas;
- Áreas onde há percepção de insegurança à noite.

Implantação de Iluminação Responsiva

A iluminação responsiva por presença, ou iluminação responsiva, é uma solução inovadora para cidades inteligentes, combinando segurança pública com eficiência energética. Utilizando sensores de movimento e plataformas IoT, esse sistema ajusta a intensidade luminosa com base na presença de pessoas ou veículos, reduzindo custos e aumentando a visibilidade em áreas críticas. Ideal para locais com pouca movimentação e alta demanda de segurança, essa tecnologia contribui para a prevenção de crimes e a gestão urbana sustentável.

A Tabela 6.3 detalha o processo de implantação, servindo como guia para gestores e profissionais de segurança.

Tabela 6.3 – Etapas para Implantação de Iluminação responsiva

Etapa	Ação
1. Mapeamento	Identificação de áreas com pouca movimentação e alta demanda de segurança.
2. Projeto técnico	Escolha dos sensores, luminárias e sistema de controle remoto.
3. Contratação	Licitação pública ou PPP com fornecedores especializados.
4. Instalação	Fixação dos sensores, substituição de luminárias e integração em rede.
5. Configuração	Programação de perfis de operação conforme horário e fluxo local.
6. Monitoramento	Acompanhamento por sistema de gestão via plataforma IoT.

6.4 Iluminação com Botão De Pânico Integrado

A instalação de botões de pânico em postes de iluminação pública é uma solução eficaz para reforçar a segurança em espaços urbanos, especialmente em áreas com pouca vigilância e maior vulnerabilidade à noite. Essa tecnologia permite que qualquer pessoa acione um pedido de ajuda rapidamente, sem depender de telefone celular, promovendo uma resposta imediata das forças de segurança.

O botão de pânico pode executar automaticamente ações, tais como:

- Aumento da intensidade luminosa na área acionada, gerando visibilidade e inibindo ações criminosas;
- Ativação de sinal sonoro e/ou visual de alerta (sirenes ou luzes piscantes);
- Envio automático de alerta geolocalizado para as centrais de segurança pública;
- Ativação de câmeras próximas

Além de aumentar a segurança em tempo real, essa solução fortalece a confiança da população nos espaços públicos, contribuindo para uma cidade mais segura e participativa. Em particular, a instalação de botões de pânico tem grande aplicação em áreas carentes e de grande pobreza, como periferias e favelas, onde a vulnerabilidade social e a violência são mais prevalentes. Essa tecnologia pode ser crucial no combate à violência de gênero, proporcionando um meio rápido e acessível para as vítimas solicitarem ajuda, sem precisar de um telefone celular ou outras formas de comunicação. Assim, os botões de pânico não apenas aprimoram a segurança, mas também promovem um ambiente mais inclusivo e protegem aqueles que mais precisam de apoio.

A instalação de postes com botão de pânico oferece diversos benefícios:

- Resposta imediata a emergências, mesmo sem acesso a celular;
- Aumento da sensação de segurança em áreas vulneráveis;
- Redução de ocorrências oportunistas;
- Fortalecimento da confiança da população no espaço urbano;
- Integração com sistemas de monitoramento e segurança existentes.

Equipe Responsável

A responsabilidade pela implantação envolve:

- Prefeituras municipais, Secretarias de Segurança, e equipe municipais que faz a gestão da iluminação pública;
- Concessionárias de iluminação pública;
- Empresas integradoras de tecnologia urbana e segurança eletrônica;
- Parceiros privados, por meio de PPPs (Parcerias Público-Privadas) ou contratos de performance.

Onde a Tecnologia Deve ser Aplicada com Prioridade

A prioridade de instalação deve contemplar áreas com maior risco percebido ou estatístico, como:

- Corredores escolares e ciclovias;
- Praças e parques com baixa movimentação;
- Entradas de estações de transporte público;
- Vias com histórico de ocorrências ou baixa visibilidade noturna;
- Zonas com concentração de pedestres em horários de risco.

Implantação de Iluminção com Botão de Pânico Integrado

A implantação de postes de iluminação pública com botão de pânico exige planejamento técnico, articulação com os órgãos de segurança pública e ações de sensibilização da população. O processo pode ser dividido em etapas práticas que orientam os gestores municipais desde o diagnóstico até o uso efetivo da tecnologia.

A Tabela 6.4 descreve as principais etapas da implantação e funcionamento do sistema.

Tabela 6.4 – Etapas para Implantação de Postes com Botão de Pânico Integrado

Etapa	Ação
1. Mapeamento	Realizar um levantamento das áreas com maior vulnerabilidade à violência e baixa cobertura de vigilância. O objetivo é identificar locais prioritários para a instalação dos postes.
2. Projeto técnico	Desenvolver o projeto de engenharia contendo as especificações dos postes, sensores, botões, tipo de conexão (elétrica e de dados) e integração com as centrais de monitoramento.
3. Contratação	Definir o modelo de contratação: licitação tradicional ou concessão público-privada. Incluir fornecimento, instalação, operação e manutenção dos equipamentos.
4. Instalação	Executar a instalação dos postes e dos botões de pânico, conectando-os à rede elétrica e ao sistema de gestão de segurança municipal.
5. Integração	Realizar testes de funcionamento e integração com as centrais de segurança pública (como Guarda Civil; Polícia Militar) para garantir o acionamento eficaz.
6. Treinamento e comunicação	Treinar as equipes de resposta para agir rapidamente após o acionamento e promover campanhas informativas à população sobre o uso correto do botão de pânico.

Tecnologias Envolvidas

O sistema de iluminação pública com botão de pânico integrado utiliza uma combinação de tecnologias para garantir funcionamento confiável e resposta imediata:

- **Botão de pânico físico robusto:** construído com materiais resistentes a intempéries (IP65 ou superior) e vandalismo (IK08 ou superior), com acionamento mecânico ou capacitivo;
- **Módulo de controle eletrônico:** placa de controle responsável por processar o acionamento e executar comandos programados;
- **Interface de comunicação:** uso de tecnologias sem fio como LoRa, NB-IoT, 4G/5G ou Wi-Fi para transmissão do alerta em tempo real para a central de segurança;
- **Integração com sistema de telegestão:** comunicação com plataformas centralizadas que controlam iluminação pública e dispositivos de segurança;
- **Fontes de energia:** alimentação elétrica pela rede pública, com opção de *backup* por bateria para garantir operação em caso de falha de energia;
- **Iluminação adaptativa:** luminárias LED reguláveis com drivers compatíveis para aumentar o fluxo luminoso instantaneamente;
- **Módulos de áudio e vídeo:** alto-falantes para mensagens de emergência e câmeras com rotação automática para registrar a ocorrência;
- **Segurança cibernética:** protocolos de criptografia e autenticação para impedir acionamentos não autorizados ou invasões.

6.5 Inteligência Artificial (IA) Aplicada à Iluminação Pública

A aplicação de inteligência artificial à iluminação pública transforma a forma como as cidades gerenciam energia e segurança. Sistemas com sensores conectados e algoritmos inteligentes permitem ajustar a intensidade da luz conforme o movimento nas vias, prever falhas e orientar ações de manutenção com base em dados reais.

Com essa tecnologia, os municípios reduzem custos operacionais, aumentam a vida útil dos equipamentos e reforçam a segurança urbana — especialmente em áreas críticas. Além disso, relatórios e painéis de informação (*dashboards)* gerados automaticamente trazem mais transparência e eficiência para a gestão pública.

A iluminação inteligente com IA também se integra a outras áreas da cidade, como trânsito, meio ambiente e segurança, tornando-se uma base estratégica para o desenvolvimento urbano digital e sustentável.

Para implantação dessa tecnologia deve ser implementada uma plataforma de gestão de iluminação pública baseada em análise de dados e inteligência artificial, com os seguintes componentes:

- **Coleta e processamento de dados:** sensores instalados em postes inteligentes (luminosidade, presença, ruído, tráfego) geram dados que alimentam algoritmos de IA para análise em tempo real;
- **Automação e otimização**: algoritmos de aprendizado de máquina (*machine learning*) ajustam dinamicamente a intensidade da iluminação com base em variáveis como fluxo de pessoas, horário e condições climáticas, otimizando o consumo energético.
- **Manutenção preditiva:** modelos preditivos identificam pontos críticos de falhas antes que ocorram, reduzindo custos e aumentando a vida útil dos equipamentos.
- **Monitoramento de segurança**: integração de dados de sensores com sistemas de segurança pública para mapear áreas de risco e reforçar a iluminação em locais com maior incidência de crimes;
- ***Dashboards* e relatórios:** ferramentas de visualização de dados fornecem indicadores de desempenho, como economia energética, tempo de resposta a falhas e impacto na segurança urbana.

Esse tipo de abordagem está alinhado às práticas de cidades inteligentes, promovendo eficiência e segurança, conforme descrito por Alves e colegas[25].

A implantação de Inteligência Artificial (IA) na iluminação pública tem como objetivos:

- **Fortalecer a segurança pública:** ambientes bem iluminados, com ajustes dinâmicos baseados em dados, reduzem a incidência de crimes e aumentam a percepção de segurança, conforme apontado pela *International Energy Agency*[26];
- **Reduzir custos operacionais**: a automação e a manutenção preditiva podem diminuir o consumo energético em até 30%, como observado no projeto CityOS de Barcelona[27];
- **Apoiar a gestão baseada em dados**: a análise de grandes volumes de dados permite decisões mais assertivas, com relatórios detalhados que promovem transparência e planejamento estratégico;
- **Modernizar a infraestrutura urbana**: a integração de IA e IoT posiciona as cidades paulistas como referência em inovação, atraindo investimentos e melhorando a qualidade de vida.
- **Contribuir para a sustentabilidade**: a eficiência energética alinha-se às metas estaduais de redução de emissões, promovendo cidades mais sustentáveis.
- **Promover a qualidade do serviço de iluminação pública com foco no cidadão: o** modelo de iluminação inteligente deve seguir o conceito de Design Centrado no Ser Humano — HCD (Human-Centered Design), que coloca as pessoas no centro das decisões do projeto. Essa abordagem busca garantir que as soluções atendam de forma eficiente, inclusiva e conectada às necessidades da população, fortalecendo a relação entre os serviços urbanos e aqueles que dependem deles diariamente.

O HCD (*Human-Centered Design*) está é uma metodologia de desenvolvimento de produtos, sistemas e serviços que considera como prioridade as necessidades, expectativas e limitações das pessoas que irão utilizá-los. Para isso, baseia-se em pesquisas aprofundadas sobre a experiência do usuário, uso de *feedback* contínuo e processos iterativos (ajustes constantes durante o desenvolvimento). O objetivo é garantir que a solução final seja intuitiva, eficaz e de fácil utilização por todos os públicos[28].

O processo de HCD geralmente envolve três fases:

- Inspiração - pesquisa para entender as necessidades, desafios e comportamentos dos usuários;
- Ideação - geração de ideias e protótipos com base nas necessidades identificadas;
- Implementação - teste e aprimoramento contínuo com a participação ativa dos usuários.

O objetivo é criar soluções que sejam não apenas tecnicamente viáveis, mas também emocionalmente satisfatórias e acessíveis aos usuários. Além disso, o HCD enfatiza a importância da empatia no design, com o designer colocando-se no lugar do usuário para identificar as melhores soluções[29].

Equipe Responsável

A execução do projeto envolve a colaboração de diversos atores:

- **Governo municipal: s**ecretarias de infraestrutura, urbanismo e tecnologia lideram o planejamento, a implantação e o monitoramento do sistema;
- **Empresas de tecnologia**: fornecedores especializados em IA, ciência de dados e IoT desenvolvem e integram a plataforma de gestão, além de oferecerem suporte técnico;
- **Concessionárias de iluminação pública**: parceiras na instalação de sensores e na manutenção dos sistemas, especialmente em modelos de parcerias público-privadas (PPP);
- **Consultorias em cidades inteligentes**: apoiam na definição de indicadores de desempenho, na análise de dados e na capacitação das equipes;
- **Universidades e centros de pesquisa**: contribuem com expertise técnica em IA e formação de profissionais qualificados, conforme sugerido por Alves e colegas[29];
- **Comunidade local**: participa de consultas públicas para garantir que a implantação atenda às necessidades de segurança e mobilidade urbana.

Onde a Tecnologia Deve ser Aplicada com Prioridade

A tecnologia deve ser aplicada em áreas estratégicas das cidades paulistas, priorizando locais onde a análise de dados e IA pode maximizar o impacto na segurança e na eficiência:

- **Centros urbanos e comerciais:** regiões com alta circulação noturna, onde a iluminação dinâmica pode prevenir crimes e melhorar a percepção de segurança;
- **Corredores viários principais**: avenidas com intenso tráfego, onde sensores de fluxo ajustam a iluminação para otimizar o consumo energético;
- **Praças e parques públicos**: espaços de convivência que se beneficiam de iluminação responsiva para promover o uso seguro à noite;
- Áreas com alta incidência de crimes: zonas mapeadas por dados policiais, onde a IA pode reforçar a iluminação em horários críticos;
- **Bairros com infraestrutura deficiente**: regiões com falhas frequentes na iluminação, identificadas por análises preditivas.

A seleção das áreas deve integrar dados criminais e de desempenho da iluminação, inspirando-se em iniciativas como o programa de luminárias inteligentes de San Diego[30].

Implantação da Inteligência Artificial Aplicada à Iluminação Pública

A implantação deve seguir um plano estruturado, focado na integração de análise de dados e IA, o que envolve principalmente as seguintes atividades:

- **Planejamento estratégico**: definir objetivos mensuráveis (por exemplo, redução de 25% no consumo energético, 10% na taxa de crimes noturnos) e indicadores de desempenho, com base em referências como IEA[26];
- **Mapeamento de dados**: levantar a infraestrutura de iluminação existente e identificar postes aptos para receber sensores IoT conectados à plataforma de IA;
- **Seleção de fornecedores**: Escolher empresas com expertise em aprendizado de máquina (*machine learning)*, análise preditiva e integração IoT, priorizando soluções escaláveis;
- **Instalação de sensores**: Equipar postes com dispositivos que coletem dados de luminosidade, presença, ruído e tráfego, conectados a redes IoT para transmissão em tempo real.
- **Desenvolvimento da plataforma de IA**: Contratar ou desenvolver uma solução que processe dados, execute modelos preditivos, ajuste a iluminação dinamicamente e gere dashboards interativos.
- **Capacitação técnica**: Treinar equipes municipais em ciência de dados, operação da plataforma e interpretação de relatórios, com apoio de universidades[25].
- **Integração com segurança pública**: Conectar a plataforma de Inteligência Artificial (IA) a sistemas de videomonitoramento e bases de dados policiais para mapear áreas de risco e otimizar a iluminação.
- **Monitoramento e otimização**: Avaliar continuamente indicadores de desempenho (por exemplo, economia energética, tempo de resposta a falhas, redução de ocorrências) e atualizar os algoritmos para melhorar a performance.

Tecnologia Envolvidas

A solução de iluminação pública inteligente com Inteligência Artificial combina diferentes componentes tecnológicos e metodologias:

- **Sensores IoT (Internet das Coisas):** dispositivos instalados nos postes para medir luminosidade, presença, tráfego, ruído, condições climáticas e qualidade do ar;
- **Plataforma de Processamento de Dados:** sistema em nuvem ou local que recebe, armazena e organiza os dados coletados, integrando diferentes fontes;
- **Algoritmos de Inteligência Artificial e Aprendizado de Máquina (*Machine Learning*)** modelos que analisam os dados em tempo real, detectam padrões, preveem falhas e otimizam o uso da iluminação;
- **Redes Neurais e Modelos Preditivos:** utilizados para antecipar necessidades de manutenção e ajustar a intensidade luminosa de forma dinâmica;
- **Infraestrutura de Comunicação:** redes sem fio (como LoRaWAN, NB-IoT, 4G/5G) para transmissão de dados entre sensores, plataforma de IA e centrais de controle;
- **Painéis de Controle e *Dashboards*:** interfaces gráficas que permitem aos gestores visualizar indicadores de desempenho, alarmes e históricos operacionais;
- **Integração com Sistemas Urbanos:** conexão com plataformas de segurança pública, trânsito e gestão ambiental para ações coordenadas.

6.6 Postes Multiuso

Postes multiuso integram iluminação LED inteligente e tecnologias de segurança para fortalecer a proteção em cidades inteligentes. Suas luzes de alta eficiência, controladas por sensores de luminosidade e presença, ajustam-se automaticamente à intensidade da luz, garantindo áreas públicas bem iluminadas à noite, garantindo riscos de crimes e acidentes. Integram sistemas de comunicação de emergência com botões de pânico e câmeras conectadas a centrais de segurança para respostas rápidas, além de wi-fi público que amplia o acesso a serviços digitais de emergência. Sensores ambientais monitoram a qualidade do ar, fornecendo dados em tempo real por meio de plataformas IoT para gestão urbana eficiente. O objetivo é promover a segurança por meio de iluminação avançada que melhora a visibilidade e evita atividades criminosas, enquanto sistemas integrados fortalecem respostas a incidentes. A visão é criar cidades inteligentes com ambientes seguros e conectados, centralizando soluções em postos multiuso. A adoção é justificada pela demanda por infraestruturas que combinem iluminação e segurança para enfrentar os desafios da urbanização, conforme relatórios da KPMG [19,22].

A adoção de postes multiuso visa:

- **Fortalecer a segurança pública:** botões de emergência e câmeras integradas permitem respostas rápidas a incidentes, enquanto a iluminação LED melhora a visibilidade noturna, reduzindo crimes, como observado em São José dos Campos (Prefeitura de São José dos Campos, 2025);
- **Promover inclusão digital**: o wi-fi gratuito amplia o acesso à internet em áreas públicas, beneficiando comunidades com exclusão digital, conforme o modelo de Buenos Aires (*Buenos Aires Ciudad*, 2025);
- **Aumentar a eficiência operacional:** a centralização de funções em uma única estrutura reduz custos de instalação e manutenção;
- **Valorizar espaços públicos**: ambientes mais seguros e conectados incentivam o uso noturno de praças, parques e avenidas, melhorando a qualidade de vida;
- **Apoiar a gestão urbana**: dados coletados por sensores ambientais e de uso informam decisões estratégicas, promovendo cidades mais sustentáveis e resilientes.

Equipe Responsável

A implantação requer a colaboração de múltiplos atores:

- **Governo municipal:** secretarias de urbanismo, segurança pública e tecnologia lideram o planejamento, a execução e o monitoramento do projeto;
- **Empresas de tecnologia e IoT**: fornecedores especializados em postes inteligentes, redes Fidelidade Sem Fio (Wi-Fi-*Wireless-Fidelity*) e sistemas de emergência desenvolvem e instalam os equipamentos;
- **Concessionárias de iluminação pública:** parceiras na instalação e manutenção dos postes, especialmente em modelos de parcerias público-privadas (PPP);
- **Operadoras de telecomunicações**: fornecem infraestrutura de conectividade para garantir a estabilidade do sinal Wi-Fi;
- **Consultorias em cidades inteligentes**: apoiam na definição de escopo, integração de sistemas e capacitação de equipes;
- **Comunidade local:** participa de consultas públicas para identificar áreas prioritárias e garantir que o projeto atenda às necessidades de segurança e conectividade.

Onde a Tecnologia Deve ser Aplicada com Prioridade

Os postes multiuso serão instalados em áreas estratégicas das cidades paulistas, priorizando locais onde a integração de iluminação, Wi-Fi e comunicação de emergência maximize o impacto:

- **Praças e parques públicos**: espaços de convivência que se beneficiam de iluminação segura, *Wi-Fi* gratuito e botões de emergência para uso noturno;
- **Avenidas e corredores viários**: regiões de grande circulação, onde a conectividade e a segurança são essenciais para motoristas e pedestres;
- **Entradas de escolas e estações de transporte público**: áreas com alta movimentação de pessoas, especialmente vulneráveis a incidentes;
- **Regiões com alta criminalidade**: zonas identificadas por dados policiais, onde botões de emergência e câmeras podem deter atividades criminosas;
- Áreas com exclusão digital: bairros periféricos ou comunidades carentes, onde o Wi-Fi público pode promover inclusão social e acesso a serviços online.

A escolha dos locais deve ser baseada em análises de dados criminais, índices de conectividade e demandas da população, inspirando-se em projetos como o de Buenos Aires[31].

Implantação de Postes Multiuso

A implantação de postes multiuso deve seguir um plano estruturado, focado na integração de tecnologias e na gestão eficiente, considerando:

- **Planejamento estratégico: d**efinir objetivos claros (por exemplo, redução de 15% em ocorrências policiais, conexão de um determinado número de usuários por mês ao Wi-Fi) e mapear áreas prioritárias com base em dados urbanos;
- **Diagnóstico de infraestrutura:** avaliar a rede elétrica, conectividade e condições dos postes existentes para determinar a necessidade de substituição ou *retrofit*;
- **Seleção de fornecedores: r**ealizar licitações ou parcerias com empresas especializadas em postes inteligentes, IoT, iluminação LED (*Light Emitting Diode*) e telecomunicações;
- **Instalação física:** montar os postes multiuso com luminárias LED, roteadores *Wi-Fi*, botões de emergência, câmeras e sensores, garantindo conexão elétrica e de dados;
- **Integração com centrais de monitoramento:** configurar a plataforma IoT para conectar os postes às centrais de segurança pública e sistemas de gestão urbana, permitindo respostas rápidas a emergências;
- **Testes e validação:** verificar o funcionamento de todos os componentes (iluminação, *Wi-Fi*, comunicação de emergência) e realizar ajustes técnicos;
- **Capacitação das equipes**: treinar servidores municipais e equipes de segurança na operação dos sistemas, manutenção dos postes e análise de dados gerados;
- **Divulgação e engajamento comunitário:** lançar campanhas educativas para orientar a população sobre o uso dos botões de emergência, acesso ao *Wi-Fi* e benefícios dos postes, promovendo aceitação social;
- **Monitoramento e manutenção:** estabelecer indicadores de desempenho (por exemplo, tempo médio de resposta a emergências e tempo em que a rede *Wi-Fi* está disponível e funcionando corretamente) e contratos de manutenção preventiva.

Tecnologias Envolvidas

Os postes multiuso são estruturas verticais equipadas com:

- Luminárias LED de alta eficiência com controle automatizado;
- Roteadores *Wi-Fi* com cobertura para áreas públicas;
- Botões de emergência com interfone e câmeras embutidas;
- Sensores ambientais (temperatura, umidade, qualidade do ar);
- Módulos de energia solar e baterias;
- Portas USB para carregamento de dispositivos móveis;
- Displays informativos ou painéis interativos.

A integração desses componentes ocorre por meio de plataformas IoT, permitindo o controle centralizado, monitoramento remoto e geração de dados em tempo real.

6.7. Geolocalização e Mapeamento de Iluminação Deficitária

A geolocalização e o mapeamento automatizado de iluminação deficitária utilizam tecnologias de georreferenciamento, sensores IoT e análise de dados para identificar áreas urbanas com iluminação insuficiente ou inoperante, que aumentam a criminalidade e reduzem a sensação de segurança. Sensores fotométricos em veículos, drones ou postes inteligentes coletam dados de luminosidade, enquanto inteligência artificial processa imagens noturnas para detectar falhas. Cidadãos podem reportar problemas via aplicativos móveis com *Sistema de Posicionamento Global* (GPS – *Global Positioning System*) e uma plataforma com *Sistema de Informação Geográfica* (GIS - *Geographic Information System*) integrada gera mapas de calor e alertas automáticos para priorizar manutenções. O objetivo é reduzir crimes em áreas mal iluminadas, agilizar a manutenção, otimizar recursos orçamentários e aumentar a transparência na gestão pública. A visão é criar cidades inteligentes com iluminação eficiente que promova segurança e bem-estar. A adoção é justificada pela necessidade de soluções proativas para gerenciar a infraestrutura urbana, conforme destacado nos relatórios da KPMG[19,22].

A adoção da geolocalização para mapeamento de iluminação deficiente visa:

- **Aumentar a segurança urbana:** áreas bem iluminadas reduzem a incidência de crimes e acidentes;
- **Agilizar a manutenção:** a identificação precisa de falhas permite intervenções rápidas, diminuindo custos operacionais e melhorando a confiabilidade da infraestrutura;
- **Promover transparência:** mapas acessíveis e relatórios detalhados fortalecem a confiança da população na gestão pública, como observado em Curitiba[32];
- **Otimizar recursos:** a priorização de investimentos em áreas críticas maximiza o impacto do orçamento municipal;
- **Fomentar a participação cidadã:** canais digitais engajam a população na gestão urbana, alinhando-se às práticas de cidades inteligentes[33].

Equipe Responsável

A implantação envolve a colaboração de diversos atores:

- **Governo municipal:** secretarias de urbanismo, serviços públicos e tecnologia lideram o planejamento, a execução e o monitoramento do sistema;
- **Empresas de tecnologia:** fornecedores de sensores IoT, softwares de sistemas de informação geográfica e aplicativos móveis desenvolvem e integram as soluções tecnológicas;
- **Concessionárias de iluminação pública:** parceiras na manutenção corretiva e preventiva dos postes identificados como deficientes;

- **Consultorias em cidades inteligentes:** apoiam na definição de indicadores chaves de desempenho, integração de dados e capacitação de equipes;
- **População:** participa ativamente por meio de aplicativos, reportando falhas e contribuindo para o mapeamento colaborativo;
- **Universidades e centros de pesquisa:** fornecem suporte técnico em geoprocessamento e análise de dados.

Onde a Tecnologia Deve ser Aplicada com Prioridade

O sistema deve ser aplicado em áreas estratégicas das cidades paulistas, priorizando locais onde a iluminação deficiente impacta a segurança e a mobilidade:

- **Regiões com alta criminalidade:** zonas mapeadas por dados policiais, onde a falta de iluminação aumenta a vulnerabilidade a crimes;
- **Áreas periféricas:** bairros com infraestrutura precária, frequentemente negligenciada em programas de manutenção;
- **Corredores de transporte coletivo:** vias com grande circulação de ônibus e pedestres, onde a iluminação é essencial para a segurança noturna;
- **Parques e praças públicas:** espaços de convivência que requerem iluminação adequada para uso noturno seguro;
- **Vias com alta circulação de pedestres:** ruas comerciais e entorno de escolas, onde pontos escuros podem comprometer a mobilidade.

A seleção das áreas deve integrar dados criminais, relatórios de manutenção e denúncias cidadãs. Pode-se inspirar, em projetos como o de Curitiba[32].

Implantação de Geolocalizaçao e Mapeamento de Iluminção Deficitária

A implantação deve seguir um plano estruturado, focado na coleta, análise e gestão de dados georreferenciados:

- **Diagnóstico inicial:** mapear a rede de iluminação existente, identificar pontos críticos (por exemplo, áreas com falhas frequentes) e levantar dados criminais para priorização;
- **Escolha da tecnologia:** Definir a combinação ideal de ferramentas, como sensores embarcados em veículos, drones com câmeras fotométricas ou aplicativos cidadãos, com base no orçamento e na infraestrutura local;
- **Seleção de fornecedores:** realizar licitações para adquirir sensores IoT, softwares e outras tecnologias e, também, plataformas de análise de dados, priorizando soluções interoperáveis;
- **Coleta de dados:** instalar sensores em veículos municipais ou drones para mapear níveis de luminosidade e lançar aplicativos móveis para relatórios cidadãos;
- **Integração com plataforma de *Sistema de Informação Geográfica* (GIS):** configurar sistemas de informação geográfica para processar dados, gerar mapas de calor e emitir alertas automáticos sobre falhas;
- **Capacitação das equipes:** treinar servidores municipais em geoprocessamento, uso de plataformas GIS e interpretação de relatórios, com apoio de consultorias especializadas;
- **Engajamento comunitário:** promover campanhas educativas para incentivar o uso de aplicativos, com recompensas sociais (reconhecimento em plataformas municipais) para aumentar a adesão;
- **Monitoramento e manutenção:** estabelecer indicadores chaves de desempenho (tempo médio de reparo, redução de ocorrências em áreas mapeadas) e contratos com cláusulas que estabelecem as responsabilidades e compromissos para manutenção de sensores.

Tecnologias Envolvidas

A geolocalização e o mapeamento de falhas na iluminação utilizam um conjunto de ferramentas tecnológicas que incluem:

- Sensores embarcados em veículos ou drones com câmeras fotométricas que percorrem vias públicas e registram níveis de luminosidade;
- Análise de imagens noturnas por Inteligência Artificial (IA) para detectar trechos com deficiência ou ausência de iluminação;
- Aplicativos móveis que permitem ao cidadão reportar pontos escuros com precisão de localização via GPS (*Global Positioning System*);
- Sistemas GIS (*Geographic Information System*) integrados a plataformas de gestão de ativos urbanos;
- Bases de dados em nuvem que atualizam mapas de iluminação em tempo real.

Referências Bibliográficas

1. INTERNATIONAL ENERGY AGENCY. **Energy technology perspectives 2020**: Special report on clean energy innovation Paris: IEA, 2020. Disponível em: https://www.iea.org/reports/energy-technology-perspectives-2020. Acesso em: 6 jun. 2025.

2. UNIVERSITY OF CHICAGO. Urban Labs. **The effects of outdoor lighting on crime and safety**. Chicago: Urban Labs, 2019. Disponível em: https://crimelab.uchicago.edu/projects/nyc-street-lighting-reducing-crime-through-environmental-design/. Acesso em: 6 jun. 2025.

3. WILSON, J. Q.; KELLING, G. L. Broken windows: **The police and neighborhood safety**. The Atlantic Monthly, v. 249, p. 29–38, 1982.

4. INTERNATIONAL TELECOMMUNICATION UNION. **Smart sustainable cities**: an analysis of definitions. Geneve: ITU, 2016.

5. INTERNATIONAL ENERGY AGENCY. **Energy efficiency 2023**. Paris: IEA, 2023. Disponível em: https://www.iea.org. Acesso em: 9 abr. 2025.

6. SÃO JOSÉ DOS CAMPOS (Cidade). **São José terá projeto piloto de tecnologia 5G no centro**. https://www.sjc.sp.gov.br/noticias/2023/julho/03/sao-jose-tera-projeto-piloto-de-tecnologia-5g-no-centro/. Acesso em: 9 abr. 2025.

7. GONZÁLEZ, M. C.; HIDALGO, C. A.; BARABÁSI, A.-L. **Understanding individual human mobility patterns.** Nature, v. 453, p. 779–782, 2008. https://doi.org/10.1038/nature06958.

8. SMART CITY EXPO. **World Congress Smart City Expo, Moving cities towards a better future**. 2025. Disponível em: https://www.smartcityexpo.com/. Acesso em: 28 abr. 2025.

9. GHYABI, Mehrdad. **Smart cities and a modern approach to structural health monitoring: autonomous visual sensing and decision making**. 2024. Tese (Doutorado) – George Mason University. Disponível em: https://www.proquest.com/openview/07c37ac757739a8025a1bb2a6ef39154/1?pq-origsite=gscholar&cbl=18750&diss=y. Acesso em: 6 jun. 2025.

10. WORLD HEALTH ORGANIZATION. **Air Pollution**. 2025. Disponível em: https://www.who.int/health-topics/air-pollution. Acesso em: 28 abr. 2025.

11. EUROPEAN COMISSION. **Smart Mobility and Urban Traffic Management**. 2025. https://ec.europa.eu/. Acesso em: 28 abr. 2025.

12. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Cybersecurity Framework**. Disponível em: https://www.nist.gov/cyberframework. Acesso em: 28 abr. 2025.

13. DIRAN, Devin; VAN VEENSTRA, Anne Fleur; TIMAN, Tjerk; TESTA, Paola; KIROVA, Maria. Artificial intelligence in smart cities and urban mobility. [S.l.]: European Parliament, July 2021. Disponível em: www.europarl.europa.eu/supporting-analyses. Acesso em: 6 jun. 2025.

14. GREEN TECH MEDIA. **Smart Streetlights with EV Charging Capabilities**. Disponível em: https://www.greentechmedia.com/. Acesso em: 28 abr. 2025.

15. INTERNATIONAL TELECOMMUNICATION UNION. **Smart Sustainable Cities – Definitions and Methodologies, 2015.** Disponível em: https://www.itu.int/. Acesso em: 28 abr. 2025.

16. KHEMAKHEM, S.; KRICHEN, L. A comprehensive survey on an IoT-based smart public street lighting system application for smart cities. **Franklin Open**, v. 8, art. 10142, Sept. 2024. https://doi.org/10.1016/j.fro.2024.100142.

17. URBAN INSTITUTE. **Do street lights reduce crime?** 2022. Disponível em: https://www.urban.org/research/publication/do-streetlights-reduce-crime. Acesso em: 6 jun. 2025.

18. AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA. Resolução normativa nº 414, de 9 setembro de 2010. Estabelece as Condições Gerais de Fornecimento de Energia Elétrica de forma atualizada e consolidada. **Diário Oficial da União**, Brasília, 15 set. 2010. Disponível em: https://www2.aneel.gov.br/cedoc/ren2010414.html. Acesso em: 06 jun. 2025.

19. KPMG. **Inovação e eficiência energética na iluminação pública.** [*S.l.*]: KPMG, 2023.

20. BOOKER, L. What does a smart city look like? How video surveillance AI is changing our cities. **IFSEC GLOBAL,** 11 apr. 2023. Disponível em: https://www.ifsecglobal.com/video-surveillance/what-does-smart-city-look-like-how-video-surveillance-ai--is-changing-cities/. Acesso em: 09 abr. 2025.

21. SÃO PAULO (Estado). **Detecta contribui para redução da criminalidade.** Notícias Alesp, 18 ago. 2023. Disponível em: https://www.al.sp.gov.br/noticia/?id=457647. Acesso em: 9 abr. 2025

22. KPMG. **Iluminação pública inteligente**: Cidades seguras e conectadas. [*S.l.*]: KPMG, 2023

23. SMART CITY HUB. **Rotterdam's growing stature as digital connectivity hub**. 2022. Disponível em: https://www.rotterdam.info/en/rotterdam-s-growing-stature-as-digital-connectivity-hub. Acesso em: 9 abr. 2025.

24. BARCELONA DIGITAL CITY. **Technology at the service of citizens.** Disponível em: https://ajuntament.barcelona.cat/digital/en/technology-service-citizens. Acesso em: 6 jun. 2025.

25. MORAIS, Filipe Daniel de Almeida. **Sistema inteligente para iluminação pública**. 2016. Dissertação (Mestrado em Engenharia Eletrotécnica e de Computadores) – Faculdade de Engenharia, Universidade do Porto, Porto, 2016. Disponível em: https://repositorio-aberto.up.pt/handle/10216/85891. Acesso em: 6 jun. 2025.

26. INTERNATIONAL ENERGY AGENCY, **Annex 81 – Data-driven smart buildings. IEA –** Energy in Buildings and Communities Programme. Disponível em: https://annex81.iea-ebc.org (accessed June 9, 2025).

27. SMART CITY EXPO. **Barcelona smart city.** Disponível em: https://www.smartcityexpo.com/. Acesso em: 9 jun. 2025.

28. BROWN, Tim. **Design thinking:** uma metodologia poderosa para decretar o fim das velhas ideias. Edição comemorativa de 10 anos. Rio de Janeiro: Alta Books, 2020.

29. NORMAN, D. A. **The design of everyday things**: revised and expanded edition. New York: Basic Books, 2013. 368 p

30. SAN DIEGO (City). **Smart Streetlight, License Plate Reader Technology Helping Solve Crimes and Keep San Diegans Safe.** Disponível em: https://www.sandiego.gov/mayor/smart-streetlight-license-plate-reader-helping-solve-crimes. Acesso em: 9 jun. 2025.

31. BUENOS AIRES (Ciudad). **Buenos Aires**: an innovative platform that supports adaptative smart city applications. Disponível em: https://www.interact-lighting.com/global/customer-stories/buenos-aires. Acesso em: 6 jun. 2025.

32. PARANÁ (Estado). Estado firma acordo com ICI para levar iniciativas inteligentes a cidades do Interior. **Agência Estadual de Notícias**, 15 ago. 2023. Disponível em: https://www.aen.pr.gov.br/Noticia/Estado-firma-acordo-com-ICI-para-levar-iniciativas-inteligentes-cidades-do-Interior. Acesso em: 6 jun. 2025.

33. ESRI. **Smart Communities & Smart Cities**. Disponível em: https://www.esri.com/en-us/smart-communities/overview. Acesso em: 09 jun. 2025.

7 Pré-requisitos para soluções inteligentes

7.1 Perfil das Cidades

A implantação de sistemas digitais deve ser adaptada às realidades dos diversos municípios do Estado de São Paulo. O IBGE (Instituto Brasileiro de Geografia e Estatística) classifica os municípios por porte populacional nas seguintes categorias:

- Pequeno Porte I, até 20.000 habitantes;
- Pequeno Porte II, de 20.001 até 50.000 habitantes;
- Médio Porte, de 50.001 até 100.000 habitantes;
- Grande Porte, de 100.001 até 900.000 habitantes;
- Metrópole, acima de 900.001 habitantes.

Para que as soluções digitais sejam realmente eficazes e confiáveis, é necessário que as cidades possam atender certos requisitos, como os indicados a seguir.

Dispor de Infraestrutura Tecnológica

A operação dos sistemas digitais exige uma base tecnológica estável. Isso inclui fornecimento de energia elétrica confiável (com suporte de nobreaks em equipamentos críticos), conexão de internet estável ou redes de comunicação dedicadas (como redes LoRa ou LTE-M), além de protocolos de interoperabilidade que permitam a integração entre sensores, softwares, centrais de comando e plataformas de serviços públicos.

Dispor de Pessoal Treinado

O uso eficaz da tecnologia depende de pessoas capacitadas para instalação, operação, manutenção e interpretação dos dados. Operadores, bombeiros, policiais, investigadores e equipes de defesa civil precisam receber treinamento periódico. Isso inclui o uso de softwares de monitoramento, respostas automáticas baseadas em protocolos de risco, leitura de alertas e simulações de emergência.

Considerar o Marco Legal e Regulatório

A digitalização deve respeitar as normas legais de proteção de dados (como a LGPD), o marco civil da internet e os códigos de obras e edificações. Além disso, o uso de drones e câmeras deve estar regulamentado, especialmente em áreas públicas e privadas sensíveis. A clareza jurídica é essencial para evitar litígios e garantir a segurança institucional das iniciativas.

Promover a Conscientização Pública

A população deve estar envolvida nos processos de segurança e preparada para conviver com os sistemas digitais. Isso inclui campanhas educativas, treinamentos comunitários e sistemas de alerta acessíveis. A colaboração dos cidadãos aumenta a eficácia das tecnologias e reduz o tempo de resposta em emergências.

Ter Plano de Manutenção

Os sistemas digitais requerem manutenção mais frequente do que os convencionais. Deve-se prever um plano de manutenção preventiva e corretiva, com atualização de softwares, substituição de componentes e verificação de desempenho, com testes periódicos. O não cumprimento desses planos pode comprometer todo o sistema.

A Tabela 7.1 resume os requisitos citados e mostra como cada um influencia diretamente o desempenho das tecnologias digitais:

Tabela 7.1 – Requisitos para Sistemas de Segurança e Emergência

Requisito	Descrição geral	Impacto na Eficácia
Infraestrutura Tecnológica	Energia elétrica confiável, conectividade via internet ou redes alternativas.	Permite operação com maior confiabilidade técnica
Pessoal Treinado	Equipes treinadas para operar e interpretar os sistemas e atuar rapidamente.	Evita falhas operacionais, acelera decisões e melhora a operação dos sistemas instalados
Marco Legal e Regulatório	Normas sobre proteção de dados, uso de drones, obrigações de notificação.	Garante segurança jurídica, aumenta a adesão e permite fiscalizações mais eficazes
Conscientização Pública	Campanhas educativas sobre emergências e uso de recursos tecnológicos.	Amplia a adesão comunitária às orientações em emergências e reduz o risco de pânico ou desinformação
Plano de Manutenção	Rotina de verificação e atualização de dispositivos e softwares.	Previne falhas técnicas, aumenta a confiabilidade e prolonga a vida útil dos equipamentos

7.2 Infraestrutura atual no Estado de São Paulo

O Estado de São Paulo já possui uma infraestrutura tecnológica relevante que pode servir como base para a implantação das tecnologias propostas neste caderno. Iniciativas como os programas **Muralha Paulista** e **Smart Sampa** demonstram que há um ponto de partida concreto para a digitalização das medidas de segurança urbana, incluindo a segurança contra incêndios.

Programas com Infraestrutura que Pode ser Aproveitada

Muralha Paulista[1]

Criado pelo Decreto nº 68.828/2024, o programa **Muralha Paulista** é uma iniciativa estadual voltada à segurança pública, com foco na redução da criminalidade. O programa utiliza mais de 7 mil câmeras distribuídas estrategicamente por todo o estado, integradas a sistemas de inteligência artificial para reconhecimento facial, leitura de placas veiculares e sensoriamento remoto. Essa infraestrutura digital permite análise de dados em tempo real e atua como base para respostas mais rápidas a eventos críticos.

Smart Sampa[2]

O programa ***Smart* Sampa**, restrito à cidade de São Paulo, tem como objetivo ampliar o videomonitoramento urbano por meio de contratos públicos desde 2023. Atualmente, integra mais de 20 mil câmeras inteligentes, com recursos de reconhecimento facial, todas conectadas a uma central unificada de monitoramento. O sistema é interoperável com serviços como o SAMU (Serviço de Atendimento Móvel de Urgência), o Corpo de Bombeiros e a Polícia Militar, favorecendo uma resposta coordenada a emergências.

Resumo do que Pode ser Aproveitado

O Estado de São Paulo tem grande quantidade de câmeras de vigilância já espalhadas pelo estado.

Só na cidade de São Paulo, o programa *Smart* Sampa conta com cerca de 20 mil câmeras inteligentes, muitas com reconhecimento facial, instaladas em pontos estratégicos como o centro histórico e áreas movimentadas.

Já o Muralha Paulista, que cobre todo o estado, traz mais de 7 mil câmeras conectadas a sistemas avançados de análise, criadas em 2023 para combater o crime. Juntas, essas redes formam mais de 25 mil câmeras na capital e outras muitas pelo interior. Essas câmeras podem, eventualmente, ser aproveitadas para o programa de digitalização da segurança proposto neste caderno e, no caso da segurança contra incêndio. Elas podem ser atualizadas com algoritmos de inteligência artificial (IA) e/ou sensores térmicos, de forma a identificar princípios de incêndio, fumaça e calor, ajudando na detecção inteligente sem grandes investimentos com equipamentos totalmente novos.

Além das câmeras, o estado de SP já possui centrais de monitoramento destinadas à segurança pública. O Centro de Gestão Integrada de Segurança Pública, por exemplo, acompanha dados em tempo real, como vídeos e informações de emergência. Esse centro pode ser ampliado com as medidas propostas neste caderno para a segurança urbana, mobilidade inteligente, prevenção de desastres e proteção ambiental, e no caso da segurança contra incêndio, para receber alertas de incêndios por meio de sensores, câmeras e drones.

O *Smart* Sampa também tem uma central ativa desde 2024, conectando órgãos como o SAMU (Serviço de Atendimento Móvel de Urgência) e o Corpo de Bombeiros, o que facilita a coordenação de respostas em tempo real na capital. No caso do Muralha Paulista, os sistemas de análise de dados usados para prever crimes podem ser expandidos para também processar informações de incêndios, tornando a resposta mais rápida e organizada em todo o estado.

Drones também são equipamentos importantes que já são usados no estado de São Paulo. A polícia estadual, dentro do contexto do programa Muralha Paulista, usa drones para vigiar áreas de risco e monitorar eventos e regiões com grande densidade populacional. Da mesma forma que para as câmeras e centrais de monitoramento, os drones podem ser aprimorados para as medidas de vigilância urbana, patrulhamento automatizado e resposta a emergências de segurança apresentadas neste caderno, e no caso da segurança contra incêndio, os drones podem ser adaptados com câmeras térmicas ou sensores de fumaça e calor para que, sobrevoando regiões, possam identificar incêndios. Isso é especialmente útil em cidades menores e regiões rurais, sem câmeras e sem corpos de bombeiros, onde a distância pode aumentar os tempos de resposta aos sinistros. Reaproveitar esses equipamentos reduz custos e aproveita o que já está disponível, tornando a implantação mais prática.

A Tabela 7.2 apresenta de modo resumido a infraestrutura atual de inteligência encontrada no Estado de São Paulo

Tabela 7.2 – Infraestrutura atual de inteligência no Estado de São Paulo

Equipamentos	Programas originados	Aprimoramentos necessários	Outras aplicações além da SCI
Câmeras de Vigilância	Muralha Paulista, *Smart* Sampa	Inclusão de sensores térmicos, detecção de fumaça e calor com IA.	Monitoramento de tráfego (mobilidade), segurança pública, controle de multidões, detecção de eventos críticos.
Centrais de Monitoramento	*Smart* Sampa	Integração de alertas de incêndio, ampliação da capacidade de resposta multissetorial.	Coordenação de serviços emergenciais (SAMU, Defesa Civil), gestão de desastres naturais, vigilância urbana.
Drones	Muralha Paulista	Instalação de câmeras térmicas e sensores de fumaça; rotas programadas para áreas remotas.	Inspeção de áreas de risco (alagamentos, deslizamentos), apoio em operações policiais, mapeamento urbano e rural.
Sistemas de Análise de Dados	Muralha Paulista, *Smart* Sampa	Inclusão de algoritmos para detecção e previsão de incêndios, integração com sensores diversos.	Apoio à tomada de decisão em planejamento urbano, resposta a emergências, controle ambiental, segurança integrada.
Infraestrutura de conectividade (rede e energia)	Programas estaduais e municipais	Garantia de disponibilidade para equipamentos críticos, integração com sistemas locais e regionais.	Suporte a sensores ambientais, iluminação inteligente, semáforos conectados, sistemas de saúde digital e outros.

A infraestrutura existente demonstra que o Estado de São Paulo possui uma base sólida para expandir a digitalização em suas cidades, facilitando a implantação de tecnologias inovadoras. A utilização e adaptação de equipamentos já instalados reduzem custos e tornam o projeto de cidades inteligentes mais viável. Dessa forma, a modernização dos serviços urbanos pode ocorrer de maneira mais eficiente, garantindo maior conectividade, automação e qualidade de vida para a população.

Referências bibliográficas

1. SÃO PAULO (Estado). **Programa muralha paulista**. 2024. Disponível em: https://www.ssp.sp.gov.br/muralha-paulista. Acesso em: 15 abr. 2025.

2. SÃO PAULO (Cidade). Decreto nº 63.552, de 4 de julho de 2024. Cria o Programa Smart Sampa, destinado a promover a adoção de soluções tecnológicas inovadoras e avançadas para a melhoria da gestão pública e o aprimoramento da segurança pública, forma e condições que especifica. **Diário Oficial do Município**, São Paulo, 05 jul. 2024. Disponível em: https://legislacao.prefeitura.sp.gov.br/leis/decreto-63552-de-4-de-julho-de-2024/detalhe. Acesso em: 15 abr. 2025.

ANEXOS

ANEXO A

Documentos Legais e Normas Técnicas

A.1 Documentos Legais

O ordenamento jurídico tem por finalidade regulamentar as relações sociais para garantir a paz e a segurança jurídica de um país. No Brasil é caracterizado como um conjunto de normas jurídicas escritas e interdependentes, que segue predominantemente o Sistema "Civil Law" (sistema jurídico que se baseia na lei escrita também conhecida como sistema romano-germânico ou direito continental), dispostas hierarquicamente com obediência ao princípio da supremacia constitucional.

Desta forma, a hierarquia das leis brasileiras está organizada de acordo com a "Pirâmide de Kensel" (representação gráfica do sistema hierárquico de um Estado, criada pelo jurista e filósofo austríaco Hans Kelsen) tendo como base a teoria do direito constitucional, em que as de menor grau obedecem às normas de maior grau, iniciando a pirâmide pelo topo com a Carta Magna, assim dispostas.

Normas Constitucionais

Constituição Federal de 1988

No topo do ordenamento jurídico brasileiro estão a Constituição e todas as suas emendas, que servem de parâmetro de validade a todas as demais espécies normativas. Entre as normas constitucionais tem-se: (a) as **normas constitucionais originárias** (elaboradas pelo Poder Constituinte Originário, ou seja, poder que desenvolve uma nova constituição; (b) as **normas constitucionais derivadas** (emendas que foram adicionadas à Constituição Federal posteriormente à sua promulgação pelo Poder Constituinte Derivado, ou seja, poder que altera a Constituição).

Tratados Internacionais de Direitos Humanos

Os tratados internacionais de direitos humanos aprovados por meio do rito ordinário são nomeados supralegais, isto é, ficam abaixo da Constituição e de suas emendas e acima das demais normas legais. Porém, já são considerados infraconstitucionais.

Normas Infraconstitucionais

Abaixo dos tratados internacionais de direitos humanos estão situadas as normas infraconstitucionais. São elas: as leis (complementares, ordinárias e delegadas), as medidas provisórias, os decretos legislativos, as resoluções e os tratados internacionais de direitos humanos aprovados por meio do rito ordinário.

Leis Complementares

São aquelas regulamentadas com a intenção de complementar e explicar a Constituição por exigência da mesma, ou seja, em casos onde a Constituição Federal estabelecer que haja uma lei específica para regulamentar a matéria em questão, é criada uma lei complementar.

Leis Ordinárias

São normas jurídicas que tratam de assuntos de competência do Estado, como direitos e deveres dos cidadãos, organização dos poderes, e políticas públicas. As leis ordinárias têm a função de complementar as normas constitucionais que não foram tratadas pelas leis complementares.

Leis Delegada

São normas jurídicas elaboradas pelo Poder Executivo, com autorização do Poder Legislativo, que permite ao Executivo legislar sobre determinados assuntos.

Medidas Provisórias

Editadas pelo Poder Executivo em casos de relevância e urgência, com prazo para conversão em lei pelo Congresso Nacional.

Normas Infralegais

As normas infralegais são regulamentos, decretos, portarias, resoluções e instruções normativas editadas por órgãos administrativos para detalhar e facilitar a aplicação das leis infraconstitucionais. Essas normas não podem criar obrigações novas ou ir além do escopo das leis que as autorizam, servindo principalmente para organizar a administração pública e assegurar que a lei seja implementada corretamente. Tem-se:

Decretos

Emitidos pelo Presidente da República, governadores de estado e prefeitos. Esses decretos são instrumentos normativos utilizados para regulamentar leis federais, estaduais ou municipais e organizar a administração pública.

Portarias

Atos normativos editados por uma ou mais autoridades singulares, por meio das quais são expedidas instruções sobre organização e funcionamento de serviços e outros atos de sua competência.

Resoluções

São atos normativos editados por colegiados legalmente instituídos

Instruções normativas

São atos administrativos que complementam leis e decretos, disciplinando a execução de atividades. São expedidas por autoridades administrativas com o objetivo de orientar agentes públicos para padronizar rotinas e atividades, e garantir a continuidade do serviço público.

Hierarquia entre Leis

No sistema jurídico brasileiro ainda existe uma hierarquia entre leis federais, estaduais, municipais ou distritais, fundamentada na distribuição de competências estabelecida pela Constituição Federal.

Leis federais

Têm alcance nacional e supremacia sobre as demais, abordando matérias de competência exclusiva da União ou em casos de conflitos entre legislações de diferentes esferas.

Leis estaduais

São aplicáveis dentro dos limites de cada estado, seguindo as diretrizes federais e abrangendo questões não exclusivas da União nem municipais.

Leis municipais

Regem dentro dos municípios e devem alinhar-se às leis federais e estaduais, focando em assuntos de interesse local como urbanismo e serviços públicos.

Principais documentos referentes à Segurança

Dentre os documentos legais, tanto de cunho geral como específicos para Segurança, merecem destaque os indicados na Tabela A.1.

Tabela A.1.1 – Principais documentos legais referentes à segurança

Documento	Descrição	Link
Lei N°10.257 de 10.07.2001 (federal)	Regulamenta os arts. 182 e 183 da Constituição Federal, estabelece diretrizes gerais da política urbana e dá outras providências..	https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm
Lei nº 11.901 de 12.01.2009 (federal)	Dispõe sobre a profissão de Bombeiro Civil e dá outras providências.	http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/L11901.htm
Lei n°12608 de 10.04.2012 (federal)	Institui a Política Nacional de Proteção e Defesa Civil - PNPDEC; dispõe sobre o Sistema Nacional de Proteção e Defesa Civil - SINPDEC e o Conselho Nacional de Proteção e Defesa Civil - CONPDEC; autoriza a criação de sistema de informações e monitoramento de desastres; altera as Leis nºs 12.340, de 1º de dezembro de 2010, 10.257, de 10 de julho de 2001, 6.766, de 19 de dezembro de 1979, 8.239, de 4 de outubro de 1991, e 9.394, de 20 de dezembro de 1996; e dá outras providências	https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12608.htm
Lei N°12.965 de23.04.20214 (federal)	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.	https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
Lei Complementar Nº 1.257 de 06.01.2015 (estadual)	Institui o Código Estadual de Proteção Contra Incêndios e Emergências e dá providências correlatas	https://www.al.sp.gov.br/repositorio/legislacao/lei.complementar/2015/lei.complementar-1257-06.01.2015.html
Lei N° 16.111 de 14.01.2016 (estadual)	Autoriza o Poder Executivo a liberar recursos para os municípios investirem em segurança, exclusivamente para as guardas municipais	https://www.al.sp.gov.br/norma/176986
Lei nº 13.425 de 30.03.2017 (federal)	Estabelece diretrizes gerais sobre medidas de prevenção e combate a incêndio e a desastres em estabelecimentos, edificações e áreas de reunião de público; altera as Leis nº s 8.078, de 11 de setembro de 1990, e 10.406, de 10 de janeiro de 2002 – Código Civil; e dá outras providências.	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13425.htm
Lei N° 13675 de 11.06.2018 (federal)	Disciplina a organização e o funcionamento dos órgãos responsáveis pela segurança pública, nos termos do § 7º do art. 144 da Constituição Federal; cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS); institui o Sistema Único de Segurança Pública (Susp); altera a Lei Complementar nº 79, de 7 de janeiro de 1994, a Lei nº 10.201, de 14 de fevereiro de 2001, e a Lei nº 11.530, de 24 de outubro de 2007; e revoga dispositivos da Lei nº 12.681, de 4 de julho de 2012.	https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm
Lei Nº 13.709 de 14.08.2018 (federal)	Lei Geral de Proteção de Dados Pessoais (LGPD)	https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
Lei N°13.089 de 12.01.2019 (federal)	Esta Lei, denominada Estatuto da Metrópole, estabelece diretrizes gerais para o planejamento, a gestão e a execução das funções públicas de interesse comum em regiões metropolitanas e em aglomerações urbanas instituídas pelos Estados, normas gerais sobre o plano de desenvolvimento urbano integrado e outros instrumentos de governança interfederativa, e critérios para o apoio da União a ações que envolvam governança interfederativa no campo do desenvolvimento urbano, com base nos incisos XX do art. 21 , IX do art. 23 e I do art. 24 , no § 3º do art. 25 e no art. 182 da Constituição Federal .	https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13089.htm
Portaria nº 108 de 12.07.2019 (federal)	Institui o Modelo Nacional de Regulamento de Segurança Contra Incêndio e Emergências	https://www.in.gov.br/web/dou/-/portaria-n-108-de-12-de-julho-de-2019-201842597

Portaria n°3027 de 04.12.2020	Define procedimentos para o envio de alertas à população sobre a possibilidade de ocorrência de desastres, em articulação com os órgãos e entidades estaduais, distritais e municipais de proteção e defesa civil, e para utilização do sistema Interface de Divulgação de Alertas Públicos para envio de alertas via mensagem de texto (SMS), televisão por assinatura ou plataforma de avisos públicos.	https://www.in.gov.br/en/web/dou/-/portaria-n-3.027-de-4-de-dezembro-de-2020-292327843
Lei nº 14.133 de 01.04.2021 (federal)	Lei de Licitações e Contratos Administrativos	https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm
Decreto N° 10.777 de24.08.2021 (federal)	Institui a Política Nacional de Inteligência de Segurança Pública.	https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10777.htm
Decreto N° 10.822 de 28.09.2021 (federal)	Institui o Plano Nacional de Segurança Pública e Defesa Social 2021-2030.	https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10822.htm
Portaria Inmetro N°62 de 17 de fevereiro de 2022 (federal)	Aprova o Regulamento Técnico da Qualidade e os Requisitos de Avaliação da Conformidade para Luminárias para a Iluminação Pública Viária	http://www.inmetro.gov.br/legislacao/detalhe.asp?seq_classe=1&seq_ato=2921
Ato Anatel N°17087 de 19.12.2022 (federal)	Estabelecer os requisitos de segurança elétrica, para fins de Avaliação da Conformidade e Homologação junto à Agência Nacional de Telecomunicações - Anatel,	https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2022/1823-ato-17087
Decreto N°11.615 de 21.07.2023 (federal)	Regulamenta a Lei nº 10.826, de 22 de dezembro de 2003, para estabelecer regras e procedimentos relativos à aquisição, ao registro, à posse, ao porte, ao cadastro e à comercialização nacional de armas de fogo, munições e acessórios, disciplinar as atividades de caça excepcional, de caça de subsistência, de tiro desportivo e de colecionamento de armas de fogo, munições e acessórios, disciplinar o funcionamento das entidades de tiro desportivo e dispor sobre a estruturação do Sistema Nacional de Armas - Sinarm.	https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11615.htm#art83
Portaria Inmetro N° 601 de 14.12.2023	Altera a Portaria Inmetro nº 221, de 23 de maio de 2022.	https://www.in.gov.br/en/web/dou/-/portaria-n-601-de-14-de-dezembro-de-2023-533945099
Decreto N°12.041 de 05.06.2024 (federal)	Instituí o Programa Cidades Verdes Resilientes – PCVR, com o objetivo de aumentar a qualidade ambiental e a resiliência das cidades brasileiras diante dos impactos causados pela mudança do clima, por meio da integração de políticas urbanas, ambientais e climáticas, do estímulo às práticas sustentáveis e da valorização dos serviços ecossistêmicos do verde urbano.	https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/d12041.htm
Decreto N° 63.552 de 04.07.2024 (do município de São Paulo	Cria o Programa Smart Sampa, destinado a promover a adoção de soluções tecnológicas inovadoras e avançadas para a melhoria da gestão pública e o aprimoramento da segurança pública, forma e condições que especifica.	https://legislacao.prefeitura.sp.gov.br/leis/decreto-63552-de-4-de-julho-de-2024/detalhe
Decreto N°68.828 de 04.09.2024 (estadual)	Institui o Programa Muralha Paulista e dá providências correlatas	https://www.al.sp.gov.br/repositorio/legislacao/decreto/2024/decreto-68828-04.09.2024.html
Decreto Nº 69.118 de 09.12.2024 (estadual)	Institui o regulamento de Segurança Contra Incêndios das edificações e áreas de risco no Estado de São Paulo e dá providências correlatas.	https://www.al.sp.gov.br/repositorio/legislacao/decreto/2024/decreto-69118-09.12.2024.html

Tabela A.1.2 – Documentos do corpo de bombeiro do Estado de São Paulo

Documento	Descrição	Link
Corpo de bombeiros Instrução técnica Nº01/2025 (estadual)	Estabelece critérios para o processo de segurança contra incêndio das edificações e áreas de risco, atendendo ao previsto no Regulamento de Segurança contra Incêndio em edificações e áreas de risco.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº05/2025 (estadual)	Estabelece condições para o deslocamento de viaturas de bombeiros nas vias públicas, possibilitando o acesso para as operações do Corpo de Bombeiros Militar, nas edificações e áreas de risco do Estado de São Paulo.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 06/2025 (estadual)	Estabelece as condições mínimas para o acesso de viaturas de bombeiros nas edificações e áreas de risco, visando o emprego operacional do Corpo de Bombeiros da Polícia Militar do Estado de São Paulo, atendendo ao previsto no Regulamento de segurança contra incêndio das edificações e áreas de risco do Estado de São Paulo.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 14/2025 (estadual)	Estabelece valores característicos de carga de incêndio nas edificações e áreas de risco, conforme a ocupação e uso específico.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 16/2025 (estadual)	1.1 Fomentar a cultura de gerenciamento de riscos de incêndios, bem como acidentes e demais emergências, nas organizações responsáveis pelas edificações e/ou áreas de risco. 1.2 Estabelecer princípios e requisitos mínimos necessários para tornar o gerenciamento eficaz. 1.3 Recomendar o desenvolvimento, implantação e aperfeiçoamento contínuo desse processo, visando a proteção da vida, do meio ambiente e do patrimônio, bem como viabilizar a continuidade dos negócios. 1.4 Estabelecer os requisitos mínimos para a elaboração, manutenção e revisão de um plano de emergência contra incêndio, acidentes e demais emergências. 1.5 Fornecer informações operacionais das edificações ou áreas de risco, padronizando, fornecendo e alocando plantas de riscos nas edificações para otimizar o atendimento operacional prestado pelo CBPMESP.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº. 19/2025 (estadual)	Estabelece os requisitos mínimos necessários para o dimensionamento dos sistemas de detecção e alarme de incêndio, destinado a alertar as pessoas sobre a existência de um incêndio em determinada área da edificação, desta forma, possibilitando o seu combate logo que descoberto, bem como, propiciando o abandono da edificação sem que os ocupantes sofram qualquer dano.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 20/2025 (estadual)	Fixa as condições exigíveis que devem satisfazer o sistema de sinalização de emergência em edificações e áreas de risco, atendendo ao previsto no Regulamento de segurança contra incêndio das edificações e áreas de risco do Estado de São Paulo, excetuando-se os túneis destinados ao transporte rodoviário, cuja sinalização de emergência deverá atender ao disposto na Instrução Técnica n° 35.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 32/2025 (estadual)	Estabelece os parâmetros para prevenir, controlar e minimizar emergências ambientais que provoquem riscos à vida, ao meio ambiente e ao patrimônio em edificações e áreas de risco, atendendo ao previsto no Regulamento Segurança Contra Incêndio das edificações e áreas de risco do Estado de São Paulo.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 42/2025 (estadual)	Estabelece procedimentos administrativos e as medidas de segurança contra incêndio para licenciamento das edificações enquadradas no Projeto Técnico Simplificado (PTS), visando à celeridade do licenciamento nos termos do Regulamento de segurança contra incêndio das edificações e áreas de risco do Estado de São Paulo.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta
Corpo de Bombeiros Instrução técnica Nº 44/2025 (estadual)	Fomenta boas práticas para a proteção ao meio ambiente, para a construção sustentável e o estímulo à adoção de padrões sustentáveis de produção e consumo de bens e serviços, atendendo às exigências do Regulamento de segurança contra incêndio das edificações e áreas de risco do Estado de São Paulo.	https://cbaplang.corpodebombeiros.sp.gov.br/internetCB/#/LegislacaoConsulta

Tão importante quando as leis indicadas na Tabela A.1.1 é a Carta Brasileira para Cidades Inteligentes1, documento de referência, lançado em 2020, que define um conceito de cidades inteligentes no Brasil e orienta políticas e programas sobre a transformação digital urbana. Ela traz 160 recomendações apoiadas em 8 objetivos estratégico (Tabela A.2.3).

Tabela A.1.3 – Objetivos estratégicos da Carta Brasileira para Cidades Inteligentes

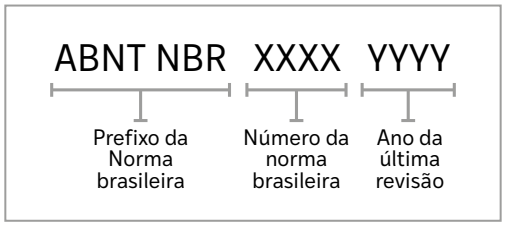
Objetivo 1	Integrar a transformação digital nas políticas, programas e ações de desenvolvimento urbano sustentável, respeitando as diversidades e considerando as desigualdades presentes nas cidades brasileiras.
Objetivo 2	Prover acesso equitativo à internet de qualidade para todas as pessoas.
Objetivo 3	Estabelecer sistemas de governança de dados e de tecnologias, com transparência, segurança e privacidade.
Objetivo 4	Adotar modelos inovadores e inclusivos de governança urbana e fortalecer o papel do poder público como gestor de impactos da transformação digital nas cidades.
Objetivo 5	Fomentar o desenvolvimento econômico local no contexto da transformação digital.
Objetivo 6	Estimular modelos e instrumentos de financiamento do desenvolvimento urbano sustentável no contexto da transformação digital.
Objetivo 7	Fomentar um movimento massivo e inovador de educação e comunicação públicas para maior engajamento da sociedade no processo de transformação digital e de desenvolvimento urbanos sustentáveis
Objetivo 8	Construir meios para compreender e avaliar, de forma contínua e sistêmica, os impactos da transformação digital nas cidades

A.2. Normas Técnicas

Normas técnicas são procedimentos estabelecidos por consenso entre as partes interessadas. Possibilitam a criação de uma linguagem comum, reduzem a variabilidade de interpretações e sistematizam a formulação e aplicação de regras.

Há vários tipos de normas, cada qual com sua finalidade, como por exemplo, as de terminologia, de processos e de serviços, entre várias.

No Brasil é a Associação Brasileira de Normas Técnicas (ABNT) que tem a missão de prover a sociedade brasileira com documentos normativos. Para a elaboração das normas ela conta com Comitês Técnicos, que coordenam, planejam e executam as atividades de normalização relacionadas ao seu âmbito de atuação. As normas ABNT são consideradas normas brasileiras, por isso são codificadas como ABNT NBR e são escritas como indicado abaixo.



A ABNT dispõe de um catálogo de normas, por meio do qual elas podem ser adquiridas. O número da norma não muda, mas elas passam por revisões, portanto é importante ao usar uma norma verificar se ela se refere à última edição.

As normas não têm obrigatoriedade de atendimento, exceto quando são citadas em documentos legais como acontece, por exemplo, na Lei Federal N°8.078 de 11 de setembro de 1990 (Código de Defesa do Consumidor). Por outro lado, na falta de documentos legais as normas brasileiras (ABNT NBR) frequentemente são usadas como tal.

As normas também têm alcances diferentes, podendo ser: internacionais, por exemplo, as normas da *Internationla Organization for Standardization* (ISO); regionais, por exemplo, as normas do Comitê Europeu (EU); sub-regionais, por exemplo, as normas MERCOSUL; nacionais, que são referentes a um país, como por exemplo, as normas da ABNT NBR.

A ABNT é membro fundador da ISO e sempre que internaliza norma desta instituição deve colocar a sigla ISO no prefixo da norma, que passa a ser ABNR NBR ISO.

Normas Técnicas de Aplicação Geral

Dentre as normas técnicas de aplicação geral merecem destaques as que seguem, que podem ser adquiridas por meio do Catálogo de Normas ABNT[2].

- ABNT NBR ISO 37101:2017. Versão corrigida 2021. Emenda 1:2024 – Desenvolvimento sustentável de comunidades- Sistema de gestão para desenvolvimento sustentável - Requisitos com orientação para uso.

  Esta norma estabelece requisitos para um sistema de gestão para desenvolvimento sustentável em comunidades, incluindo cidades, utilizando uma abordagem holística, visando assegurar a coerência com a política para desenvolvimento sustentável de comunidades.

- ABNT NBR ISO 37104:2024. - Cidades de comunidades sustentáveis. Transformando nossas cidades – Recomendações para a implementação prática da ABNT NBR ISO 37101 no âmbito local.

  Este documento fornece orientações sobre como implementar e manter um sistema de gestão para o desenvolvimento sustentável com base nos princípios da ABNT NBR ISO 37101, especificamente no contexto das cidades, mas aplicável a outras formas de assentamento. Estabelece uma estrutura metodológica para avaliação sistemática as iniciativas e resultados para o desenvolvimento sustentável na cidade ou em outros assentamentos, cm base na análise cruzada dos seis propósitos de sustentabilidade e das 12 áreas de ação da ABNT NBR ISO 37101.

- ABNT NBR ISO 37120:2021 - Cidades e comunidades sustentáveis - Indicadores para serviços urbanos e qualidade de vida

  Esta norma define e estabelece metodologias para um conjunto de indicadores, a fim de orientar e medir o desempenho de serviços urbanos e qualidade de vida. Ela se aplica a qualquer cidade, municipalidade ou governo local que intencione medir seu desempenho de uma forma comparável e verificável, independentemente do tamanho e da localização.

  Os indicadores contidos nesta norma podem ser utilizados para rastrear e monitorar o progresso do desempenho da cidade e assim avaliar a gestão de seus serviços urbanos e de sua prestação de serviços.

- ABNT NBR ISO 37122:2020. Versão corrigida 2021. Errata 1:2021. - Cidades e comunidades sustentáveis - Indicadores para cidades inteligentes

  Esta norma especifica e estabelece definições e metodologias para um conjunto de indicadores de cidades inteligentes. Ela se aplica a qualquer cidade, municipalidade ou governo local que intencione medir seu desempenho de uma forma comparável e verificável, independentemente do tamanho e da localização. Ela, juntamente coma ABNT NBR ISO 37120, se destina a fornecer um conjunto completo de indicadores para medir o progresso em direção a uma cidade inteligente.

- ABNT NBR ISO 37123:2021 - Cidades e comunidades sustentáveis - Indicadores para cidades resilientes

  Esta norma especifica e estabelece definições e metodologias para um conjunto de indicadores de cidades resilientes. Ela se aplica a qualquer cidade, municipalidade ou governo local que intencione medir seu desempenho de uma forma comparável e verificável, independentemente do tamanho e da localização. Ela, juntamente coma ABNT NBR ISO 37120, se destina a fornecer um conjunto completo de indicadores para medir o progresso em direção a uma cidade resiliente.

Normas técnicas relacionadas ao Caderno Técnico Segurança

A Tabela A.2.1 relaciona as normas citadas nesse caderno.

Tabela A.2.1 – Principais normas técnicas referentes à segurança

Documento	Descrição	Link
ABNT NBR 17240:2010	Sistemas de detecção e alarme de incêndio	Requisitos para projeto, instalação e manutenção de sistemas de detecção e alarme de incêndio.
ABNT NBR 14023:2024	Registro de dados de ocorrências de incêndios e emergências	Estabelece um sistema para padronização do registro de dados, contendo o mínimo necessário para o seu processamento apropriado por órgãos ou instituições competentes, para fins estatísticos e, quando aplicável, legais.
Família ABNT NBR ISO 7240, tem 31 partes e vai de 2017 a 2025	Sistemas de detecção e alarme de incêndio	Especifica um conjunto de diretrizes gerais e definições utilizadas para descrever o sistema de detecção e alarme de incêndio, equipamentos instalados dentro e ao redor de edificações, e os ensaios e requisitos para estes equipamentos em outras partes da ISO 7240. Cada parte (31 no total) dessa família de Norma trata de um componente específico do sistema de detecção e alarme.
ABNT NBR 13570:2021	Instalações elétricas em locais de afluência de público — Requisitos específicos	Esta Norma estabelece os requisitos específicos para as instalações elétricas em locais de afluência de público, a fim de garantir o seu funcionamento adequado, a segurança de pessoas e de animais domésticos e a conservação dos bens.
ABNT NBR 10898:2023	Sistema de iluminação de emergência	Esta Norma especifica os requisitos mínimos para os sistemas de iluminação de emergência a serem instalados nas edificações ou em áreas e passagens onde tais sistemas são requeridos, na falta de iluminação natural ou falha da iluminação normal instalada.
ABNT NBR IEC 62676-1-1:2019	Sistemas de videomonitoramento para uso em aplicações de segurança Parte 1-1: Requisitos de sistema — Generalidades	Esta Parte da ABNT NBR IEC 62676 especifica os requisitos mínimos e fornece as recomendações para os sistemas de videomonitoramento (VSS), até agora chamados de CFTV, instalados para as aplicações de segurança. Esta Norma especifica os requisitos mínimos de desempenho e os requisitos funcionais a serem acordados entre o cliente, os órgãos responsáveis pela aplicação das leis, quando aplicável, e o fornecedor nos requisitos operacionais, mas não inclui requisitos de projeto, planejamento, instalação, ensaios, operação ou manutenção.
ABNT NBR IEC 62676-1-2:2019	Sistemas de videomonitoramento para uso em aplicações de segurança Parte 1-2: Requisitos de sistema — Requisitos de desempenho para transmissão de vídeo	Esta Parte da ABNT NBR IEC 62676 apresenta os requisitos gerais de transmissão de vídeo. Esta Norma abrange os requisitos gerais para transmissão de vídeo relativos ao desempenho, a segurança e a conformidade à conectividade IP básica, baseada nas normas internacionais disponíveis bem conhecidas.
ABNT NBR 5410: 2004- Versão corrigida 2008	Instalações elétricas de baixa tensão	Esta Norma estabelece as condições a que devem satisfazer as instalações elétricas de baixa tensão, a fim de garantir a segurança de pessoas e animais, o funcionamento adequado da instalação e a conservação dos bens.
ABNT NBR ISO/ IEC 27001:2022 Versão Corrigida:2023	Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos	Este documento especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Este documento também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos estabelecidos neste documento são genéricos e destinam-se a ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.
ABNT NBR ISO/ IEC 27004:2017 Versão corrigida 2023	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação	Este documento fornece orientações que têm como objetivo auxiliar as organizações a avaliarem o desempenho da segurança da informação e a eficácia do SGSI a fim de atender aos requisitos da ABNT NBR ISO/IEC 27001:2013.
ABNT NBR ISO/IEC 27003:2020	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações	Este documento fornece explicações e orientações sobre a aplicação da ABNT NBR ISO/IEC 27001:2013.
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação	Este documento fornece um conjunto de referência de controles genéricos de segurança da informação, incluindo orientação para implantação.

ABNT NBR 14276:2020	Brigada de incêndio e emergência - Requisitos e procedimentos	Esta Norma estabelece os requisitos e procedimentos para composição, treinamento e atividades das brigadas de emergência de incêndio, para proteger a vida e o patrimônio, bem como para reduzir as consequências sociais e os danos ao meio ambiente.
ABNT NBR 14096:2016. Versão corrigida 2021	Viaturas de combate a incêndio – Requisitos	Esta Norma estabelece as condições mínimas exigíveis para o projeto, fabricação, desempenho e ensaio de viaturas de combate a incêndio. Aplica-se a viaturas novas para combate a incêndio urbano, com ou sem bombeamento e apoio às operações associadas aos Corpos de Bombeiros públicos e privados.
ABNT NBR 15219:2020	Plano de emergência — Requisitos e procedimentos	Esta Norma especifica os requisitos e procedimentos para a elaboração, implantação e manutenção de um plano de emergência contra incêndio, para proteger a vida e o patrimônio, bem como reduzir as consequências sociais e os danos ao meio ambiente.
Família ABNT NBR 15965:2011 a 2022	Sistema de classificação da informação da construção	Define um sistema de classificação para informações da construção, essencial para a implantação do BIM (Building Information Modeling). Família dividida em 7 partes.
ABNT NBR 14608:2021	Bombeiro civil - Requisitos e procedimentos	Esta Norma estabelece os requisitos e procedimentos para composição, treinamento e atuação de bombeiros civis, para proteger a vida e o patrimônio, bem como reduzir as consequências sociais e os danos ao meio ambiente.
ABNT NBR 14561:2000	Veículos para atendimento a emergências médicas e resgate	Esta Norma fixa as condições mínimas exigíveis para o projeto, construção e desempenho de veículos para atendimento a emergências médicas e resgate, descrevendo veículos que estão autorizados a ostentar o símbolo "estrela da vida" e a palavra "resgate", estabelecendo especificações mínimas, parâmetros para ensaio e critérios essenciais para desempenho, aparência e acessórios, visando propiciar um grau de padronização para estes veículos.
ABNT NBR ISO/IEC 27557:2023	Segurança da Informação, segurança cibernética e proteção da privacidade — Aplicação da ABNT NBR ISO 31000:2018 para gestão de riscos de privacidade organizacional	Este Documento fornece diretrizes para gestão de riscos de privacidade organizacional, estendido da ABNT NBR ISO 31000:2018.
ABNT NBR ISO 31000:2018	Gestão de riscos – Handbook orientativo	O objetivo deste handbook é auxiliar as organizações que buscam orientações sobre como integrar a gestão de riscos e suas atividades. O handbook inclui, portanto, informações sobre os princípios de gestão de riscos, estrutura, papéis e responsabilidade, planejamento, processos, comunicação, monitoramento e análise crítica, e melhoria contínua.
ABNT NBR 5101:2024	Iluminação viária — Procedimentos	Esta Norma especifica os requisitos mínimos para a iluminação de vias de domínio público e privado, de forma a propiciar segurança aos tráfegos de pedestres e veículos.

Referências Bibliográficas

1. MINISTÉRIO DAS CIDADES. **Política Nacional de Desenvolvimento Urbano**. Brasília: MC, 2018. Disponível em: https://sites.tcu.gov.br/relatorio-de-politicas/2018/politica-nacional-de-desenvolvimento-urbano.htm. Acesso em: 9 abr. 2025.

2. INSTITUTO DE PESQUISA DE ECONÔMICA APLICADA. 11 - **Cidades e Comunidades Sustentáveis**. Disponível em: https://www.ipea.gov.br/ods/ods11.html. Acesso em: 9 abr. 2025.

3. MINISTÉRIO DAS CIDADES. **Carta Brasileira Cidades Inteligentes**. Disponível em https://www.gov.br/cidades/pt-br/acesso-a-informacao/acoes-e-programas/desenvolvimento-urbano-e-metropolitano/projeto-andus/carta-brasileira-para-cidades-inteligentes. Acesso em: 8 abr. 2025.

4. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Consulta ao catálogo. Rio de Janeiro, ABNT, 2025. Disponível em: https://www.abntcatalogo.com.br/. Acesso em: 09 mar. 2025

ANEXO B

Inteligência Artificial: Conceitos e Desafios

B.1 Introdução

Até pouco tempo atrás, a Inteligência Artificial (IA) era algo presente somente em laboratórios de pesquisas científicas. Para o público em geral, era conhecida apenas em filmes de ficção científica. Atualmente, essa realidade mudou completamente, o tema tem se difundido por todas as mídias e já se pode observar o uso de IA no dia a dia das pessoas. Isso está acontecendo diante dos grandes avanços recentes nesse campo, que permitiram o desenvolvimento de aplicações práticas que estão revolucionando as mais diversas áreas de atuação humana[1].

Os primeiros estudos formais de IA surgiram nos anos 1950, com pesquisadores como Allen Newell e Herbert Simon nos EUA, mas o campo evoluiu enormemente desde então. No século XXI, a IA ganhou protagonismo graças ao aumento do poder computacional, do volume de dados disponíveis e de avanços em algoritmos de *machine learning* (aprendizado de máquina), *deep learning* (aprendizado profundo) e outras subáreas[2].

De forma simplificada, podemos dizer que a Inteligência Artificial (IA) consiste em simular mecanismos de raciocínio humano por meio da computação, com algoritmos que podem analisar grandes quantidades de dados[3], tomar decisões com base em regras ou padrões aprendidos e "acumular conhecimento" durante o processo[1]. A importância da utilização da IA na administração pública cresce à medida que as cidades enfrentam problemas cada vez mais complexos e lidam com volumes massivos de dados[4]. O conceito de cidades inteligentes surgiu nesse contexto, exatamente para destacar o uso efetivo de tecnologias digitais na gestão urbana. IA pode ser peça-chave ao ser adotada por prefeituras e órgãos públicos, abrindo novas possibilidades para o planejamento urbano, a prestação de serviços e o atendimento às demandas da população de forma mais ágil, personalizada e com menor custo[4].

Em vez de decisões baseadas apenas na intuição, os gestores passam a dispor de ferramentas que permitem extrair informações relevantes de grandes volumes de dados digitais, gerando maior eficiência no uso de recursos públicos e uma nova forma de tomar decisões, orientada por evidências. Isso significa que as informações obtidas com o uso de tecnologias digitais e IA permitem que se tenha uma espécie de camada invisível sobre o mapa de uma cidade, que auxilia a mensurar muitos fatores antes imensuráveis.

Entre as principais aplicações da Inteligência Artificial (IA) na gestão pública destacam-se as indicadas na Figura B.1.1

Figura B.1.1. – Principais aplicações da IA na gestão pública [5, 6, 7].

Previsão	Utiliza informações históricas para antecipar situações futuras e apoiar decisões mais seguras e planejadas.
Reconhecimento de padrões	Analisa grandes volumes de dados para detectar tendências e comportamentos, permitindo respostas rápidas e eficazes.
Reconhecimento de imagens e vídeos	Facilita o monitoramento automático de situações ou problemas, aumentando a eficiência na gestão.
Processamento de linguagem natural	Possibilita que sistemas compreendam e processem textos e diálogos humanos, automatizando atendimentos e interpretando demandas.
Reconhecimento de voz e análise de sentimentos	Identificam rapidamente situações críticas e avaliam automaticamente o nível de satisfação das pessoas com os serviços oferecidos.
Sistemas de recomendação	Analisam dados passados para oferecer serviços adaptados às necessidades específicas dos cidadãos.
Gêmeos digitais	Criam modelos digitais da cidade, permitindo testar virtualmente ações e projetos antes de realizá-los na prática, reduzindo riscos e custos.
Sistemas de otimização	Ajudam a definir a melhor forma de usar recursos disponíveis, promovendo economia e sustentabilidade.

Essas aplicações, combinadas, capacitam as administrações públicas a atuar de forma mais proativa, inteligente e eficaz, potencializando os esforços governamentais em cumprir seu papel e melhorar a qualidade de vida das pessoas nas cidades.

B.2 Vantagens e Limitações do Uso de IA em Cidades Inteligentes

Vários benefícios do uso da Inteligência Artificial podem ser destacados. A Figura B.2.1 apresenta alguns.

Figura B.2.1. –Benefícios do uso da Inteligência Artificial

Maior eficiência de custos operacionais

Tarefas repetitivas ou análises complexas que tomariam horas dos servidores podem ser automatizadas, liberando a equipe para atividades de maior valor estratégico. Processos internos tornam-se mais ágeis e há economia de recursos no médio prazo.

Decisões mais embasadas e proatividade

Com a IA identificando padrões ocultos em bases de dados extensas, prefeituras conseguem prever eventos futuros ou necessidades, por exemplo antecipar demanda por certos serviços ou risco de ocorrências e planejar ações preventivas. A tomada de decisão torna-se mais científica, orientada por dados ao invés de intuições.

Melhoria nos serviços ao cidadão

Os moradores percebem a cidade "funcionando melhor". Isso aumenta a confiança do público na administração. Ferramentas como assistentes virtuais também ampliam a disponibilidade de atendimento (24/7) e a conveniência para o usuário, elevando a satisfação.

Transparência e controle

Muitos sistemas de IA vêm acompanhados de dashboards e indicadores em tempo real. Isso permite aos gestores acompanhar de perto a performance de serviços públicos e medir resultados de políticas quase que instantaneamente. Também pode-se disponibilizar parte desses dados para a população, aumentando a transparência das ações do governo local.

Apesar dos benefícios é preciso atentar aos obstáculos e cuidados ao introduzir IA na esfera municipal. A seguir são indicados alguns desafios.

Qualidade e disponibilidade dos dados

A eficácia de qualquer modelo de IA depende diretamente da quantidade e qualidade dos dados disponíveis para treiná-lo. Muitas prefeituras ainda enfrentam bases de dados fragmentadas entre secretarias, informações desatualizadas ou inconsistentes. É necessário investir em governança de dados, integrando bancos de dados das diversas áreas do município e garantindo que estejam limpos, atualizados e anonimizados quando contêm dados pessoais. Sem dados confiáveis, a IA pode gerar resultados imprecisos.

Infraestrutura tecnológica insuficiente

Algoritmos avançados demandam infraestrutura de TI adequada – conexões de internet rápidas, servidores ou serviços de nuvem com poder de processamento e armazenamento, e dispositivos IoT (sensores, câmeras) espalhados pela cidade para coletar informações. No Brasil, ainda há uma lacuna de conectividade, pois poucos municípios contam com cobertura 5G, recurso cada vez mais essencial para suportar aplicações urbanas inteligentes.

Capacitação técnica e recursos humanos

A presença de profissionais qualificados em ciência de dados, análise de dados e desenvolvimento de IA no quadro das prefeituras é necessária. O mercado de TI já demanda mais especialistas em IA do que as universidades conseguem formar, e o setor público compete com o privado por esse talento escasso. Assim, governos locais precisam investir na capacitação de suas equipes e/ou buscar parcerias para suprir essa expertise. Além disso, é importante promover uma cultura organizacional aberta à inovação, treinando também servidores não técnicos a interagir com as novas ferramentas.

Custos iniciais e sustentabilidade

Implementar IA pode exigir investimentos significativos na fase inicial – compra de equipamentos, contratação de sistemas ou consultorias, treinamento de pessoal. Para prefeituras com orçamento limitado, justificar esses gastos requer planejamento e talvez adoção gradual (projetos-piloto). Além disso, é preciso prever os custos de manutenção dessas soluções a longo prazo (atualizações, suporte técnico, renovação de licenças), evitando que projetos morram após o entusiasmo inicial por falta de recursos continuados.

Questões éticas, legais e de privacidade

O uso de IA na gestão pública traz responsabilidade de respeitar a privacidade dos cidadãos e evitar vieses discriminatórios. Sistemas de reconhecimento facial, por exemplo, levantam preocupações legais (conformidade com a Lei Geral de Proteção de Dados – LGPD) e éticas (possibilidade de identificar erroneamente alguém inocente). Decisões automatizadas precisam de transparência e supervisão humana, principalmente em áreas sensíveis como segurança e assistência social, para garantir que direitos individuais não sejam violados. As prefeituras devem implementar IA de forma responsável, com algoritmos auditáveis e adoção de diretrizes para evitar preconceitos embutidos nos modelos.

Em suma, a incorporação da Inteligência Artificial na gestão municipal deve ser feita com planejamento e cautela. Não se trata de uma solução mágica, mas sim de uma ferramenta poderosa que requer dados de qualidade, infraestrutura, pessoas capacitadas e bom senso na aplicação. Uma visão clara dos problemas a serem resolvidos e do objetivo almejado com a IA é fundamental para que a tecnologia gere valor público efetivo e não se torne um investimento subutilizado.

B.3 Modelo de Maturidade para Implantação de IA nas Cidades

Cada cidade está em um estágio diferente de prontidão para adotar soluções de gestão de dados e IA. Enquanto algumas cidades já possuem infraestrutura avançada e equipes dedicadas à análise de dados, muitos municípios, especialmente os menores, estão apenas começando a digitalizar seus processos básicos[8].

Para orientar a evolução tecnológica das cidades, é fundamental utilizar um Modelo de Maturidade[9]. Esse modelo consiste em uma estrutura de níveis ou estágios que permite verificar o quão preparada uma cidade está para se tornar mais inteligente e capaz de implantar IA de forma eficaz, bem como quais passos deve seguir para alcançar esse objetivo.

No contexto brasileiro, o Ministério da Ciência, Tecnologia e Inovações (MCTI) lançou recentemente a plataforma Inteligente[10], que oferece um diagnóstico de maturidade para Cidades Inteligentes

e Sustentáveis. Esse diagnóstico foi construído com base em um modelo internacional da União Internacional de Telecomunicações (UIT/ITU) adaptado à realidade dos municípios brasileiros. Nele, a maturidade da cidade é avaliada em quatro dimensões principais – econômica, ambiental, sociocultural e capacidades institucionais – e cada dimensão possui indicadores que posicionam o município em um determinado nível de desenvolvimento tecnológico/digital.

São definidos sete níveis de maturidade (Figura B.3.1) no modelo da UIT, que vão desde estágios iniciais (onde a cidade tem infraestrutura muito básica e quase nenhum serviço digitalizado) até estágios avançados (cidade altamente integrada digitalmente, com uso extensivo de tecnologias de análise de dados e IA em serviços e processos). Ferramentas como essa permitem às prefeituras identificar em que patamar estão e traçar um plano de evolução, alinhado a padrões internacionais, para avançar na escala de cidades inteligentes.

Figura B.3.1 – Os sete níveis de maturidade do modelo UIT

Adesão	A cidade reconhece desafios, mas ainda não possui um plano de transformação digital. Há baixa digitalização, infraestrutura desigual e falta de integração entre setores.
Engajamento	Início da articulação para modernização, com identificação de áreas prioritárias, investimentos em infraestrutura básica e digitalização inicial dos serviços públicos.
Planejamento	Definição de estratégias e políticas de dados, com acompanhamento por indicadores. Há interoperabilidade entre setores e identificação de áreas prioritárias para gestão e monitoramento.
Alinhamento	Implementação de Tecnologias de Informação e Comunicação (TICs) para melhorar serviços e soluções. A cidade inicia ações de inclusão digital, monitoramento contínuo e pesquisas de satisfação.
Desenvolvimento	Expansão da tecnologia para aprimorar a gestão pública. Os serviços atendem a maior parte da população de forma integrada, com participação ativa da sociedade.
Integração	Consolidação da estratégia digital, integração territorial com outros municípios e uso de TICs avançadas para suporte a serviços em tempo real. Governança pública com forte participação social.
Otimização	Cidade inteligente consolidada, sustentável e inclusiva. Infraestrutura totalmente digitalizada, automatização avançada e uso de grandes volumes de dados para previsão e aprimoramento contínuo dos serviços públicos.

Para avaliar a prontidão e planejar a implantação de análise de dados e IA, alguns critérios de maturidade são particularmente importantes, como a disponibilidade de dados, infraestrutura e capacitação de equipes, como destacado a seguir.

Disponibilidade e Qualidade de Dados

É possivelmente o critério mais importante[11]. Uma cidade madura para efetuar análises avançadas de dados e uso de IA precisa ter dados abundantes, acessíveis e confiáveis sobre seus diversos setores. Isso envolve desde manter bases cadastrais atualizadas (de cidadãos, imóveis, empresas) até coletar dados operacionais contínuos (sensores de trânsito, registros de atendimento, indicadores de saúde e outros).

Além da existência dos dados, é necessário que eles possuam boa qualidade e sejam integrados entre os setores interessados. Cidades mais avançadas no caminho de se tornarem inteligentes já implementam *data warehouses* ou *data lakes* centralizados, onde diferentes bancos de dados municipais se conectam, possibilitando correlações e análises intersetoriais.

Em uma avaliação de maturidade as perguntas efetuadas sobre dados visarão identificar: q*ue dados a cidade tem? Em que formato? Com que frequência são coletados e atualizados? Eles estão prontos para alimentar algoritmos de IA.* Quanto mais respostas positivas para perguntas como essas, maior o nível de maturidade da cidade.

Infraestrutura tecnológica[12]

Refere-se aos meios físicos e digitais disponíveis para suportar soluções de IA. Isso inclui conectividade (redes de internet rápidas, Wi-Fi público, cobertura móvel 4G/5G), equipamentos (servidores, computadores, câmeras, sensores IoT nas ruas) e plataformas de software adequadas (sistemas em nuvem, ferramentas de big data e outros).

Uma cidade com baixa maturidade talvez não tenha computadores suficientes ou internet estável nas repartições públicas, enquanto uma cidade com alta maturidade investe em centros de dados robustos e pode ter infraestrutura mais robusta, como redes 5G e computação em nuvem híbrida. A diferença entre esses casos é muito significativa: municípios com tecnologia deficiente terão dificuldade em rodar algoritmos complexos ou coletar dados em tempo real, ao passo que cidades bem equipadas conseguem implementar projetos mais avançados em tecnologias digitais, como semáforos inteligentes, vigilância com IA, aplicativos móveis integrados, dentre outros.

Ao avaliar maturidade, verifica-se o nível de informatização da gestão, a presença de sensores e automação na cidade (por exemplo, iluminação pública telecontrolada, semáforos conectados) e a capacidade de armazenar e processar dados em larga escala (localmente ou via cloud). A existência de uma boa infraestrutura denota que a cidade pode não só implantar como também escalar soluções de IA.

Capacitação de equipes

Um critério fundamental para a transformação das cidades em inteligentes é avaliar o capital humano e a cultura institucional da prefeitura para lidar com dados e IA. Cidades mais avançadas possuem em seu quadro (ou ao alcance por meio de parceiros) especialista como cientistas de dados, analistas de TI, engenheiros de software e gestores de inovação. Por outro lado, cidades iniciantes no assunto, geralmente não dispõe de uma equipe de TI própria estruturada.

É importante destacar que evoluir em maturidade é um processo contínuo. Uma boa prática é começar com projetos piloto de análise de dados e IA em áreas estratégicas e, aprender com eles, e expandir o conhecimento adquirido a outros setores. Paralelamente, investir em melhorar a infraestrutura de dados e capacitar pessoas garante que, ao longo do tempo, a prefeitura suba os degraus da maturidade.

O modelo de maturidade serve como um mapa para a cidade se orientar na jornada da transformação digital. Ele mostra onde a cidade está, onde pode chegar, e quais lacunas precisa preencher – seja melhorar sua base de dados, modernizar equipamentos ou treinar sua equipe – para implantar a Inteligência Artificial de forma bem-sucedida e colher todos os benefícios das tecnologias emergentes.

B.4 Salas de Situação e Compartilhamento de Dados

Salas de Situação

Uma sala de situação é um espaço físico (ou virtual) onde informações de múltiplas fontes são reunidas e analisadas em conjunto por uma equipe multidisciplinar, para o monitoramento e a coordenação das ações da cidade. Representa a materialização prática do conceito de gestão orientada por dados (*data-driven*). Ela cria um ambiente onde a IA, os sistemas de monitoramento e as equipes humanas trabalham em sintonia, resultando em uma administração municipal mais conectada, informada e preparada para otimizar serviços no dia a dia quanto para enfrentar crises quando necessário.

Uma sala de situação moderna assemelha-se a um centro de controle, onde telões exibem mapas da cidade, imagens de câmeras espalhadas pelo município e gráficos de indicadores atualizados a cada minuto. Em torno dessas telas, ficam posicionados profissionais de várias secretarias e analistas de dados, todos acompanhando as informações e trabalhando de forma coordenada.

Um ponto fundamental de salas de situação é a integração de dados entre diferentes níveis de governo e setores. Muitos problemas urbanos atravessam as fronteiras departamentais – ou até mesmo as fronteiras municipais – e requerem cooperação. Por isso, essas salas costumam ser alimentadas não só por dados da própria prefeitura, mas também por informações de órgãos estaduais e federais e de entidades privadas parceiras. Isso significa que, ao detectar pela câmara um veículo roubado, por exemplo, o alerta chega simultaneamente à guarda municipal na sala e polícia militar, que pode interceptar o carro. Ou, no caso de um incêndio em um prédio, os Bombeiros são acionados imediatamente e podem coordenar a resposta junto com a Defesa Civil municipal.

Em resumo, a sala de situação traz consciência situacional para a administração municipal: uma visão unificada e em tempo real de tudo o que importa na cidade, facilitando decisões baseadas em dados e a atuação conjunta das áreas envolvidas.

Compartilhamento de Dados (Portais de Dados Abertos)

Enquanto na sala de situação o foco é o uso interno das informações pelos gestores públicos para operação e planejamento em tempo real os portais de dados abertos são aqueles que disponibilizam publicamente dados governamentais em formato acessíveis e licenciados para reutilização, permitindo que qualquer pessoa (cidadãos, pesquisadores, empresas) os análise e crie aplicações a partir deles. No Brasil, a Lei de Acesso à Informação e a Política de Dados Abertos incentiva os órgãos públicos a publicar suas bases de dados não sigilosos.

Uma boa integração de dados (interna e entre entes federativos) que alimenta a sala de situação também facilita a publicação de dados abertos padronizados, e vice-versa. Em ambos os casos, a interoperabilidade e a atualização contínua dos dados são vitais.

É fundamental que os dados abertos sejam anonimizados e tratados para não expor informações pessoais sensíveis. A prefeitura deve remover identificadores pessoais (como nome, CPF, endereço específico) e agregar dados quando necessário, para cumprir a LGPD e garantir a privacidade. Feito isso, a maioria das bases – especialmente dados estatísticos ou geográficos – pode ser liberada sem receios. Outro ponto é fornecer os dados em formatos padronizados e fáceis de consumir (CSV, JSON, APIs abertas), para atrair a comunidade de desenvolvedores.

Referências Bibliográficas

1. LEE, K.; BARBAO, M. **Inteligência Artificial.** Rio de Janeiro: Globo Livros, 2019. 292 p. Disponível em: https://books.google.com.br/books?id=cNYfywEACAAJ. Acesso em: 02 maio 2025.

2. RUSSELL, S. J.; NORVIG, P. **Artificial intelligence**: a modern approach. Hoboken, NJ: Pearson Education, 2016.

3. MARTIAN, N. **Smart cities and urban innovation:** a simplified guide for everyone. [*S. l.: s. n.*], 2025. 232 p.

1. ADJE, K. D.; LETAIFA, A. B.; HADDAD, M.; HABACHI, O. Smart city based on open data: a survey. **IEEE Access**, v. 11, p. 56726–56748, 2023. Doi:10.1109/access.2023.3283436

2. COZMAN, F. G.; PLONKI, G. A.; NERI, H.G. A. **Inteligência artificial**: avanços e tendências. São Paulo: Universidade de São Paulo, Instituto de Estudos Avançados, 2021. 414 p. Doi:10.11606/9786587773131

3. INÁCIO, A. D.; LEAL, A. G.; GAVA, V. L.; SANTOS, A. S. Salas de Situação: Implantação de monitoramento inteligente como suporte às Políticas Públicas. *In:* WORKSHOP DE COMPUTAÇÃO APLICADA EM GOVERNO ELETRÔNICO, 2021, Florianópolis. **Anais [...].** Porto Alegre: Sociedade Brasileira de Computação, 2021. p. 283–290. Doi:10.5753/wcge.2021.15997

4. BHATIA, V.; JAGLAN, V. Integrating Artificial Intelligence and IoT for Smart Cities. In: DALAL, S. et al. Reshaping Intelligent Business and Industry: Convergence of AI and IoT at the Cutting Edge. Hoboken, NJ: Wiley, 2024. Cap. 17**.**

5. ALJOWDER, T.; ALI, M.; KURNIA, S. Systematic literature review of the smart city maturity model. *In:* INTERNATIONAL CONFERENCE ON INNOVATION AND INTELLIGENCE FOR INFORMATICS, COMPUTING, AND TECHNOLOGIES (3ICT), 2019, Bahrain. **Proceedings [...].** Piscataway: IEEE, 2019. p. 1–9. Doi:10.1109/3ict.2019.8910321

6. KLAR, R.; ARVIDSSON, N.; ANGELAKIS, V. Digital Twins' Maturity: The Need for Interoperability. **IEEE Systems Journal,** v. 18, n. 1, p. 713–724, 2024. Doi:10.1109/jsyst.2023.3340422

7. PASETO, L.; GONTIJO, J. G.; DE AZAMBUJA, E. E.; VIDAL, K. D.; ALVES, A. M.; MUNIZ, C. R.; CORSO, M. R. inteli.gente Platform: Tool for Diagnosing Maturity in Brazilian Sustainable Smart Cities. *In:* INTERNATIONAL SMART CITIES CONFERENCE (ISC2), 2021. **Proceedings [...].** Piscataway: IEEE, 2021. p. 1-6. Doi:10.1109/isc253183.2021.9562934

8. GUPTA, S.; KUMAR, A.; MAITI, J. A critical review on system architecture, techniques, trends and challenges in intelligent predictive maintenance. **Safety Science**, v. 177, art. 106590, Sept. 2024. Doi:10.1016/j.ssci.2024.106590

9. SILVA, L. C.; RIEDO, I. G.; MENDONÇA, J. C.; NOBRE, L. B.; MAIOLI, S. F. Understanding smart cities: a systematic review. **Revista de Administração da UFSM**, v. 17, n. 1, e7, 2024. Doi:10.5902/1983465973468

ANEXO C

Indicadores para Cidades Inteligentes, Resilientes e Sustentáveis

C.1 Relação entre Cidades Inteligentes, Resilientes e Sustentáveis

As palavras inteligente, resiliente e sustentável, quando presentes após o nome *cidade*, são adjetivos de caráter geral e que envolvem ações de certa forma interligadas entre si. Assim, a inter-relação entre **cidades inteligentes**, **resilientes** e **sustentáveis** está no fato de que esses três conceitos, embora distintos, se complementam e se fortalecem mutuamente quando aplicados em conjunto no planejamento e desenvolvimento urbano.

De modo resumido pode-se dizer que: cidades inteligentes usam a tecnologia de dados para melhorar a eficiência dos serviços urbanos, a qualidade de vida dos cidadãos e a gestão dos recursos; cidades resilientes são capazes de resistir, se adaptar e se recuperar de crises e desastres naturais ou humanos; cidades sustentáveis têm como objetivo o equilíbrio entre o desenvolvimento urbano e a preservação ambiental, promovendo justiça social e bem-estar das futuras gerações.

Uma cidade inteligente usa a tecnologia para ser mais eficiente, mas ela precisa ser sustentável para durar e resiliente para enfrentar desafios. Esses três pilares são essenciais para construir um futuro urbano equilibrado, onde a tecnologia serve às pessoas, respeita o planeta e garante segurança diante das incertezas (Figura C.1.1).

Figura C.1.1 – Pilares para um futuro urbano equilibrado

C.2 Indicadores para Cidades Inteligentes, Resilientes e Sustentáveis

As cidades apresentam inúmeras diferenças entre si. Essas variações podem ser observadas em diversos aspectos, como infraestrutura, cultura, economia, clima, tamanho populacional, acesso a serviços públicos e qualidade de vida, entre outros.

Apesar das diferenças, as cidades possuem um objetivo comum, que pode ser resumido em promover o bem-estar da população por meio do desenvolvimento sustentável, da inclusão social, do crescimento econômico e da valorização cultural. Para tal ela se apoia em um Planejamento Urbano elaborado de acordo com o perfil da cidade. Porém, é essencial que ela verifique se a implantação desse planejamento está tendo os resultados e evoluções desejáveis. Isto pode ser feito por meio de indicadores de desempenho, que podem ser medidas quantitativas, qualitativas ou descritivas.

Definir um conjunto de indicadores para uma cidade não consiste de tarefa fácil. Cidades são complexas, com seus elementos sociais, políticos, econômicos e culturais interagindo e reagindo com a espacialidade e o ambiente construído da cidade. Qualquer conjunto de indicadores, não será capaz de refletir plenamente a complexidade urbana e as muitas escalas em que os impactos urbanos são sentidos[1]. Apesar dessa restrição, os indicadores são necessários e atendem a múltiplos propósitos. Por exemplo, podem se tornar parte da avaliação e comparação de condições e tendências no espaço e no tempo, monitorando o progresso em direção a metas e objetivos, informando o planejamento e a tomada de decisões, aumentando a conscientização, encorajando mudanças políticas e comportamentais, promovendo a participação pública e melhorando a comunicação[1].

A Figura C.2.1 traz exemplos de indicadores, com o objetivo apenas de dar uma visão geral de cada caso específico de cidade. Seria fácil se os indicadores se restringissem a esses exemplos, mas gestores municipais enfrentam o desafio de selecionar indicadores para monitoramento sistemático de suas cidades. Essa escolha é muito importante, pois afeta diretamente a gestão e a tomada de decisões da cidade, sendo que os gestores devem estar atentos para não se perderem na quantidade de dados urbanos complexos[2].

Figura C.2.1 – Exemplos de indicadores

Exemplos de indicadores para cidades sustentáveis

- Emissões de CO2 (tonelada habitante/ano)
- Qualidade do ar
- Áreas verdes (metro quadrado/habitante)
- Reciclagem de resíduos sólidos urbanos (porcentagem do total gerado)
- Consumo de energia renovável (porcentagem da matriz energética)
- Transporte sustentável (porcentagem da população)

Exemplos de indicadores para cidades inteligentes

- Acesso à internet de alta velocidade (porcentagem da população)
- Serviços públicos digitalizados (porcentagem dos serviços)
- Aplicativos de mobilidade urbana (quantidade)
- Sistema inteligente de transporte (existe ou não)
- Plataformas online (número de interações/ano)

Exemplos de indicadores para cidades resilientes

- Plano de gestão de riscos e desastres atualizados (existe ou não)
- Tempo médio de resposta a emergências (minutos)
- População em área de risco com monitoramento ativo (porcentagem da população)
- Infraestruturas adaptadas a eventos extremos (porcentagem adaptada)
- Simulados de treinamento de emergência (número por ano)

Existem centenas de indicadores disponíveis, cada qual com uma finalidade específica. Cabe à cidade definir quais são os melhores indicadores de desempenho para o seu caso e criar um banco de dados[3], que integrado são capazes de fornecer uma base para tomada de decisão pelos gestores municipais. A definição de que indicadores devem ser usados e quando, pode requerer conhecimento especializado, para compreender a utilidade e as fragilidades dos sistemas de indicadores que se pretende implantar em uma cidade[2].

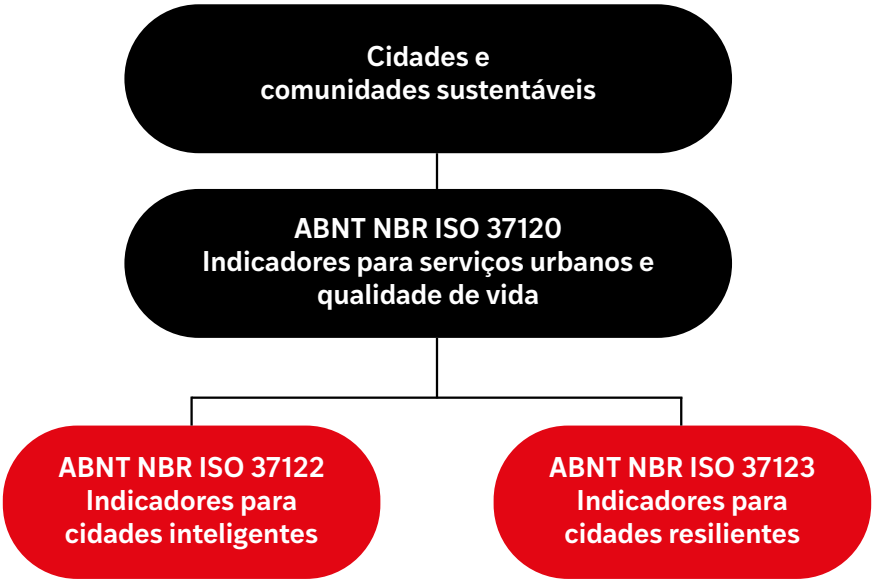
Organismos internacionais têm trabalhado na questão da padronização de indicadores para cidades sustentáveis, inteligentes e resilientes. Essa padronização é importante porque proporciona harmonização, confiabilidade, transparência nos métodos de cálculo e comparabilidade dos resultados.

A ISO (*International Organization for Standardization*) desenvolveu algumas normas, que trazem indicadores e como eles se relacionam entre si. Estas normas foram internalizadas no Brasil como normas ABNT NBR ISO.

C.3 Indicadores ISO

No conjunto de normas ABNT NBR ISO os indicadores de cidades inteligentes e resilientes estão atrelados a uma hierarquia de indicadores que se complementam (Figura C.3.1).

Figura C.3.1 – Relação entre família de normas para indicadores da cidade



ABNT NBR ISO 37120 - Indicadores para Serviços Urbanos e Qualidade de Vida.

A norma *ABNT NBR ISO 37120:2021 – Cidades e Comunidades Sustentáveis – Indicadores para serviços urbanos e qualidade de vida*[4], classifica os indicadores em três tipos:

- **Indicadores essenciais:** que são requeridos para demonstrar o desempenho da prestação de serviços urbanos e qualidade de vida;
- **Indicadores de apoio:** que são recomendados para demonstrar o desempenho da prestação de serviços urbanos e qualidade de vida. Estes indicadores podem ser selecionados de acordo com os objetivos da cidade;
- **Indicadores de perfil:** que são recomendados para fornecer estatísticas básicas e informações do contexto para auxiliar as cidades a realizar comparações entre pares. Indicadores de perfil são utilizados como uma referência informativa.

A norma *ABNT NBR ISO 37120:2021* trata de vários temas, sendo que cada tema corresponde a uma seção (Quadro C.3.1).

Quadro C.3.1 – Temas tratados pela ANBT NBR 37120 e suas seções[4]

Tema	Número da seção onde tema é tratado
Economia	5
Educação	6
Energia	7
Meio ambiente e mudanças climáticas	8
Finanças	9
Governança	10
Saúde	11
Habitação	12
População e condições sociais	13
Recreação	14
Segurança	15
Resíduos sólidos	16
Esporte e cultura	17
Telecomunicações	18
Transporte	19
Agricultura urbana/local e segurança alimentar	20
Planejamento urbano	21
Esgotos	22
Água	23

A norma *ABNT NBR ISO 37120:2021* traz para cada tema os indicadores essenciais, os indicadores de apoio e os indicadores de perfil e, também, aponta como devem ser obtidos. A título de ilustração, o Quadro C.3.2 apresenta esses indicadores para o tema Economia.

Quadro C.3.2 – Indicadores essenciais de apoio e de perfil para o tema economia[4]

Tema	Indicador essencial	Indicadores de apoio	Indicador de perfil
Economia	Taxa de desemprego da cidade	Valor de avaliação de propriedades comerciais e industriais como porcentagem do valor de avaliação total de todas as propriedades Porcentagem da população com emprego em tempo integral Taxa de desemprego de jovens Número de empresas por cem mil habitantes Número anual de estadias (pernoites) de visitantes por cem mil habitantes Conectividade aérea (número de partidas de voos comerciais sem escala)	Renda familiar média (US$) Taxa anual de inflação baseada na média dos últimos cinco anos Produto da cidade per capita (US$)

ABNT NBR ISO 37122 - Indicadores para Cidades Inteligentes

A norma *ABNT NBR ISO 37122:2020 – Cidades e Comunidades Sustentáveis – Indicadores para cidades inteligente*[5] complementa a norma ABNT NBR ISO 37120, pois houve a necessidade de indicadores adicionais para cidades inteligentes. Ainda, estabelece indicadores com definições e metodologias para medir, considerando aspectos e práticos.

Essa norma trata de vários temas, sendo que cada tema corresponde a uma seção da norma, conforme apresentado no Quadro C.3.3.

Quadro C.3.3 – Temas tratados pela ANBT NBR 37122 e suas seções[5]

Tema	Número da seção onde tema é tratado
Economia	5
Educação	6
Energia	7
Meio ambiente e mudanças climáticas	8
Finanças	9
Governança	10
Saúde	11
Habitação	12
População e condições sociais	13
Recreação	14
Segurança	15
Resíduos sólidos	16
Esporte e cultura	17
Telecomunicações	18
Transporte	19
Agricultura local/urbana e segurança alimentar	20
Planejamento urbano	21
Esgotos	22
Água	23
Relatório e manutenção de registros	24

A norma *ABNT NBR ISO 37122:2020* também traz os indicadores de cada tema e aponta como devem ser obtidos. A título de ilustração o Quadro C.3.4 apresenta um dos indicadores para o tema Segurança, item 15 da norma em questão.

Quadro C.3.4 – Indicadores para o tema Segurança na norma ABNT NBR ISO 37122:2020

Tema	Indicadores (subitem da seção)
Segurança (item 15)	Porcentagem de áreas da cidade coberta por câmera digital (15.1)

A norma *ABNT NBR ISO 37122:2020* traz, em seu Anexo B, um mapeamento dos seus indicadores para os Objetivos de Desenvolvimento Sustentável das Nações Unidas (ODS). Para cada um dos 17 ODS são apresentados os indicadores correspondentes, varrendo todos os temas da norma.

ABNT NBR ISO 37123 - Indicadores para Cidades Resilientes

A norma *ABNT NBR ISO 3713:2021 – Cidades e Comunidades Sustentáveis – Indicadores para cidades resilientes*[6] complementa a norma ABNT NBR IS 37120, pois embora esta, como primeira norma da série, contenha indicadores importantes para o planejamento resiliente e avaliação de uma cidade, foi identificada a necessidade de mais indicadores para cidades resilientes, que constam na norma ABNT NBR ISO 37123 e ajudam as cidades a: se prepararem, se recuperarem e se adaptarem para quando ocorrerem choques e tensões; e aprenderem umas com as outras pela comparação entre uma vasta gama de medidas de desempenho e compartilhamento de boas práticas.

A norma *ABNT NBR ISO 3713:2021* trata de temas divididos em seções, conforme apresentado no Quadro C.3.5.

Quadro C.3.5– Temas tratados pela ANBT NBR 37123 e suas seções[6]

Tema	Número da seção onde tema é tratado
Economia	5
Educação	6
Energia	7
Meio ambiente e mudanças climáticas	8
Finanças	9
Governança	10
Saúde	11
Habitação	12
População e condições sociais	13
Recreação	14
Segurança	15
Resíduos sólidos	16
Esporte e cultura	17
Telecomunicações	18
Transporte	19
Agricultura urbana/local e segurança alimentar	20
Planejamento urbano	21
Esgotos	22
Água	23
Relatório e manutenção de registros	24

A norma ABNT NBR ISO 37123:2021 traz os indicadores referentes a cada tema, com definições e metodologias para medir. Também traz informações de utilidade em seus anexos, a seguir indicados:

- Anexo A, apresenta uma tipologia de ameaças enfrentadas por cidades, como caráter informativo;
- Anexo B, apresenta como os indicadores constantes na norma se relacionam com as principais etapas do processo de gerenciamento de risco (contexto do risco, avaliação de riscos, tratamento do risco, cooperação e consulta, monitoramento e revisão);
- Anexo C, apresenta como os indicadores constantes na norma estão relacionados aos principais elementos do processo de gerenciamento de desastres (minimização, preparação, resposta, recuperação/reconstrução);
- Anexo D, apresenta um mapeamento dos indicadores da norma para os 17 Objetivos de Desenvolvimento Sustentável das Nações Unidas (ODS).

C.4 Considerações

Os indicadores de desempenho são inúmeros e a escolha de quais usar é um grande desafio para os gestores municipais, que têm à sua frente um leque diversificado, advindo de referências normativas, de artigos técnicos e de práticas empregadas.

Os gestores municipais não devem se impressionar com a quantidade de indicadores. Ter muitos indicadores implantados não necessariamente significa ter dados de utilidade. Melhor procurar aqueles que trarão repostas confiáveis e consistentes, que possam ser utilizadas ao longo do tempo para, de fato, acompanhar a evolução da cidade.

Referências Bibliográficas

1. KLOPPA, J. M; PETRETTAB, D. The urban sustainable development goal: Indicators, complexity and the politics of measuring cities. **Cities,** v. 63, p. 92–97, Mar. 2017.

2. HUOVILA, A.; BOSCH, P.; AIRAKSINEN, M. Comparative analysis of standardized indicators for smart sustainable cities: What indicators and standards to use and when? **Cities,** v. 89, p. 141-153, June 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S0264275118309120. Acesso em: 19 abr. 2025.

3. KHATIBI, H.; WILKINSON, S.; DIANAT, H.; BAGHERSAD, M.; GHAEDI, K.; JAVANMARDI, A. Indicators bank for smart and resilient cities: design of excellence. **Built Environment Project and Asset Management,** v. 12, n. 1, p. 5-19, 2022. Doi: https://doi.org/10.1108/BEPAM-07-2020-0122

4. ABNT. **NBR ISO 37120:2021:** Cidades e comunidades sustentáveis. Indicadores para serviços urbanos e qualidade de vida. Rio de Janeiro: ABNT, 2020. Disponível em: https://www.abntcatalogo.com.br/grd.aspx. Acesso em: 25.04.2025.

5. ABNT. **NBR ISO 37122:2020. Versão corrigida 2021**. Cidades e comunidades sustentáveis. Indicadores para cidades inteligentes. Rio de Janeiro: ABNT, 2020. Disponível em: https://www abntcatalogo.com.br/grd.aspx. Acesso em: 25.04.2025.

6. ABNT. **NBR ISO 37123:2021:** Cidades e comunidades sustentáveis. Indicadores para cidades resilientes. Rio de Janeiro: ABNT, 2021. Disponível em: https://www.abntcatalogo.com.br/grd.aspx. Acesso em: 25.04.2025.

Secretaria de
Desenvolvimento Econômico

SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS