

ARTIGO

Governança da comunicação de emergência em cidades inteligentes: uma arquitetura teórica para municípios resilientes

Emergency communication governance in smart cities: a theoretical architecture for resilient municipalities

Gobernanza de la comunicación de emergencia en ciudades inteligentes: una arquitectura teórica para municipios resilientes

Moisés Figueiredo da Silva¹

¹ Universidade Nove de Julho (UNINOVE), São Paulo, SP, Brasil. ORCID: <https://orcid.org/0000-0002-3012-3402>

SUBMETIDO	ACEITO	PUBLICADO	DOI
17/05/2024	11/10/2024	06/12/2024	em processamento

RESUMO

A comunicação de emergência depende de infraestrutura tecnológica, coordenação institucional, confiança pública, acessibilidade e capacidade de alcançar grupos sociais heterogêneos. Este artigo propõe uma arquitetura teórica para a governança da comunicação de emergência em cidades inteligentes. O estudo adota abordagem teórico-integrativa e articula governança multinível, teorias de comunicação de crise e risco, modelos comportamentais de resposta a alertas, sistemas de alerta precoce, telecomunicações resilientes, inclusão comunicacional, participação comunitária e aprendizagem institucional. A análise identifica seis dimensões interdependentes: autoridade institucional definida, interoperabilidade operacional e tecnológica, redundância entre canais digitais e analógicos, mensagens acessíveis e acionáveis, coprodução comunitária da resiliência e auditoria pós-evento. Argumenta-se que municípios tecnologicamente avançados podem permanecer vulneráveis quando dependem de um único canal, operam com responsabilidades fragmentadas ou não alcançam populações expostas. Discutem-se ainda vulnerabilidades sociotécnicas associadas ao tecnocentrismo, à dependência de fornecedores, ao viés algorítmico, à desinformação e à sustentabilidade

administrativa dos sistemas municipais. Conclui-se que a resiliência comunicacional constitui uma capacidade sociotécnica de manter informações confiáveis, compreensíveis e úteis antes, durante e depois das crises, e que essa capacidade deve ser tratada como política pública permanente, e não como resposta episódica a eventos extremos.

Palavras-chave: comunicação de emergência; cidades inteligentes; governança; defesa civil; resiliência urbana

ABSTRACT

Emergency communication depends on technological infrastructure, institutional coordination, public trust, accessibility, and the capacity to reach heterogeneous social groups. This article proposes a theoretical architecture for emergency communication governance in smart cities. The study adopts a theoretical-integrative approach combining multilevel governance, crisis and risk communication theory, behavioral models of warning response, early warning systems, resilient telecommunications, communication inclusion, community participation, and institutional learning. The analysis identifies six interdependent dimensions: clearly defined institutional authority, operational and technological interoperability, redundancy between digital and analog channels, accessible and actionable messages, community co-production of resilience, and post-event auditing. It argues that technologically advanced municipalities may remain vulnerable when they depend on a single channel, operate with fragmented responsibilities, or fail to reach exposed populations. The article also discusses sociotechnical vulnerabilities associated with technocentrism, vendor dependency, algorithmic bias, misinformation, and the administrative sustainability of municipal systems. Communication resilience is therefore understood as a sociotechnical capacity to maintain reliable, understandable, and useful information before, during, and after crises, one that should be treated as a permanent public policy rather than an episodic response to extreme events.

Keywords: emergency communication; smart cities; governance; civil defense; urban resilience

RESUMEN

La comunicación de emergencia depende de infraestructura tecnológica, coordinación institucional, confianza pública, accesibilidad y capacidad para alcanzar grupos sociales heterogéneos. Este artículo propone una arquitectura teórica para la gobernanza de la comunicación de emergencia en ciudades inteligentes. El estudio adopta un enfoque teórico-integrador y articula gobernanza multinivel, teorías de comunicación de crisis y riesgo,

modelos conductuales de respuesta a alertas, sistemas de alerta temprana, telecomunicaciones resilientes, inclusión comunicacional, participación comunitaria y aprendizaje institucional. El análisis identifica seis dimensiones interdependientes: autoridad institucional definida, interoperabilidad operativa y tecnológica, redundancia entre canales digitales y analógicos, mensajes accesibles y accionables, coproducción comunitaria de resiliencia y auditoría posterior a los eventos. Se sostiene que municipios tecnológicamente avanzados pueden seguir siendo vulnerables cuando dependen de un único canal, operan con responsabilidades fragmentadas o no alcanzan a las poblaciones expuestas. Se discuten además vulnerabilidades sociotécnicas asociadas al tecnocentrismo, a la dependencia de proveedores, al sesgo algorítmico, a la desinformación y a la sostenibilidad administrativa de los sistemas municipales. Se concluye que la resiliencia comunicacional es una capacidad sociotécnica para mantener información confiable, comprensible y útil antes, durante y después de las crisis, y que esa capacidad debe tratarse como política pública permanente, y no como respuesta episódica a eventos extremos.

Palabras clave: comunicación de emergencia; ciudades inteligentes; gobernanza; protección civil; resiliencia urbana

INTRODUÇÃO

A intensificação de eventos climáticos extremos, desastres socioambientais, crises sanitárias e falhas em infraestruturas críticas tem submetido os governos locais a situações nas quais o tempo disponível para decidir é reduzido e a incerteza permanece elevada. Em áreas urbanas densamente ocupadas, uma mensagem emitida com atraso, redigida em linguagem ambígua ou distribuída com alcance restrito pode comprometer rotas de evacuação, ampliar a exposição de grupos vulneráveis e dificultar o trabalho das equipes de resposta. A comunicação de emergência, portanto, não constitui uma atividade acessória da defesa civil. Ela integra o próprio núcleo da capacidade estatal de proteger vidas, coordenar recursos e preservar a confiança pública em contextos de incerteza aguda.

O avanço das cidades inteligentes ampliou os instrumentos disponíveis para monitoramento e difusão de alertas. Sensores ambientais, sistemas georreferenciados, plataformas integradas, redes móveis e análise de grandes volumes de dados permitem identificar ameaças e distribuir informações com rapidez incomparável em relação às décadas anteriores. Entretanto, a existência de infraestrutura digital não elimina problemas de

governança. Sistemas podem permanecer desconectados entre si, órgãos podem disputar a autoridade sobre o conteúdo da mensagem e parcelas relevantes da população podem não receber ou não compreender o aviso. A tecnologia melhora a comunicação apenas quando está inserida em arranjos institucionais capazes de definir responsabilidades, validar informações e sustentar canais alternativos durante falhas.

O problema de pesquisa decorre desse descompasso entre sofisticação tecnológica e capacidade institucional. Municípios que investem em centros de controle e aplicativos podem continuar vulneráveis se não dispuserem de protocolos comuns entre defesa civil, saúde, mobilidade, segurança pública, comunicação social e concessionárias de serviços públicos. A fragmentação produz mensagens contraditórias, atrasos, duplicidade de esforços e perda de credibilidade institucional. Em situações de risco, a confiança funciona como recurso operacional: orientações oficiais tendem a ser menos eficazes quando a população não reconhece a autoridade emissora ou percebe inconsistência entre fontes públicas, um fenômeno já documentado na literatura sobre resposta comportamental a alertas (Lindell & Perry, 2012; Mileti & Sorensen, 1990).

A pesquisa se justifica por três razões. Primeiro, a literatura brasileira sobre cidades inteligentes ainda trata a comunicação de risco como apêndice técnico, quando deveria ser tratada como subsistema de governança dotado de lógica própria. Segundo, a literatura internacional de gestão de emergências oferece conceitos maduros sobre coordenação, alerta e comportamento de resposta, mas raramente é articulada com os debates sobre infraestrutura urbana inteligente, produzindo um hiato entre campos que deveriam dialogar. Terceiro, eventos recentes no Brasil e em outros países, entre eles enchentes urbanas, deslizamentos, ondas de calor e falhas em sistemas de telecomunicações durante desastres, evidenciaram que a ausência de arquitetura de governança compromete resultados mesmo quando a tecnologia disponível é adequada.

A questão orientadora deste artigo é a seguinte: como estruturar uma arquitetura de governança da comunicação de emergência que integre recursos tecnológicos, coordenação institucional, inclusão e participação comunitária em municípios inteligentes? O objetivo geral é propor um modelo teórico capaz de orientar diagnóstico, planejamento e avaliação de sistemas municipais de comunicação de risco e crise. Como objetivos específicos, o artigo busca: (a) sistematizar os principais aportes teóricos sobre governança multinível, comunicação de crise e sistemas de alerta precoce aplicáveis ao contexto municipal; (b) identificar dimensões

constitutivas de uma arquitetura de governança comunicacional; e (c) discutir vulnerabilidades sociotécnicas que comprometem a efetividade dessas arquiteturas mesmo em contextos de alta capacidade tecnológica.

A contribuição do artigo reside em tratar a resiliência comunicacional como capacidade sociotécnica, evitando tanto o reducionismo tecnológico, que supõe que mais dados e mais plataformas resolvem o problema, quanto a leitura estritamente administrativa, que reduz a comunicação de emergência a um fluxograma de competências. O argumento central sustenta que a comunicação resiliente resulta da articulação entre autoridade, interoperabilidade, redundância, qualidade das mensagens, capilaridade social e aprendizagem organizacional. Essas dimensões não funcionam de modo independente. Uma mensagem tecnicamente correta pode fracassar sem canal de alcance adequado; uma rede redundante pode difundir orientações inconsistentes quando não há comando definido; e a participação comunitária perde efetividade quando não está vinculada aos protocolos oficiais. A arquitetura proposta neste texto busca explicitar essas interdependências e oferecer, a pesquisadores e gestores públicos, um vocabulário comum para analisar e desenhar sistemas municipais de comunicação de emergência.

O artigo está organizado em sete seções, além desta introdução. A segunda seção apresenta o referencial teórico, articulando governança multinível, cidades inteligentes e resiliência urbana, teorias de comunicação de crise e risco, modelos comportamentais de resposta a alertas e sistemas de alerta precoce. A terceira seção descreve o percurso metodológico da revisão integrativa. A quarta seção detalha as seis dimensões da arquitetura proposta. A quinta seção discute vulnerabilidades sociotécnicas e limites do tecnocentrismo. A sexta seção trata de aplicação municipal e indicadores de maturidade. A sétima seção apresenta as considerações finais.

REFERENCIAL TEÓRICO

A construção do modelo articula cinco campos: governança multinível, cidades inteligentes e resiliência urbana, teorias de comunicação de crise e risco, modelos comportamentais de resposta a alertas, e sistemas de alerta precoce e telecomunicações de emergência. Essa aproximação é necessária porque crises urbanas atravessam fronteiras administrativas, técnicas e disciplinares. O risco é detectado por determinados sistemas, interpretado por equipes especializadas, transformado em decisão por autoridades e comunicado a pessoas que possuem diferentes recursos, conhecimentos e condições de mobilidade. O desempenho final depende da cadeia completa,

não apenas de um componente isolado, o que exige um referencial capaz de conectar administração pública, ciência política, estudos urbanos, gestão de desastres e comunicação organizacional.

Governança multinível e coordenação institucional em desastres

A gestão de emergências raramente pode ser conduzida por uma única organização. Governos federal, estaduais e municipais, serviços de saúde, forças de segurança, corpos de bombeiros, concessionárias de energia e telecomunicações, organizações comunitárias e meios de comunicação participam de etapas distintas do ciclo de gestão de risco. A governança multinível descreve arranjos em que competências e recursos são distribuídos entre níveis e atores interdependentes, com autoridade dispersa entre esferas jurisdicionais sobrepostas (Hooghe & Marks, 2003; Piattoni, 2009). Em desastres, essa interdependência torna-se particularmente visível, porque decisões locais frequentemente dependem de dados produzidos em nível estadual ou federal, de infraestrutura operada por empresas privadas e de apoio logístico externo ao município.

A coordenação horizontal é igualmente relevante e, em muitos casos, mais difícil de alcançar do que a coordenação vertical. Secretarias municipais costumam operar com sistemas, terminologias e rotinas próprias, desenvolvidas ao longo de décadas de funcionamento setorial. Sem protocolos compartilhados, a informação circula lentamente ou perde precisão ao atravessar fronteiras organizacionais. A governança colaborativa oferece elementos para compreender a construção de fóruns interinstitucionais, regras de participação, confiança e compromisso entre atores com histórico de desconfiança mútua ou de competição por recursos (Ansell & Gash, 2008). Na comunicação de emergência, esses elementos precisam ser definidos antes da crise, quando ainda existe tempo hábil para negociar responsabilidades, testar fluxos de informação e resolver incompatibilidades técnicas e políticas.

A literatura sobre liderança em crises reforça esse ponto ao descrever a gestão de crise como um processo de sensemaking coletivo sob pressão temporal, no qual líderes precisam simultaneamente compreender o evento, coordenar a resposta e comunicar significado a públicos internos e externos (Boin & 't Hart, 2003; Boin et al., 2005). Comfort (2007) descreve esse desafio como um problema de cognição, comunicação, coordenação e controle: sistemas de resposta a desastres falham não apenas por escassez de recursos, mas por incapacidade de processar e compartilhar informação relevante no ritmo exigido pelo evento. Weick (1988) já havia observado que

situações de crise se caracterizam por baixa capacidade de interrupção da ação para deliberação, o que exige estruturas organizacionais capazes de atuar e aprender simultaneamente, e não sequencialmente.

A clareza de comando não implica concentração absoluta de todas as decisões em uma única instância. Determinadas ameaças exigem conhecimento distribuído entre unidades territoriais e respostas descentralizadas, sobretudo em cidades extensas e heterogêneas. O ponto decisivo é definir quem valida o alerta, quem autoriza sua emissão, quais órgãos complementam a mensagem com informação especializada e como divergências entre interpretações técnicas são solucionadas. A ausência dessas regras favorece tanto o silêncio institucional, quando nenhum órgão se sente autorizado a agir, quanto a proliferação de mensagens concorrentes, quando vários órgãos agem sem coordenação. A arquitetura de governança aqui proposta deve, portanto, combinar autoridade técnica, legitimidade política e capacidade operacional, retomando a distinção clássica entre valor público, legitimidade e capacidade administrativa presente na literatura de administração pública (Bozeman, 2007).

Cidades inteligentes e resiliência urbana sociotécnica

O conceito de cidade inteligente foi inicialmente associado à digitalização de serviços, à conectividade ampliada e ao uso intensivo de dados urbanos. Estudos posteriores demonstraram que a infraestrutura tecnológica, por si só, não define a inteligência urbana; capacidades institucionais, participação cidadã e sustentabilidade ambiental também integram o conceito de forma constitutiva, e não apenas complementar (Caragliu et al., 2011; Albino et al., 2015). A crítica ao tecnocentrismo é especialmente relevante na gestão de emergências, pois sistemas sofisticados podem falhar justamente quando a infraestrutura é submetida a condições extremas, como picos de demanda em redes móveis durante evacuações em massa ou interrupção de energia em centros de dados.

Autores como Kitchin (2014) alertam que a promessa de cidades orientadas por dados frequentemente ignora as condições sociais e organizacionais necessárias para transformar dados em decisão útil. Morozov (2013) descreve como "solucionismo tecnológico" a tendência de tratar problemas complexos, de natureza social e institucional, como se fossem resolvidos por aplicativos ou plataformas isoladas. Essa crítica não nega o valor da tecnologia, mas indica que seu benefício depende de mediação institucional: um sensor que detecta um alagamento não produz, por si, uma decisão de evacuação, nem garante que a informação chegue a quem precisa dela.

A resiliência urbana corresponde à capacidade de um sistema urbano resistir, absorver, adaptar-se e recuperar-se de perturbações, preservando suas funções essenciais (Meerow et al., 2016). Essa definição envolve tanto sistemas físicos quanto sistemas sociais. Redes elétricas, telecomunicações e transporte são componentes tão importantes da resiliência quanto confiança institucional, conhecimento local, coordenação interorganizacional e solidariedade comunitária. Coaffee (2013) descreve a resiliência urbana como um objetivo de planejamento que combina infraestrutura física, governança e capacidade social de adaptação, argumentando que cidades resilientes não são apenas cidades bem equipadas, mas cidades capazes de aprender com perturbações recorrentes.

A comunicação conecta essas dimensões de modo particular: ela informa sobre a ameaça, orienta comportamentos individuais e coletivos, organiza recursos de resposta e permite que instituições atualizem sua compreensão do evento à medida que ele se desenvolve. A noção de resiliência comunicacional, tal como empregada neste artigo, designa a capacidade de manter fluxos informacionais confiáveis durante mudanças bruscas, interrupções de infraestrutura e condições de incerteza elevada. Não se trata apenas de continuidade técnica de um sistema. Uma rede pode permanecer tecnicamente ativa e, ainda assim, produzir mensagens incompreensíveis, contraditórias ou inadequadas ao contexto local. A resiliência comunicacional precisa, portanto, ser avaliada segundo critérios de disponibilidade, integridade, alcance, acessibilidade, coerência entre fontes e utilidade prática da informação para quem a recebe.

Teorias de comunicação de crise e risco

Um segundo pilar teórico, ausente na versão inicial deste trabalho e aqui incorporado por ser central ao problema investigado, é o campo da comunicação de crise e de risco, desenvolvido sobretudo nas últimas três décadas nos estudos de comunicação organizacional e saúde pública. O modelo de Comunicação de Risco e Emergência em Crise, conhecido pela sigla em inglês CERC, propõe que a comunicação eficaz em situações de crise segue estágios reconhecíveis, do pré-evento à resolução, cada um exigindo objetivos comunicacionais distintos, como reduzir incerteza inicial, orientar ações protetivas imediatas e, posteriormente, prestar contas e restaurar a confiança pública (Reynolds & Seeger, 2005). Esse modelo reforça um ponto já central na arquitetura proposta neste artigo: a comunicação de emergência não é um evento único, mas um processo contínuo que começa antes da crise, com a construção de credibilidade institucional, e continua depois dela, com a prestação de contas.

A Teoria Situacional de Comunicação de Crise, desenvolvida por Coombs (2007) no campo da gestão de reputação organizacional, oferece outra contribuição relevante ao propor que a estratégia de resposta comunicacional deve ser proporcional ao nível de responsabilidade atribuído pelo público à organização emissora e ao histórico de crises anteriores. Embora formulada originalmente para o contexto corporativo, essa teoria auxilia a compreender por que municípios com histórico de comunicação falha durante emergências anteriores enfrentam maior resistência pública mesmo quando emitem alertas tecnicamente corretos: a credibilidade acumulada, ou a falta dela, molda a recepção da mensagem antes mesmo de seu conteúdo ser avaliado.

Deetz (2001) chama atenção para a dimensão relacional da comunicação organizacional, argumentando que a comunicação entre instituições e públicos não deve ser compreendida apenas como transmissão de informação, mas como processo de construção de sentido compartilhado, no qual a forma de comunicar tanto quanto o conteúdo comunicado determina a legitimidade da instituição perante seus interlocutores. Essa perspectiva é relevante para a comunicação de emergência porque desloca a atenção da simples emissão de alertas para a qualidade da relação entre poder público e cidadãos construída ao longo do tempo.

Modelos comportamentais de resposta a alertas

Um terceiro pilar incorporado nesta versão ampliada diz respeito à pergunta sobre o que leva pessoas a agir, ou a não agir, diante de um alerta oficial. O Modelo de Decisão de Ação Protetiva, formulado por Lindell e Perry (2012) a partir de décadas de pesquisa empírica sobre comportamento em desastres, descreve o processo pelo qual indivíduos recebem, interpretam e decidem responder, ou não, a informações de risco. O modelo identifica variáveis como a percepção da ameaça, a confiança na fonte, as normas sociais do grupo de referência e os recursos disponíveis para agir, como transporte próprio ou rede de apoio, como determinantes centrais da resposta comportamental. A implicação prática é direta: emitir um alerta tecnicamente correto não garante ação adequada, porque a decisão de agir depende de fatores que extrapolam o conteúdo textual da mensagem.

Perry e Lindell (2003) sistematizam achados anteriores de pesquisa sociológica sobre desastres, indicando que a maior parte da população não reage a um primeiro alerta com ação imediata, mas busca confirmação por meio de múltiplas fontes antes de agir, um comportamento denominado busca de confirmação (milling). Esse achado tem consequência direta para o

desenho de sistemas municipais: se pessoas tendem a verificar um alerta antes de agir, a arquitetura de comunicação precisa disponibilizar múltiplos canais coerentes entre si, de modo que a confirmação seja rápida e não introduza contradição. Quarantelli (1988) e Drabek (1986), em suas revisões clássicas de pesquisa sociológica sobre desastres, já haviam demonstrado que mitos populares sobre pânico generalizado em emergências são, em geral, infundados; o comportamento predominante é de busca racional de informação e de ajuda mútua entre vizinhos, o que reforça a relevância da dimensão comunitária discutida adiante neste artigo.

A percepção de risco também não é uniforme entre grupos sociais. Wachinger et al. (2013), em revisão sobre o chamado paradoxo da percepção de risco, mostram que indivíduos que residem há mais tempo em áreas expostas a ameaças recorrentes podem desenvolver subestimação do risco, um efeito que a comunicação pública precisa considerar ao evitar mensagens padronizadas que ignorem a experiência acumulada da população local. Cutter et al. (2003) desenvolveram, por sua vez, um índice de vulnerabilidade social a riscos ambientais que permanece amplamente utilizado para identificar populações com menor capacidade de resposta a desastres, considerando variáveis como renda, idade, composição familiar e acesso a recursos, e que pode orientar o mapeamento territorial de prioridades comunicacionais discutido na seção 4 deste artigo.

Sistemas de alerta precoce e telecomunicações de emergência

Sistemas de alerta precoce articulam conhecimento do risco, monitoramento contínuo, disseminação de avisos e capacidade de resposta da população e das instituições (Basher, 2006). A detecção de uma ameaça não reduz danos quando o aviso não chega às pessoas expostas ou não produz ação adequada. Essa cadeia enfatiza que comunicação e preparação comunitária são partes constitutivas do sistema de alerta, e não etapas posteriores a ele. O município precisa conhecer áreas expostas, grupos com necessidades específicas, meios de comunicação efetivamente disponíveis à população local e barreiras que podem impedir a adoção das orientações emitidas.

Documentos internacionais de referência para redução de risco de desastres, como o Marco de Hyogo (UNISDR, 2005) e seu sucessor, o Marco de Sendai (UNDRR, 2015), destacam explicitamente sistemas de alerta precoce centrados nas pessoas como prioridade de ação para governos nacionais e locais, reconhecendo que a eficácia de um alerta depende tanto da qualidade científica da previsão quanto da capacidade das comunidades de compreendê-lo e agir sobre ele. A norma internacional ISO 22320:2018,

voltada à gestão de incidentes, reforça a necessidade de estruturas de comando, controle e coordenação claramente definidas como pré-condição para resposta eficaz, alinhando-se ao argumento sobre autoridade institucional desenvolvido na seção 4.1 deste artigo.

Redes móveis, difusão celular, mensagens geolocalizadas, rádio, televisão, sirenes e plataformas digitais podem formar, em conjunto, um ecossistema de alerta. A escolha dos canais deve considerar o tipo de ameaça, o tempo disponível até o impacto, as características do território e as condições de infraestrutura local. Alertas súbitos, como rompimentos de barragens ou deslizamentos repentinos, exigem meios de grande alcance e baixa dependência de ação prévia do usuário, como a difusão celular por radiodifusão de área (cell broadcast), que não exige cadastro nem aplicativo instalado. Eventos de evolução mais lenta, como cheias graduais ou ondas de calor prolongadas, permitem comunicação progressiva, atualização de cenários e preparação antecipada de abrigos.

A redundância não equivale à simples multiplicação de canais. Canais diversos precisam ser acionados por procedimentos coordenados e transmitir conteúdo consistente entre si. Também devem possuir dependências técnicas distintas. Dois aplicativos que utilizam a mesma infraestrutura de rede móvel não representam redundância efetiva diante de um colapso de telecomunicações. A combinação entre meios digitais, radiodifusão tradicional, sirenes, rádio operacional de uso institucional e redes comunitárias reduz a probabilidade de falha comum, um princípio de engenharia de confiabilidade aplicado ao domínio comunicacional. Estudos sobre crise informatics, campo que examina o uso de mídias digitais durante desastres, mostram que redes sociais funcionam como canal complementar valioso, tanto para disseminação oficial quanto para captação de relatos de campo, mas não substituem canais formais de alerta, sobretudo entre populações com menor letramento digital (Palen & Anderson, 2016; Sutton et al., 2008).

PERCURSO METODOLÓGICO

O estudo adota revisão teórica integrativa, modalidade adequada à construção de modelos conceituais que articulam campos de conhecimento distintos e que ainda não dispõem de síntese consolidada (Torraco, 2016). O procedimento não buscou produzir estimativa quantitativa de efeitos, tampouco testar hipóteses causais, mas identificar conceitos, relações e condições relevantes para a governança municipal da comunicação de emergência. Foram examinadas contribuições de administração pública,

ciência política, estudos urbanos, gestão de desastres, sistemas de informação e comunicação organizacional, buscando deliberadamente atravessar fronteiras disciplinares que, na literatura corrente, tendem a permanecer isoladas.

A análise ocorreu em quatro movimentos sucessivos. O primeiro consistiu no mapeamento de lacunas entre a literatura de cidades inteligentes, predominantemente centrada em infraestrutura e dados, e os estudos de defesa civil e gestão de desastres, predominantemente centrados em coordenação institucional e comportamento humano. O segundo organizou uma matriz conceitual cruzando dimensões institucionais, tecnológicas e sociais identificadas em ambos os campos. O terceiro traduziu essa matriz em componentes de uma arquitetura de governança, buscando formulações aplicáveis à realidade de municípios brasileiros de diferentes portes. O quarto examinou relações de dependência entre os componentes, riscos de falha e possibilidades de aplicação municipal, incluindo indicadores de maturidade discutidos na seção 6.

Foram priorizadas obras seminais e amplamente citadas em seus respectivos campos, complementadas por contribuições publicadas até 2024, coerentemente com o período editorial do volume. A síntese considera tanto literatura acadêmica consolidada, publicada em periódicos como *Journal of Contingencies and Crisis Management*, *Disaster Prevention and Management*, *Public Administration Review* e *Journal of Urban Technology*, quanto documentos institucionais internacionais relevantes para a redução de riscos de desastres, produzidos por organismos como a Organização das Nações Unidas e a International Organization for Standardization. Como se trata de proposta teórica, a validade do modelo depende de posterior confronto com estudos de caso, exercícios simulados e dados de eventos reais em municípios brasileiros. Essa limitação é assumida como parte da agenda de pesquisa apresentada nas considerações finais.

ARQUITETURA TEÓRICA DA GOVERNANÇA DA COMUNICAÇÃO DE EMERGÊNCIA

A arquitetura proposta parte de uma premissa simples, mas frequentemente negligenciada na prática municipal: a comunicação de emergência é um serviço público crítico e deve ser governada como sistema. Isso significa definir objetivos, autoridades, fluxos de informação, recursos, controles, indicadores de desempenho e mecanismos de aprendizagem contínua. A aquisição de equipamentos ou plataformas representa apenas uma parte, e frequentemente a parte menos determinante, desse sistema. O desempenho

depende de como esses recursos são integrados às rotinas administrativas e às relações interorganizacionais construídas ao longo do tempo.

As seis dimensões que compõem o modelo formam uma estrutura interdependente, e não um checklist de itens independentes. A autoridade estabelece legitimidade e capacidade decisória; a interoperabilidade integra dados e atores dispersos; a redundância mantém continuidade sob falha; a qualidade das mensagens transforma informação bruta em orientação útil; a participação amplia alcance e adequação territorial; e a aprendizagem corrige falhas e atualiza o sistema ao longo do tempo. O modelo pode ser utilizado tanto para diagnóstico de maturidade institucional quanto para desenho de políticas públicas e avaliação pós-evento, conforme detalhado na seção 6.

Autoridade institucional definida e clareza de papéis

A primeira dimensão corresponde à definição da autoridade responsável pela emissão do alerta e pela coordenação geral da comunicação de emergência. Em muitos municípios brasileiros, defesa civil, gabinete do prefeito, secretaria de comunicação e órgãos setoriais possuem competências parcialmente sobrepostas, resultado de estruturas administrativas construídas de forma incremental, sem revisão sistemática. A indefinição pode retardar avisos ou permitir que considerações políticas interfiram em decisões que deveriam seguir critérios técnicos. Protocolos formais precisam indicar níveis de alerta, critérios objetivos de acionamento, responsáveis nominais e seus substitutos em cada nível hierárquico.

A autoridade deve ser acompanhada de mecanismos claros de validação técnica. Dados preliminares frequentemente contêm incerteza significativa, e a busca por certeza absoluta antes de agir pode atrasar medidas preventivas de forma perigosa. O protocolo precisa estabelecer como comunicar incertezas ao público sem comprometer a credibilidade da mensagem, e como atualizar recomendações à medida que novas informações chegam. Também precisa definir quem fala oficialmente em nome do município, como especialistas técnicos participam da formulação da mensagem e de que modo informações produzidas por órgãos estaduais ou federais, como institutos de meteorologia ou agências de bacia hidrográfica, são incorporadas ao processo decisório local.

A continuidade de comando exige escalas de plantão, contatos alternativos e delegação formal de autoridade registrada em norma interna. Emergências frequentemente ocorrem fora do horário administrativo regular e podem afetar diretamente os próprios agentes responsáveis pela decisão, seja por

deslocamento, indisponibilidade de comunicação ou impacto pessoal do evento. Planos que dependem de uma única pessoa ou de uma autorização singular são estruturalmente frágeis. A governança deve prever substituição automática, registro formal das decisões tomadas e autonomia proporcional ao risco enfrentado, de modo que agentes de plantão não precisem aguardar autorização de superiores indisponíveis diante de ameaça iminente.

Interoperabilidade operacional e tecnológica

Interoperabilidade é a capacidade de sistemas e organizações trocarem informações preservando seu significado original. No plano técnico, envolve formatos de dados, interfaces de programação, identificadores comuns e protocolos de segurança. No plano organizacional, envolve terminologia compartilhada, critérios de classificação comuns entre órgãos e procedimentos claros de uso da informação recebida. A mera integração tecnológica, sem acordo prévio sobre conceitos e critérios, pode apenas acelerar a circulação de dados incompatíveis entre si, produzindo a ilusão de integração sem seus benefícios reais.

Centros de operação municipais precisam consolidar informações provenientes de meteorologia, mobilidade urbana, saúde pública, serviços de infraestrutura urbana e relatos de campo das equipes de resposta. A qualidade dessa consolidação depende de frequência de atualização, rastreabilidade da origem dos dados e procedimentos claros de validação antes da divulgação pública. Dados de sensores automatizados precisam ser combinados com o conhecimento territorial acumulado por equipes locais e por moradores das áreas de risco, evitando que decisões sejam tomadas exclusivamente a partir de painéis digitais desconectados da realidade observada em campo. A interoperabilidade não elimina a necessidade de julgamento humano qualificado; ela amplia a base disponível para esse julgamento.

Acordos formais com concessionárias de energia, água e telecomunicações são essenciais, pois essas empresas influenciam simultaneamente o nível de risco enfrentado pela população e a capacidade municipal de resposta. Esses acordos devem definir compartilhamento tempestivo de informações operacionais, níveis mínimos de serviço durante emergências, contatos institucionais de emergência disponíveis vinte e quatro horas e critérios claros de proteção de dados pessoais eventualmente compartilhados. A dependência de infraestrutura privada não pode resultar em opacidade para o poder público responsável por proteger a população, especialmente em

municípios onde a concessão de serviços essenciais é operada por empresas com sede fora do território local.

Redundância entre canais digitais e analógicos

A redundância estrutural pressupõe a existência de canais com tecnologias, alcances e vulnerabilidades distintas entre si, de modo que a falha de um não comprometa o funcionamento dos demais. Aplicativos e redes sociais são úteis para atualização detalhada e para engajamento contínuo com a população, mas dependem de conectividade estável e de comportamento ativo do usuário, como manter notificações habilitadas e revisar o conteúdo recebido. Difusão celular por radiodifusão de área e mensagens de texto possuem alcance potencialmente maior por não exigirem cadastro prévio, embora também dependam do funcionamento da rede móvel local. Rádio, televisão, sirenes, carros de som e redes de comunicação comunitária podem operar como alternativas relativamente independentes dessas infraestruturas digitais.

O planejamento municipal deve mapear áreas sem cobertura de rede, pontos de sombra em terrenos acidentados, comunidades relativamente isoladas e infraestruturas críticas cuja falha comprometeria múltiplos canais simultaneamente. Testes periódicos, e não apenas simulações teóricas em gabinete, permitem verificar o alcance real de cada canal e o tempo efetivo de acionamento em condições próximas às de uma emergência real. Equipamentos de reserva, como geradores para sirenes e estações de rádio, precisam de manutenção regular, fontes de energia alternativa e pessoal treinado para operá-los sob pressão. A redundância inexistente no cotidiano administrativo dificilmente será improvisada com sucesso durante a crise propriamente dita.

Também é necessário evitar o excesso descoordenado de mensagens, problema tão prejudicial quanto a ausência de comunicação. A emissão simultânea por diversos canais deve preservar identidade visual, fonte identificável e instrução central consistente, evitando que pequenas variações de redação entre canais sejam interpretadas pelo público como sinal de divergência institucional. Atualizações subsequentes precisam indicar claramente horário de emissão e o que exatamente mudou em relação à mensagem anterior. Essa coerência entre meios reduz a circulação de rumores e facilita a verificação da informação por parte de cidadãos e de instituições parceiras, como escolas e unidades de saúde.

Mensagens acessíveis, contextualizadas e acionáveis

Uma mensagem de emergência precisa responder a perguntas práticas e concretas: qual é o perigo específico, onde ele ocorre, quem está exposto, o que a pessoa deve fazer, quando agir e onde obter atualizações confiáveis. Linguagem excessivamente técnica transfere ao público a tarefa de interpretar o risco a partir de termos especializados, o que é particularmente problemático sob pressão de tempo. Mensagens vagas, por outro lado, não oferecem orientação de ação suficiente, mesmo quando tecnicamente corretas. A redação deve equilibrar precisão informativa, brevidade e clareza da orientação, seguindo princípios já sistematizados pela literatura sobre alertas públicos há mais de três décadas (Mileti & Sorensen, 1990).

A acionabilidade de uma mensagem depende fortemente do contexto territorial em que ela será recebida. Recomendações de evacuação precisam indicar rotas específicas, pontos de encontro reconhecíveis e abrigos com endereço e capacidade conhecidos, e não apenas a instrução genérica de "deixar a área de risco". Orientações de permanência no local devem explicar objetivamente como reduzir exposição durante o período de espera. Quando informações ainda são incertas, a mensagem pode e deve indicar cenários possíveis e critérios objetivos para atualização futura, em vez de aguardar certeza completa antes de comunicar qualquer coisa. Ocultar a incerteza existente compromete a confiança pública no momento em que previsões inevitavelmente mudam ao longo do evento.

Modelos de mensagem previamente aprovados por todas as instâncias competentes aceleram significativamente a emissão em situações de urgência, mas não substituem a necessidade de adaptação ao contexto específico de cada evento. Bancos de textos padronizados devem contemplar diferentes tipos de ameaça e diferentes públicos, incluindo versões em linguagem simples e versões acessíveis a pessoas com deficiência sensorial ou cognitiva. Testes com moradores de diferentes perfis, realizados fora do período de crise, permitem identificar ambiguidades de redação que frequentemente não são percebidas por especialistas técnicos habituados ao vocabulário próprio de sua área de atuação.

Participação comunitária e coprodução da resiliência

Comunidades não são apenas destinatárias passivas da comunicação oficial. Moradores conhecem rotas alternativas, pontos recorrentes de alagamento, pessoas com mobilidade reduzida em sua vizinhança e redes informais de apoio mútuo que frequentemente não constam em nenhum cadastro público. A coprodução incorpora esse conhecimento local ao planejamento e à

resposta institucional, conceito desenvolvido originalmente por Ostrom (1996) para descrever a produção conjunta de bens públicos por Estado e sociedade civil. Núcleos comunitários de proteção, associações de moradores, escolas e unidades básicas de saúde podem ampliar significativamente a capilaridade e a credibilidade da comunicação oficial, funcionando como pontos intermediários de confiança entre a administração municipal e a população.

A participação precisa ocorrer antes dos eventos, e não apenas como resposta emergencial improvisada durante a crise. Reuniões comunitárias, mapeamentos participativos de risco e exercícios simulados permitem discutir prioridades locais e testar previamente a compreensão de mensagens junto à própria população que as receberá. A escada de participação proposta por Arnstein (1969), embora formulada originalmente para o planejamento urbano, permanece útil para distinguir formas superficiais de consulta, que apenas informam a população sobre decisões já tomadas, de formas efetivas de parceria, nas quais moradores influenciam concretamente o desenho do sistema de alerta. Lideranças comunitárias podem apoiar a difusão de informações, mas não devem ser utilizadas como substitutos permanentes de infraestrutura pública adequada. A parceria precisa ser formalmente reconhecida, sustentada por treinamento contínuo e integrada aos canais oficiais de comunicação, e não tratada como recurso informal e descartável.

Informações produzidas pela própria população também exigem verificação cuidadosa antes de orientar decisões oficiais. Plataformas colaborativas de relato podem indicar ocorrências em tempo real com utilidade operacional considerável, como demonstrado por estudos sobre uso de mídias sociais em incêndios florestais e outros desastres (Sutton et al., 2008), porém rumores, informações desatualizadas e duplicidades de relato são possibilidades constantes que a governança precisa antecipar. É necessário criar mecanismos claros de triagem, confirmação cruzada e devolutiva à comunidade, evitando que o incentivo à participação resulte em sobrecarga informacional para as equipes responsáveis pela análise desses relatos.

Aprendizagem pós-evento e auditoria comunicacional

Cada emergência revela aspectos que planos formais elaborados em condições de rotina não conseguem antecipar. Auditorias sistemáticas realizadas após cada evento devem reconstruir decisões tomadas, tempos de resposta em cada etapa, canais efetivamente utilizados, alcance real da mensagem e nível de compreensão alcançado pela população. O objetivo

dessa auditoria não é apenas atribuir responsabilidade por eventuais falhas, mas produzir aprendizagem organizacional genuína, no sentido desenvolvido por Argyris e Schön (1978), que distinguem entre correções superficiais de procedimento e mudanças mais profundas nos pressupostos que orientam a ação institucional. Registros de mensagens emitidas, logs de sistemas, entrevistas com equipes envolvidas e dados de atendimento de emergência ajudam a identificar gargalos que passariam despercebidos em relatórios puramente administrativos.

A avaliação precisa incluir sistematicamente a perspectiva do público receptor, e não apenas a perspectiva institucional de quem emitiu a mensagem. Saber que uma mensagem foi tecnicamente enviada não demonstra que ela foi efetivamente recebida, muito menos que foi corretamente compreendida pelo destinatário. Pesquisas de opinião pós-evento, reuniões comunitárias de avaliação e análise sistemática de reclamações e dúvidas recebidas permitem avaliar a eficácia real da comunicação praticada. Grupos em situação de maior vulnerabilidade precisam ser ouvidos de modo específico e direcionado, pois médias gerais de satisfação ou compreensão podem facilmente ocultar exclusões significativas de subgrupos populacionais.

As recomendações produzidas por essas auditorias devem ser formalmente incorporadas a planos municipais, contratos com fornecedores, programas de treinamento continuado e peças orçamentárias, com responsáveis nomeados e prazos definidos para implementação. Relatórios de avaliação sem responsáveis claros e sem prazos estabelecidos tendem sistematicamente a não produzir mudança concreta na prática institucional. A aprendizagem institucional genuína ocorre quando a experiência acumulada efetivamente modifica rotinas, protocolos e critérios decisórios, e não apenas quando ela é cuidadosamente documentada em relatórios que permanecem arquivados.

VULNERABILIDADES SOCIOTÉCNICAS E LIMITES DO TECNOCENTRISMO

A principal vulnerabilidade identificada na análise é a crença, ainda difundida entre gestores públicos, de que sistemas digitais sofisticados substituem capacidades institucionais consolidadas. Centros de controle municipais podem exibir grande quantidade de dados em telas e painéis sem que essa abundância se traduza em decisão coerente e tempestiva. A abundância informacional pode inclusive dificultar a priorização de ações quando não existem critérios claros de triagem, um fenômeno que a

literatura sobre sobrecarga de informação já documentou em outros contextos organizacionais. A tecnologia, nesse sentido, amplia tanto capacidades quanto fragilidades já existentes na estrutura administrativa que a utiliza; ela raramente cria capacidade institucional do zero.

Outra vulnerabilidade relevante é a dependência excessiva de fornecedores privados de tecnologia. Plataformas proprietárias podem restringir o acesso do próprio município à documentação técnica completa, à integração com outros sistemas e à auditoria independente de seu funcionamento. Contratos de aquisição precisam prever cláusulas explícitas de continuidade do serviço, suporte técnico mínimo garantido, possibilidade de exportação integral de dados e obrigação de comunicação tempestiva de incidentes de segurança. O município deve conservar conhecimento técnico interno suficiente para operar alternativas em caso de descontinuidade contratual e para avaliar de forma independente os resultados apresentados pelo fornecedor, evitando a situação, observada em diversos contextos administrativos, na qual apenas a empresa contratada compreende plenamente o funcionamento do sistema adquirido pelo poder público.

A automação de processos decisórios também pode introduzir vieses sistemáticos difíceis de perceber sem auditoria específica. Modelos preditivos treinados com registros históricos incompletos tendem a representar melhor áreas já monitoradas e populações já visíveis aos sistemas oficiais existentes. Regiões informais, assentamentos precários ou territórios com menor presença estatal histórica podem aparecer, em painéis de risco automatizados, como áreas de baixo risco, quando na realidade existe apenas ausência de dados e não ausência de ameaça real. Eubanks (2018) documenta, em contexto distinto mas conceitualmente aplicável, como sistemas automatizados podem reproduzir e até amplificar desigualdades preexistentes quando implementados sem escrutínio adequado sobre seus dados de treinamento. A governança municipal deve, portanto, combinar deliberadamente informação automatizada com observação de campo qualificada e conhecimento comunitário acumulado, tratando esses dois tipos de saber como complementares e não como substitutos hierarquicamente ordenados.

A segurança cibernética integra necessariamente a resiliência comunicacional contemporânea. Sistemas de alerta podem ser alvo de ataques de indisponibilidade, tentativas de adulteração de conteúdo ou uso indevido para disseminação de informação falsa sob aparência oficial. Controle de acesso, mecanismos de autenticação robustos, registro auditável de ações e planos de contingência específicos para incidentes cibernéticos

são necessários em qualquer sistema municipal crítico. Ao mesmo tempo, medidas de segurança excessivamente rígidas não podem impedir o acionamento rápido de um alerta em situação de urgência real. O desenho técnico precisa equilibrar cuidadosamente proteção contra uso indevido e operacionalidade sob pressão de tempo, um equilíbrio que raramente é trivial de alcançar na prática.

A sustentabilidade financeira também impõe limites concretos aos sistemas municipais de comunicação de emergência. Equipamentos exigem manutenção periódica, licenciamento de software, conectividade contínua e capacitação regular de pessoal. Projetos financiados apenas na etapa de implantação inicial, sem previsão orçamentária para as etapas subsequentes de manutenção, tendem sistematicamente a deteriorar-se ao longo de poucos anos. O planejamento municipal deve considerar explicitamente o custo total de ciclo de vida de cada componente do sistema e priorizar soluções tecnicamente robustas e compatíveis com a capacidade administrativa e financeira efetivamente disponível no município, e não necessariamente as soluções mais sofisticadas encontradas no mercado.

Fragmentação institucional e conflitos de autoridade

A fragmentação institucional pode produzir falhas graves de comunicação mesmo quando cada órgão envolvido executa adequadamente sua própria função interna, isoladamente considerada. A defesa civil pode monitorar corretamente o risco meteorológico, a secretaria de comunicação pode controlar de forma competente os canais oficiais e a secretaria de mobilidade pode administrar bem as rotas de trânsito, mas a ausência de procedimento comum entre esses órgãos impede que capacidades individualmente sólidas se convertam em resposta integrada. Conflitos de autoridade aparecem tipicamente quando diferentes órgãos interpretam de maneira distinta o momento adequado para emitir um alerta ou o conteúdo específico que deve ser divulgado ao público. Em situações de rápida evolução do evento, a negociação improvisada entre órgãos consome tempo escasso e aumenta consideravelmente a possibilidade de mensagens contraditórias chegarem à população.

A solução para esse problema não consiste simplesmente em centralizar toda a comunicação em um único órgão, decisão que muitos municípios adotam intuitivamente após uma crise mal gerida. A centralização excessiva pode reduzir a velocidade de resposta e ignorar informações relevantes produzidas localmente por equipes territoriais. O desenho institucional precisa, em vez disso, distinguir claramente entre decisões estratégicas,

validação técnica do conteúdo e execução operacional da comunicação. A autoridade central deve assegurar coerência geral da mensagem, enquanto equipes territoriais e setoriais contribuem com dados atualizados e adaptações necessárias ao contexto local específico. Protocolos de escalonamento tornam-se especialmente importantes quando a ameaça atravessa limites municipais ou envolve serviços cuja gestão pertence a outro nível de governo, situação comum em bacias hidrográficas compartilhadas por múltiplos municípios.

A formalização de protocolos deve ser necessariamente acompanhada de relações de trabalho construídas antes da ocorrência de qualquer crise. Reuniões intersetoriais regulares, exercícios simulados conjuntos e avaliação compartilhada de resultados permitem que agentes de diferentes órgãos conheçam pessoalmente as competências e limitações uns dos outros. A confiança interpessoal construída entre equipes reduz significativamente o custo de coordenação durante a emergência propriamente dita e facilita a circulação de informações ainda preliminares, que de outra forma poderiam ser retidas por precaução. Sem esse vínculo prévio, órgãos tendem a reter dados por receio de responsabilização individual ou, no extremo oposto, a divulgar informações sem validação técnica suficiente por pressão de urgência percebida.

Desinformação, rumores e disputa pela atenção pública

Ambientes digitais contemporâneos permitem que relatos, imagens e interpretações pessoais circulem amplamente antes de qualquer confirmação oficial sobre um evento em curso. Essa velocidade de circulação pode apoiar a identificação inicial de ocorrências pela própria administração municipal, mas também favorece a propagação de rumores infundados, registros retirados de contexto original e orientações potencialmente perigosas apresentadas como se fossem oficiais. A comunicação pública precisa competir por atenção com fontes informais e com conteúdos emocionalmente mobilizadores, que frequentemente se espalham com maior velocidade do que comunicados institucionais mais sóbrios. Respostas institucionais lentas criam um vazio informacional que tende a ser rapidamente ocupado por versões não verificadas do que está acontecendo.

A gestão ativa de rumores deve integrar formalmente o plano municipal de comunicação, e não ser tratada como resposta reativa e improvisada. Equipes designadas precisam monitorar continuamente dúvidas recorrentes da população, identificar precocemente informações falsas com potencial concreto de dano e responder por canais reconhecidamente oficiais e já

estabelecidos. A correção de informações falsas deve ser direta, apresentar imediatamente a orientação válida correspondente e evitar amplificar desnecessariamente conteúdos irrelevantes ao simplesmente repeti-los para desmenti-los. A transparência explícita sobre o que já é conhecido com segurança, o que ainda permanece incerto e quando haverá nova atualização fortalece a credibilidade institucional ao longo do tempo, mesmo quando a informação disponível em determinado momento é limitada.

Parcerias formais com rádios comunitárias locais, veículos de imprensa, escolas, unidades de saúde e organizações comunitárias ampliam significativamente a capacidade municipal de confirmação e disseminação de informação verificada. Essas instituições funcionam como mediadoras de confiança entre o poder público e a população, podendo adaptar a linguagem da mensagem original ao contexto de seu público específico sem alterar a orientação central transmitida. O município deve disponibilizar proativamente materiais verificáveis e contatos oficiais atualizados para que esses parceiros não precisem depender de interpretações fragmentadas ou de informações de segunda mão obtidas informalmente.

Proteção de dados, segurança e continuidade operacional

Sistemas municipais de comunicação de emergência frequentemente lidam com dados sensíveis de localização, cadastros de pessoas em situação de vulnerabilidade e informações detalhadas sobre infraestruturas críticas do território. O uso responsável desses dados precisa respeitar rigorosamente princípios de finalidade específica, necessidade mínima e segurança adequada ao risco envolvido. A coleta indiscriminada de dados amplia riscos de exposição indevida sem necessariamente melhorar a qualidade da resposta institucional. O município deve definir com clareza quais informações são efetivamente indispensáveis para a operação do sistema, quem exatamente pode acessá-las e por quanto tempo elas serão mantidas armazenadas antes de descarte seguro.

A continuidade operacional do sistema exige cópias de segurança regulares, fontes de energia alternativa, equipamentos substitutos prontamente disponíveis e procedimentos manuais de contingência para o caso de falha completa dos sistemas digitais. Dependências invisíveis à primeira vista precisam ser cuidadosamente identificadas durante o planejamento. Um sistema municipal pode possuir servidores tecnicamente redundantes e, ainda assim, falhar completamente se todos esses servidores utilizarem o mesmo provedor único de conectividade à internet, ou se o acesso ao sistema depender de autenticação centralizada que fica indisponível

justamente durante um apagão de energia elétrica. Mapear essas dependências ocultas é parte essencial, e frequentemente negligenciada, do planejamento de resiliência tecnológica municipal.

Incidentes cibernéticos também podem comprometer diretamente a confiabilidade de alertas emitidos. A adulteração de uma mensagem oficial, seja por invasão externa seja por erro interno não detectado, possui elevado potencial de dano à população e à credibilidade institucional de longo prazo. Controles de acesso rigorosos, autenticação forte de múltiplos fatores, registros auditáveis de toda ação realizada e exigência de validação por mais de um responsável são necessários especificamente para os sistemas classificados como críticos. Contudo, esses controles de segurança precisam ser cuidadosamente compatibilizados com a urgência operacional: procedimentos excessivamente complexos de autenticação podem, na prática, impedir a emissão tempestiva de um alerta exatamente no momento em que ele se torna mais necessário.

Comunicação para grupos em situação de maior vulnerabilidade

O mapeamento de vulnerabilidade comunicacional deve ser simultaneamente territorial e social, combinando dados geográficos com características sociodemográficas da população residente. Áreas com baixa cobertura de rede, ocupações irregulares consolidadas, instituições de longa permanência, hospitais, escolas e locais com grande circulação de pessoas demandam estratégias comunicacionais específicas e diferenciadas entre si. A vulnerabilidade comunicacional não decorre apenas da ausência local de infraestrutura tecnológica; ela pode resultar igualmente de barreiras linguísticas entre grupos migrantes, limitações sensoriais não atendidas pelo desenho padrão das mensagens, baixa confiança histórica nas instituições públicas locais ou impossibilidade física concreta de cumprir a orientação recebida, como ocorre com pessoas idosas sem meio de transporte próprio.

Mensagens de evacuação, por exemplo, são estruturalmente insuficientes quando as pessoas destinatárias não possuem meio de transporte disponível, apoio familiar ou comunitário próximo, ou destino seguro conhecido para onde se deslocar. A comunicação eficaz precisa estar articulada, desde sua concepção, à capacidade material efetiva de resposta da população-alvo. Informar sem simultaneamente oferecer condições concretas de cumprimento da orientação pode transferir indevidamente a responsabilidade pelo próprio risco para a população mais vulnerável, aprofundando desigualdades sociais já existentes em vez de mitigá-las. Abrigos com localização conhecida, transporte assistido para pessoas com

mobilidade reduzida e equipes de apoio direto devem ser previstos em conjunto com os canais formais de aviso, não como medidas adicionais e eventuais.

A participação ativa de pessoas com deficiência e de representantes comunitários no próprio desenho do sistema de comunicação, e não apenas em sua avaliação posterior, melhora consideravelmente a adequação prática das mensagens produzidas. Testes de usabilidade conduzidos com usuários reais e exercícios simulados revelam problemas concretos que documentos técnicos elaborados em gabinete frequentemente não conseguem antecipar. Pequenas alterações na escolha de palavras, na sinalização visual utilizada ou na sequência de apresentação das instruções podem produzir diferenças importantes na compreensão efetiva alcançada pela população, especialmente entre grupos com menor familiaridade com a linguagem administrativa habitualmente empregada pelo poder público.

Sustentabilidade administrativa e capacidade burocrática

A manutenção de longo prazo de um sistema municipal de comunicação de emergência depende fundamentalmente de capacidade burocrática consolidada. Municípios precisam contar com equipes relativamente estáveis, conhecimento técnico internalizado, contratos adequadamente gerenciados e orçamento recorrente garantido, e não apenas recursos extraordinários obtidos em momentos de comoção pública após um desastre recente. A alta rotatividade de pessoal e a terceirização de funções críticas sem efetiva transferência de conhecimento para servidores efetivos fragilizam progressivamente a memória institucional do município. Quando um sistema é compreendido em profundidade apenas pelo fornecedor externo contratado ou por um único servidor específico, sua continuidade fica perigosamente exposta a mudanças de gestão ou de contrato.

Planos municipais devem especificar explicitamente custos previstos de manutenção continuada, substituição periódica de equipamentos e treinamento regular de pessoal, incorporando esses itens ao planejamento orçamentário plurianual. Equipamentos instalados sem testes periódicos ou sem atualização regular podem criar uma falsa sensação de segurança institucional, mascarando problemas que só se revelam no momento em que o sistema é efetivamente necessário. A sustentabilidade de longo prazo também envolve um princípio de simplificação deliberada: sistemas excessivamente complexos podem simplesmente ser incompatíveis com a escala administrativa e a capacidade técnica disponível em municípios de menor porte. Soluções tecnicamente robustas, mas compreensíveis e

operáveis pela equipe local, tendem a ser mais úteis na prática do que plataformas sofisticadas que exigem conhecimento especializado indisponível no quadro efetivo do município.

Consórcios intermunicipais e mecanismos de cooperação regional podem reduzir custos individuais, permitir o compartilhamento de especialistas escassos e integrar sistemas de alerta para riscos que, por sua própria natureza física, não respeitam fronteiras administrativas, como bacias hidrográficas ou áreas de instabilidade geológica compartilhadas entre municípios vizinhos. Essa cooperação regional precisa, no entanto, preservar responsabilidades locais claramente definidas e mecanismos próprios de decisão em cada município participante, evitando que a cooperação se transforme em diluição indevida de responsabilidade. O compartilhamento de infraestrutura entre municípios deve sempre ser acompanhado de acordos formais e claros sobre governança conjunta, divisão de financiamento e regras de uso compartilhado dos dados produzidos.

APLICAÇÃO MUNICIPAL E INDICADORES DE MATURIDADE

A arquitetura teórica proposta neste artigo pode ser operacionalizada por meio de um diagnóstico de maturidade institucional, permitindo que gestores municipais identifiquem em que estágio seu sistema atual se encontra e quais prioridades de investimento fazem mais sentido em cada momento. Um município em estágio inicial de maturidade tipicamente possui responsabilidades pouco definidas entre órgãos, canais de comunicação isolados entre si e baixa frequência de testes práticos de seus protocolos. No estágio intermediário, protocolos formais já existem no papel, mas a integração efetiva entre sistemas e a participação comunitária ainda permanecem desiguais entre diferentes regiões do município. Em estágio avançado, a comunicação de emergência é efetivamente governada como sistema integrado, com redundância testada, acessibilidade incorporada ao desenho, monitoramento contínuo e mecanismos ativos de aprendizagem institucional.

Indicadores de autoridade institucional incluem a existência formal de protocolo escrito, o tempo médio efetivamente necessário para autorização de um alerta e a clareza documentada dos critérios de substituição em caso de indisponibilidade do responsável primário. Indicadores de interoperabilidade podem ser avaliados pelo número de órgãos efetivamente integrados ao sistema, pela frequência de atualização dos dados compartilhados e pelo tempo médio necessário para compartilhamento de

informação relevante entre setores. Indicadores de redundância envolvem cobertura territorial efetivamente testada, grau de independência tecnológica entre os canais disponíveis e capacidade demonstrada de funcionamento sob condições de falha parcial da infraestrutura. Indicadores de qualidade das mensagens podem ser medidos por taxas de compreensão aferidas em pesquisa, grau de acionabilidade percebida pelos destinatários e nível de consistência entre diferentes canais utilizados simultaneamente.

Indicadores de participação comunitária podem ser observados pela presença efetiva e ativa de núcleos comunitários organizados, pela realização regular de exercícios simulados com participação popular e pela inclusão documentada de grupos em situação de vulnerabilidade no planejamento do sistema. Indicadores de aprendizagem institucional envolvem a realização sistemática de auditorias pós-evento, a taxa de execução efetiva das recomendações produzidas por essas auditorias e a frequência de atualização formal dos planos municipais à luz da experiência acumulada. É importante ressaltar que esses indicadores devem apoiar prioritariamente a melhoria contínua do sistema, e não servir apenas para produzir rankings comparativos entre municípios sem considerar diferenças relevantes de contexto. Comparações entre municípios distintos precisam necessariamente considerar diferenças de território, de recursos disponíveis e de perfil específico de risco enfrentado por cada localidade.

A implementação prática da arquitetura pode começar de forma focalizada, priorizando as ameaças de maior relevância local em vez de buscar cobertura simultânea de todos os riscos possíveis. Municípios sujeitos a inundações recorrentes podem começar mapeando bacias hidrográficas, rotas de evacuação viáveis e comunidades já conhecidamente expostas; cidades com riscos tecnológicos relevantes, como proximidade a instalações industriais de risco, podem priorizar a integração com empresas responsáveis e com serviços de saúde especializados. A estrutura conceitual da arquitetura permanece comum a diferentes contextos, mas os protocolos concretos de aplicação devem necessariamente refletir as particularidades de cada território. A padronização excessiva de protocolos, sem adaptação ao contexto local, pode ignorar diferenças que efetivamente determinam o sucesso ou o fracasso da resposta em cada caso concreto.

Exercícios simulados constituem instrumento central e insubstituível dessa arquitetura de governança. Eles permitem testar, em condições controladas, a cadeia completa de decisão, a formulação de mensagens, o funcionamento efetivo dos canais disponíveis e a reação real da comunidade, sem que seja necessário aguardar a ocorrência de um desastre verdadeiro para descobrir

falhas no sistema. Simulações bem desenhadas devem incluir deliberadamente cenários de falha de energia, indisponibilidade temporária de rede móvel e ausência inesperada de agentes-chave do processo decisório, testando assim a robustez do sistema sob condições adversas e não apenas seu funcionamento ideal. A avaliação de cada exercício precisa registrar cuidadosamente os tempos observados e as decisões efetivamente tomadas em cada etapa, produzindo ao final um plano concreto de correção com responsáveis e prazos definidos, replicando a mesma lógica de aprendizagem institucional discutida na seção 4.6.

CONSIDERAÇÕES FINAIS

Este artigo propôs uma arquitetura teórica para a governança da comunicação de emergência em cidades inteligentes, construída a partir da articulação entre governança multinível, teorias de comunicação de crise e risco, modelos comportamentais de resposta a alertas, estudos sobre cidades inteligentes e resiliência urbana, e literatura consolidada sobre sistemas de alerta precoce. O modelo proposto reúne seis dimensões interdependentes: autoridade institucional definida, interoperabilidade operacional e tecnológica, redundância entre canais digitais e analógicos, mensagens acessíveis e acionáveis, participação comunitária efetiva e aprendizagem institucional contínua. A análise realizada ao longo do artigo demonstra, de forma consistente, que a resiliência comunicacional depende sempre da combinação entre infraestrutura tecnológica disponível e capacidade estatal de coordenação, e não de qualquer um desses fatores isoladamente considerado.

A contribuição central deste trabalho consiste em deslocar deliberadamente o debate público e acadêmico da quantidade de tecnologia disponível para a qualidade da governança efetivamente praticada. Sensores ambientais, plataformas integradas e recursos de inteligência analítica podem certamente apoiar de forma relevante a proteção da população, mas eles não substituem protocolos claros, coordenação interorganizacional testada e confiança pública construída ao longo do tempo. Municípios genuinamente resilientes são aqueles capazes de manter comunicação útil e confiável mesmo quando partes significativas de sua infraestrutura tecnológica falham, precisamente porque sua resiliência não depende de um único componente, mas de um sistema deliberadamente redundante e bem coordenado.

A arquitetura proposta também evidencia, de forma que merece destaque, que a inclusão comunicacional não constitui dimensão periférica ou opcional

do sistema. Um sistema que alcança rapidamente a maioria da população, mas sistematicamente exclui grupos já em situação de maior exposição ao risco, não pode ser razoavelmente considerado eficaz, independentemente de sua sofisticação técnica geral. A acessibilidade deve orientar o desenho do sistema desde sua concepção inicial, e a participação comunitária deve integrar organicamente o planejamento municipal, e não ser tratada como etapa complementar acrescentada ao final do processo de desenvolvimento tecnológico.

Como limitação principal, é importante reconhecer que o modelo aqui apresentado é de natureza teórica e requer validação empírica subsequente para confirmar sua aplicabilidade prática em diferentes contextos municipais brasileiros. Estudos futuros podem aplicar essa arquitetura em municípios de diferentes portes populacionais e capacidades administrativas, comparar níveis de maturidade institucional entre eles e analisar retrospectivamente eventos reais de emergência à luz das seis dimensões propostas. Pesquisas subsequentes também podem desenvolver escalas de mensuração mais precisas para cada dimensão, examinar de forma sistemática os custos efetivos de implementação em diferentes contextos e investigar empiricamente a relação entre confiança institucional prévia, compreensão efetiva da mensagem recebida e comportamento real de resposta da população durante emergências concretas.

Para a gestão pública municipal, a implicação prática mais direta deste trabalho é a seguinte: a comunicação de emergência deve ser tratada como política pública permanente, dotada de orçamento próprio, responsabilidades claramente atribuídas, testes regulares e avaliação sistemática de resultados, e não como resposta episódica mobilizada apenas depois da ocorrência de um desastre. A preparação institucional construída deliberadamente em períodos de normalidade administrativa determina, em última análise, a capacidade real do município de informar adequadamente e proteger efetivamente sua população no momento em que a crise finalmente ocorre.

REFERÊNCIAS

- Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, 22(1), 3-21. <https://doi.org/10.1080/10630732.2014.942092>
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543-571. <https://doi.org/10.1093/jopart/mum032>

- Argyris, C., & Schön, D. A. (1978). *Organizational learning: A theory of action perspective*. Addison-Wesley.
- Arnstein, S. R. (1969). A ladder of citizen participation. *Journal of the American Institute of Planners*, 35(4), 216-224. <https://doi.org/10.1080/01944366908977225>
- Basher, R. (2006). Global early warning systems for natural hazards: Systematic and people-centred. *Philosophical Transactions of the Royal Society A*, 364(1845), 2167-2182. <https://doi.org/10.1098/rsta.2006.1819>
- Boin, A., & 't Hart, P. (2003). Public leadership in times of crisis: Mission impossible? *Public Administration Review*, 63(5), 544-553. <https://doi.org/10.1111/1540-6210.00318>
- Boin, A., 't Hart, P., Stern, E., & Sundelius, B. (2005). *The politics of crisis management: Public leadership under pressure*. Cambridge University Press.
- Bozeman, B. (2007). *Public values and public interest: Counterbalancing economic individualism*. Georgetown University Press.
- Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. *Journal of Urban Technology*, 18(2), 65-82. <https://doi.org/10.1080/10630732.2011.601117>
- Coaffee, J. (2013). *Resilient cities: Urban planning, risk and disaster management*. Routledge.
- Comfort, L. K. (2007). Crisis management in hindsight: Cognition, communication, coordination, and control. *Public Administration Review*, 67(s1), 189-197. <https://doi.org/10.1111/j.1540-6210.2007.00827.x>
- Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review*, 10(3), 163-176. <https://doi.org/10.1057/palgrave.crr.1550049>
- Cutter, S. L., Boruff, B. J., & Shirley, W. L. (2003). Social vulnerability to environmental hazards. *Social Science Quarterly*, 84(2), 242-261. <https://doi.org/10.1111/1540-6237.8402002>
- Dawes, S. S. (2009). Stewardship and usefulness: Policy principles for information-based transparency. *Government Information Quarterly*, 27(4), 377-383.
- Deetz, S. (2001). Conceptualizing organization-stakeholder communication. *Management Communication Quarterly*, 15(1), 51-60. <https://doi.org/10.1177/0893318901151003>
- Drabek, T. E. (1986). *Human system responses to disaster: An inventory of sociological findings*. Springer-Verlag.
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Hooghe, L., & Marks, G. (2003). Unraveling the central state, but how? Types of multi-level governance. *American Political Science Review*, 97(2), 233-243.
<https://doi.org/10.1017/S000305540300064X>

International Organization for Standardization. (2018). ISO 22320:2018 - Security and resilience: Emergency management - Guidelines for incident management.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences*. Sage.

Lindell, M. K., & Perry, R. W. (2012). The protective action decision model: Theoretical modifications and additional evidence. *Risk Analysis*, 32(4), 616-632.
<https://doi.org/10.1111/j.1539-6924.2011.01647.x>

Meerow, S., Newell, J. P., & Stults, M. (2016). Defining urban resilience: A review. *Landscape and Urban Planning*, 147, 38-49. <https://doi.org/10.1016/j.landurbplan.2015.11.011>

Mileti, D. S., & Sorensen, J. H. (1990). *Communication of emergency public warnings: A social science perspective and state-of-the-art assessment*. Oak Ridge National Laboratory.

Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. PublicAffairs.

Ostrom, E. (1996). Crossing the great divide: Coproduction, synergy, and development. *World Development*, 24(6), 1073-1087. [https://doi.org/10.1016/0305-750X\(96\)00023-X](https://doi.org/10.1016/0305-750X(96)00023-X)

Palen, L., & Anderson, K. M. (2016). Crisis informatics—New data for extraordinary times. *Science*, 353(6296), 224-225. <https://doi.org/10.1126/science.aag2579>

Perry, R. W., & Lindell, M. K. (2003). Understanding citizen response to disasters with implications for terrorism. *Journal of Contingencies and Crisis Management*, 11(2), 49-60.
<https://doi.org/10.1111/1468-5973.1102001>

Piattoni, S. (2009). Multi-level governance: A historical and conceptual analysis. *European Integration Online Papers*, 13(2), 1-25.

Quarantelli, E. L. (1988). Disaster crisis management: A summary of research findings. *Journal of Management Studies*, 25(4), 373-385. <https://doi.org/10.1111/j.1467-6486.1988.tb00043.x>

Reynolds, B., & Seeger, M. W. (2005). Crisis and emergency risk communication as an integrative model. *Journal of Health Communication*, 10(1), 43-55.
<https://doi.org/10.1080/10810730590904571>

Sutton, J., Palen, L., & Shklovski, I. (2008). Backchannels on the front lines: Emergent uses of social media in the 2007 southern California wildfires. *Proceedings of the 5th International ISCRAM Conference*, 624-632.

Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review*, 15(4), 404-428. <https://doi.org/10.1177/1534484316671606>

United Nations Office for Disaster Risk Reduction. (2015). Sendai framework for disaster risk reduction 2015-2030. United Nations.

United Nations International Strategy for Disaster Reduction. (2005). Hyogo framework for action 2005-2015: Building the resilience of nations and communities to disasters. United Nations.

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). The risk perception paradox—Implications for governance and communication of natural hazards. *Risk Analysis*, 33(6), 1049-1065. <https://doi.org/10.1111/j.1539-6924.2012.01942.x>

Waugh, W. L., & Streib, G. (2006). Collaboration and leadership for effective emergency management. *Public Administration Review*, 66(s1), 131-140. <https://doi.org/10.1111/j.1540-6210.2006.00673.x>

Weick, K. E. (1988). Enacted sensemaking in crisis situations. *Journal of Management Studies*, 25(4), 305-317. <https://doi.org/10.1111/j.1467-6486.1988.tb00039.x>

CONTRIBUIÇÃO DO AUTOR

Moisés Figueiredo da Silva: conceituação, metodologia, investigação, análise formal, redação do manuscrito original, revisão e edição e supervisão. Curadoria de dados e obtenção de financiamento não se aplicam a este estudo teórico.

DECLARAÇÕES EDITORIAIS

Financiamento: o estudo não recebeu financiamento externo.

Conflito de interesses: o autor declara não haver conflito de interesse.

Uso de inteligência artificial: não declarado pelo autor.