noemicajournal.org

e-ISSN: 3086-7037

ARTICLE

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

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

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

Moisés Figueiredo da Silva[1]

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

SUBMITTED	ACCEPTED	PUBLISHED	DOI
17/05/2024	11/10/2024	06/12/2024	in process

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

INTRODUCTION

The intensification of extreme weather events, socio-environmental disasters, health crises, and critical infrastructure failures has placed local governments in situations where the time available to decide is short and uncertainty remains high. In densely occupied urban areas, a message issued late, worded ambiguously, or distributed with limited reach can compromise evacuation routes, increase the exposure of vulnerable groups, and hinder the work of response teams. Emergency communication is therefore not an ancillary activity of civil defense. It is part of the very core of the state's capacity to protect lives, coordinate resources, and preserve public trust in contexts of acute uncertainty.

The advance of smart cities has expanded the tools available for monitoring and disseminating alerts. Environmental sensors, georeferenced systems, integrated platforms, mobile networks, and large-scale data analysis make it possible to identify threats and distribute information with a speed unmatched in previous decades. However, the existence of digital infrastructure does not eliminate governance problems. Systems can remain disconnected from one another, agencies can dispute authority over message content, and significant portions of the population may fail to receive or understand the warning. Technology improves communication only when it is embedded in institutional arrangements capable of defining responsibilities, validating information, and sustaining alternative channels during failures.

The research problem stems from this mismatch between technological sophistication and institutional capacity. Municipalities that invest in control centers and applications can remain vulnerable if they lack common protocols among civil defense, health, mobility, public safety, communications, and public service providers. Fragmentation produces contradictory messages, delays, duplicated effort, and loss of institutional credibility. In risk situations, trust functions as an operational resource: official guidance tends to be less effective when the population does not recognize the issuing authority or perceives inconsistency among public sources, a phenomenon already documented in the literature on behavioral response to warnings (Lindell & Perry, 2012; Mileti & Sorensen, 1990).

The research is justified for three reasons. First, the Brazilian literature on smart cities still treats risk communication as a technical appendix, when it should instead be treated as a governance subsystem with its own logic. Second, the international emergency management literature offers mature concepts on coordination, warning, and response behavior, but is rarely connected to debates on smart urban infrastructure, producing a gap between fields that should be in dialogue. Third, recent events in Brazil and other countries, including urban flooding, landslides, heat waves, and telecommunications failures during disasters, have shown that the absence of a governance architecture undermines outcomes even when the available technology is adequate.

The guiding question of this article is as follows: how can a governance architecture for emergency communication be structured that integrates technological resources, institutional coordination, inclusion, and community participation in smart municipalities? The general objective is to propose a theoretical model capable of guiding the diagnosis, planning, and evaluation of municipal risk and crisis communication systems. As specific objectives, the article seeks to: (a) systematize the main theoretical contributions on multilevel governance, crisis communication, and early warning systems applicable to the municipal context; (b) identify the constitutive dimensions of a communication governance architecture; and (c) discuss sociotechnical vulnerabilities that undermine the effectiveness of these architectures even in contexts of high technological capacity.

The article's contribution lies in treating communication resilience as a sociotechnical capacity, avoiding both technological reductionism, which assumes that more data and more platforms solve the problem, and a strictly administrative reading, which reduces emergency communication to a flowchart of competencies. The central argument holds that resilient communication results from the articulation of authority, interoperability, redundancy, message quality, social reach, and organizational learning. These dimensions do not operate independently. A technically correct message can fail without an adequate reach channel; a redundant network can spread inconsistent guidance when there is no defined command; and community participation loses effectiveness when it is not linked to official protocols. The architecture proposed in this text seeks to make these interdependencies explicit and to offer researchers and public managers a shared vocabulary for analyzing and designing municipal emergency communication systems.

The article is organized into seven sections, in addition to this introduction. The second section presents the theoretical framework, articulating multilevel governance, smart cities and urban resilience, crisis and risk communication theories, behavioral models of warning response, and early warning systems. The third section describes the methodological path of the integrative review. The fourth section details the six dimensions of the proposed architecture. The fifth section discusses sociotechnical vulnerabilities and the limits of technocentrism. The sixth section addresses municipal application and maturity indicators. The seventh section presents the final considerations.

THEORETICAL FRAMEWORK

The construction of the model draws on five fields: multilevel governance, smart cities and urban resilience, crisis and risk communication theories, behavioral models of warning response, and early warning systems and emergency telecommunications. This approach is necessary because urban crises cross administrative, technical, and disciplinary boundaries. Risk is detected by certain systems, interpreted by specialized teams, turned into decisions by authorities, and communicated to people who have different resources, knowledge, and mobility conditions. Final performance depends on the entire chain, not just one isolated component, which requires a framework capable of connecting public administration, political science, urban studies, disaster management, and organizational communication.

Multilevel governance and institutional coordination in disasters

Emergency management can rarely be carried out by a single organization. Federal, state, and municipal governments, health services, security forces, fire departments, energy and telecommunications providers, community organizations, and the media all take part in distinct stages of the risk management cycle. Multilevel governance describes arrangements in which competencies and resources are distributed among interdependent levels and actors, with authority dispersed across overlapping jurisdictional spheres (Hooghe & Marks, 2003; Piattoni, 2009). In disasters, this interdependence becomes especially visible, because local decisions frequently depend on data produced at the state or federal level, on infrastructure operated by private companies, and on logistical support from outside the municipality.

Horizontal coordination is equally important and, in many cases, harder to achieve than vertical coordination. Municipal departments often operate with their own systems, terminology, and routines, developed over decades of sector-specific operation. Without shared protocols, information circulates slowly or loses precision as it crosses organizational boundaries. The collaborative governance literature offers elements for understanding the construction of interinstitutional forums, participation rules, trust, and commitment among actors with a history of mutual distrust or competition for resources (Ansell & Gash, 2008). In emergency communication, these elements need to be defined before the crisis, while there is still time to negotiate responsibilities, test information flows, and resolve technical and political incompatibilities.

The literature on crisis leadership reinforces this point by describing crisis management as a process of collective sensemaking under time pressure, in which leaders must simultaneously understand the event, coordinate the response, and communicate meaning to internal and external audiences (Boin & 't Hart, 2003; Boin et al., 2005). Comfort (2007) describes this challenge as a problem of cognition, communication, coordination, and control: disaster response systems fail not only from a lack of resources, but from an inability to process and share relevant information at the pace the event demands. Weick (1988) had already observed that crisis situations are characterized by a low capacity to interrupt action for deliberation, which requires organizational structures able to act and learn simultaneously rather than sequentially.

Clarity of command does not imply concentrating all decisions in a single body. Certain threats require knowledge distributed across territorial units and decentralized responses, especially in large and heterogeneous cities. The decisive point is to define who validates the alert, who authorizes its issuance, which agencies supplement the message with specialized information, and how disagreements between technical interpretations are resolved. The absence of such rules favors both institutional silence, when no agency feels authorized to act, and a proliferation of competing messages, when several agencies act without coordination. The governance architecture proposed here must therefore combine technical authority, political legitimacy, and operational capacity, drawing on the classic distinction between public value, legitimacy, and administrative capacity found in the public administration literature (Bozeman, 2007).

Smart cities and sociotechnical urban resilience

The concept of the smart city was initially associated with the digitization of services, expanded connectivity, and the intensive use of urban data. Later studies showed that technological infrastructure alone does not define urban intelligence; institutional capacities, citizen participation, and environmental sustainability are also constitutive elements of the concept, not merely complementary ones (Caragliu et al., 2011; Albino et al., 2015). The critique of technocentrism is especially relevant to emergency management, since sophisticated systems can fail precisely when infrastructure is subjected to extreme conditions, such as demand spikes on mobile networks during mass evacuations or power outages at data centers.

Authors such as Kitchin (2014) warn that the promise of data-driven cities often ignores the social and organizational conditions needed to turn data into useful decisions. Morozov (2013) describes as "technological solutionism" the tendency to treat complex problems of a social and institutional nature as though they could be solved by standalone apps or platforms. This critique does not deny the value of technology, but indicates that its benefit depends on institutional mediation: a sensor that detects flooding does not, by itself, produce an evacuation decision, nor does it guarantee that the information reaches those who need it.

Urban resilience corresponds to the capacity of an urban system to resist, absorb, adapt to, and recover from disturbances while preserving its essential functions (Meerow et al., 2016). This definition encompasses both physical and social systems. Power grids, telecommunications, and transportation are components of resilience as important as institutional trust, local knowledge, interorganizational coordination, and community solidarity. Coaffee (2013) describes urban resilience as a planning objective that combines physical infrastructure, governance, and social capacity for adaptation, arguing that resilient cities are not merely well-equipped cities, but cities capable of learning from recurring disturbances.

Communication connects these dimensions in a particular way: it informs about the threat, guides individual and collective behavior, organizes response resources, and allows institutions to update their understanding of the event as it unfolds. The notion of communication resilience, as used in this article, designates the capacity to maintain reliable information flows during sudden changes, infrastructure disruptions, and conditions of heightened uncertainty. This is not merely the technical continuity of a system. A network can remain technically active and still produce messages that are incomprehensible, contradictory, or unsuited to the local context. Communication resilience must therefore be assessed according to criteria of availability, integrity, reach, accessibility, consistency across sources, and the practical usefulness of the information for those who receive it.

Crisis and risk communication theories

A second theoretical pillar, absent from the initial version of this work and incorporated here because it is central to the problem under investigation, is the field of crisis and risk communication, developed mainly over the last three decades in organizational communication and public health studies. The Crisis and Emergency Risk Communication model, known by the acronym CERC, proposes that effective communication in crisis situations follows recognizable stages, from the pre-event phase to resolution, each requiring distinct communication objectives, such as reducing initial uncertainty, guiding immediate protective actions, and later, accounting for decisions and restoring public trust (Reynolds & Seeger, 2005). This model reinforces a point already central to the architecture proposed in this article: emergency communication is not a single event, but a continuous process that begins before the crisis, with the building of institutional credibility, and continues after it, with accountability.

Situational Crisis Communication Theory, developed by Coombs (2007) in the field of organizational reputation management, offers another relevant contribution by proposing that the communication response strategy should be proportional to the level of responsibility the public attributes to the issuing organization and to its history of previous crises. Although originally formulated for the corporate context, this theory helps explain why municipalities with a history of poor communication during previous emergencies face greater public resistance even when they issue technically correct alerts: accumulated credibility, or the lack of it, shapes how a message is received even before its content is evaluated.

Deetz (2001) draws attention to the relational dimension of organizational communication, arguing that communication between institutions and publics should not be understood merely as the transmission of information, but as a process of building shared meaning, in which how something is communicated matters as much as what is communicated in determining the institution's legitimacy with its interlocutors. This perspective is relevant to emergency communication because it shifts attention from the simple issuance of alerts to the quality of the relationship built over time between government and citizens.

Behavioral models of warning response

A third pillar incorporated in this expanded version concerns the question of what leads people to act, or not to act, in response to an official warning. The Protective Action Decision Model, formulated by Lindell and Perry (2012) based on decades of empirical research on disaster behavior, describes the process by which individuals receive, interpret, and decide whether or not to respond to risk information. The model identifies variables such as threat perception, trust in the source, the social norms of the individual's reference group, and the resources available to act, such as personal transportation or a support network, as central determinants of behavioral response. The practical implication is direct: issuing a technically correct alert does not guarantee an appropriate response, because the decision to act depends on factors that go beyond the textual content of the message.

Perry and Lindell (2003) synthesize earlier findings from sociological disaster research, showing that most of the population does not respond to a first warning with immediate action, but instead seeks confirmation from multiple sources before acting, a behavior known as milling. This finding has a direct consequence for the design of municipal systems: if people tend to verify a warning before acting, the communication architecture needs to provide multiple channels that are consistent with one another, so that confirmation is fast and does not introduce contradiction. Quarantelli (1988) and Drabek (1986), in their classic reviews of sociological disaster research, had already shown that popular myths about widespread panic in emergencies are generally unfounded; the predominant behavior is a rational search for information and mutual aid among neighbors, which reinforces the relevance of the community dimension discussed later in this article.

Risk perception is also not uniform across social groups. Wachinger et al. (2013), in a review of the so-called risk perception paradox, show that individuals who have lived longer in areas exposed to recurring threats may develop an underestimation of risk, an effect that public communication needs to take into account by avoiding standardized messages that ignore the accumulated experience of the local population. Cutter et al. (2003), for their part, developed a social vulnerability index to environmental hazards that remains widely used to identify populations with lower capacity to respond to disasters, considering variables such as income, age, family composition, and access to resources, and which can guide the territorial mapping of communication priorities discussed in section 4 of this article.

Early warning systems and emergency telecommunications

Early warning systems combine risk knowledge, continuous monitoring, dissemination of warnings, and the response capacity of both the population and institutions (Basher, 2006). Detecting a threat does not reduce harm when the warning fails to reach exposed people or fails to prompt an adequate response. This chain emphasizes that communication and community preparedness are constitutive parts of the warning system, not steps that come after it. The municipality needs to know the exposed areas, groups with specific needs, the means of communication actually available to the local population, and the barriers that may prevent the guidance issued from being followed.

Leading international documents on disaster risk reduction, such as the Hyogo Framework (UNISDR, 2005) and its successor, the Sendai Framework (UNDRR, 2015), explicitly highlight people-centered early warning systems as a priority for action by national and local governments, recognizing that the effectiveness of a warning depends both on the scientific quality of the forecast and on communities' ability to understand it and act on it. The international standard ISO 22320:2018, focused on incident management, reinforces the need for clearly defined command, control, and coordination structures as a precondition for effective response, in line with the argument on institutional authority developed in section 4.1 of this article.

Mobile networks, cell broadcast, geolocated messages, radio, television, sirens, and digital platforms can together form a warning ecosystem. The choice of channels should consider the type of threat, the time available before impact, the characteristics of the territory, and local infrastructure conditions. Sudden alerts, such as dam failures or unexpected landslides, require far-reaching means with low dependence on prior user action, such as cell broadcast, which requires no registration or installed application. Slower-developing events, such as gradual flooding or prolonged heat waves, allow for progressive communication, updated scenarios, and advance preparation of shelters.

Redundancy does not simply mean multiplying channels. Different channels need to be activated through coordinated procedures and must convey consistent content across one another. They should also have distinct technical dependencies. Two applications that rely on the same mobile network infrastructure do not represent effective redundancy in the face of a telecommunications collapse. Combining digital media, traditional broadcasting, sirens, institutional operational radio, and community networks reduces the probability of common-mode failure, a reliability engineering principle applied to the communication domain. Studies on crisis informatics, a field that examines the use of digital media during disasters, show that social networks serve as a valuable complementary channel, both for official dissemination and for gathering field reports, but they do not replace formal warning channels, especially among populations with lower digital literacy (Palen & Anderson, 2016; Sutton et al., 2008).

METHODOLOGICAL APPROACH

The study adopts an integrative theoretical review, a method well suited to building conceptual models that combine distinct fields of knowledge that do not yet have a consolidated synthesis (Torraco, 2016). The procedure did not seek to produce a quantitative estimate of effects, nor to test causal hypotheses, but to identify concepts, relationships, and conditions relevant to the municipal governance of emergency communication. Contributions from public administration, political science, urban studies, disaster management, information systems, and organizational communication were examined, deliberately seeking to cross disciplinary boundaries that, in the current literature, tend to remain isolated.

The analysis proceeded through four successive movements. The first consisted of mapping the gaps between the smart cities literature, predominantly focused on infrastructure and data, and civil defense and disaster management studies, predominantly focused on institutional coordination and human behavior. The second organized a conceptual matrix crossing institutional, technological, and social dimensions identified in both fields. The third translated this matrix into components of a governance architecture, seeking formulations applicable to the reality of Brazilian municipalities of different sizes. The fourth examined the dependency relationships among the components, failure risks, and possibilities for municipal application, including the maturity indicators discussed in section 6.

Priority was given to seminal and widely cited works in their respective fields, complemented by contributions published up to 2024, consistent with the volume's editorial period. The synthesis draws on both established academic literature, published in journals such as the Journal of Contingencies and Crisis Management, Disaster Prevention and Management, Public Administration Review, and Journal of Urban Technology, and relevant international institutional documents on disaster risk reduction, produced by bodies such as the United Nations and the International Organization for Standardization. As this is a theoretical proposal, the validity of the model depends on subsequent confrontation with case studies, simulation exercises, and data from real events in Brazilian municipalities. This limitation is acknowledged as part of the research agenda presented in the final considerations.

THEORETICAL ARCHITECTURE OF EMERGENCY COMMUNICATION GOVERNANCE

The proposed architecture starts from a simple premise that is frequently overlooked in municipal practice: emergency communication is a critical public service and must be governed as a system. This means defining objectives, authorities, information flows, resources, controls, performance indicators, and mechanisms for continuous learning. Acquiring equipment or platforms represents only one part of this system, and often the least determining part. Performance depends on how these resources are integrated into administrative routines and interorganizational relationships built over time.

The six dimensions that make up the model form an interdependent structure, not a checklist of independent items. Authority establishes legitimacy and decision-making capacity; interoperability integrates dispersed data and actors; redundancy maintains continuity under failure; message quality turns raw information into useful guidance; participation expands reach and territorial fit; and learning corrects failures and updates the system over time. The model can be used both to diagnose institutional maturity and to design public policy and post-event evaluation, as detailed in section 6.

Clearly defined institutional authority and role clarity

The first dimension corresponds to defining the authority responsible for issuing the alert and for the overall coordination of emergency communication. In many Brazilian municipalities, civil defense, the mayor's office, the communications department, and sectoral agencies have partially overlapping competencies, a result of administrative structures built incrementally, without systematic review. This lack of definition can delay warnings or allow political considerations to interfere with decisions that should follow technical criteria. Formal protocols need to specify alert levels, objective activation criteria, named officials responsible, and their substitutes at each level of the hierarchy.

Authority must be accompanied by clear mechanisms for technical validation. Preliminary data often contain significant uncertainty, and seeking absolute certainty before acting can dangerously delay preventive measures. The protocol needs to establish how to communicate uncertainty to the public without undermining the message's credibility, and how to update recommendations as new information arrives. It also needs to define who officially speaks on the municipality's behalf, how technical specialists take part in formulating the message, and how information produced by state or federal agencies, such as meteorological institutes or river basin agencies, is incorporated into the local decision-making process.

Continuity of command requires on-call rosters, alternative contacts, and formal delegation of authority set out in internal rules. Emergencies frequently occur outside regular administrative hours and can directly affect the very agents responsible for the decision, whether through displacement, unavailability of communication, or the personal impact of the event. Plans that depend on a single person or a single authorization are structurally fragile. Governance must provide for automatic substitution, formal recording of decisions taken, and authority proportional to the risk faced, so that on-call agents do not need to wait for authorization from unavailable superiors in the face of an imminent threat.

Operational and technological interoperability

Interoperability is the capacity of systems and organizations to exchange information while preserving its original meaning. On the technical level, it involves data formats, application programming interfaces, common identifiers, and security protocols. On the organizational level, it involves shared terminology, common classification criteria among agencies, and clear procedures for using the information received. Mere technological integration, without prior agreement on concepts and criteria, may only accelerate the circulation of mutually incompatible data, creating the illusion of integration without its real benefits.

Municipal operations centers need to consolidate information from meteorology, urban mobility, public health, urban infrastructure services, and field reports from response teams. The quality of this consolidation depends on how often data is updated, the traceability of its origin, and clear validation procedures before public release. Data from automated sensors need to be combined with the territorial knowledge accumulated by local teams and by residents of at-risk areas, avoiding decisions made solely on the basis of digital dashboards disconnected from conditions observed in the field. Interoperability does not eliminate the need for qualified human judgment; it expands the base available for that judgment.

Formal agreements with energy, water, and telecommunications providers are essential, since these companies simultaneously influence both the level of risk faced by the population and the municipality's capacity to respond. Such agreements should establish timely sharing of operational information, minimum service levels during emergencies, institutional emergency contacts available around the clock, and clear criteria for protecting any personal data that is shared. Dependence on private infrastructure cannot result in opacity toward the public authorities responsible for protecting the population, especially in municipalities where the provision of essential services is operated by companies headquartered outside the local territory.

Redundancy between digital and analog channels

Structural redundancy presupposes the existence of channels with distinct technologies, reach, and vulnerabilities, so that the failure of one does not compromise the functioning of the others. Applications and social networks are useful for detailed updates and continuous engagement with the population, but they depend on stable connectivity and active user behavior, such as keeping notifications enabled and reviewing content received. Cell broadcast and text messages potentially have wider reach because they do not require prior registration, although they also depend on the local mobile network functioning. Radio, television, sirens, sound trucks, and community communication networks can operate as alternatives that are relatively independent of these digital infrastructures.

Municipal planning should map areas without network coverage, shadow zones in rugged terrain, relatively isolated communities, and critical infrastructure whose failure would compromise multiple channels at once. Periodic tests, not merely theoretical desktop simulations, make it possible to verify each channel's real reach and the actual time needed for activation under conditions close to a real emergency. Backup equipment, such as generators for sirens and radio stations, needs regular maintenance, alternative power sources, and personnel trained to operate them under pressure. Redundancy that does not exist in day-to-day administration is unlikely to be improvised successfully during the crisis itself.

It is also necessary to avoid uncoordinated message overload, a problem just as harmful as the absence of communication. Simultaneous issuance across multiple channels should preserve visual identity, an identifiable source, and a consistent core instruction, avoiding small wording variations between channels being interpreted by the public as a sign of institutional disagreement. Subsequent updates need to clearly indicate the time of issuance and exactly what changed relative to the previous message. This consistency across media reduces the spread of rumors and makes it easier for citizens and partner institutions, such as schools and health units, to verify information.

Accessible, contextualized, and actionable messages

An emergency message needs to answer practical, concrete questions: what exactly is the danger, where does it occur, who is exposed, what should the person do, when should they act, and where can they get reliable updates. Overly technical language shifts onto the public the task of interpreting risk from specialized terms, which is particularly problematic under time pressure. Vague messages, on the other hand, do not provide sufficient guidance for action, even when technically correct. Wording should balance informational precision, brevity, and clarity of guidance, following principles that have been systematized in the literature on public warnings for more than three decades (Mileti & Sorensen, 1990).

The actionability of a message depends heavily on the territorial context in which it will be received. Evacuation recommendations need to indicate specific routes, recognizable meeting points, and shelters with known addresses and capacity, rather than the generic instruction to "leave the risk area." Shelter-in-place guidance should clearly explain how to reduce exposure during the waiting period. When information is still uncertain, the message can and should indicate possible scenarios and objective criteria for future updates, rather than waiting for complete certainty before communicating anything. Hiding existing uncertainty undermines public trust at the moment when forecasts inevitably change over the course of the event.

Message templates pre-approved by all competent bodies significantly speed up issuance in urgent situations, but they do not replace the need to adapt to the specific context of each event. Banks of standardized text should cover different types of threat and different audiences, including plain-language versions and versions accessible to people with sensory or cognitive disabilities. Testing with residents of different profiles, carried out outside of crisis periods, helps identify wording ambiguities that are often not noticed by technical specialists accustomed to their field's own vocabulary.

Community participation and co-production of resilience

Communities are not merely passive recipients of official communication. Residents know alternative routes, recurring flooding spots, people with reduced mobility in their neighborhood, and informal mutual support networks that often appear in no public registry. Co-production incorporates this local knowledge into institutional planning and response, a concept originally developed by Ostrom (1996) to describe the joint production of public goods by the state and civil society. Community protection groups, resident associations, schools, and basic health units can significantly expand the reach and credibility of official communication, acting as intermediate points of trust between the municipal administration and the population.

Participation needs to occur before events happen, not merely as an improvised emergency response during the crisis. Community meetings, participatory risk mapping, and simulation exercises make it possible to discuss local priorities and pre-test how well messages are understood by the very population that will receive them. Arnstein's (1969) ladder of participation, although originally formulated for urban planning, remains useful for distinguishing superficial forms of consultation, which merely inform the population about decisions already made, from effective forms of partnership, in which residents concretely influence the design of the warning system. Community leaders can support the dissemination of information, but they should not be used as permanent substitutes for adequate public infrastructure. The partnership must be formally recognized, sustained by continuous training, and integrated into official communication channels, rather than treated as an informal, disposable resource.

Information produced by the population itself also requires careful verification before it can guide official decisions. Collaborative reporting platforms can indicate real-time occurrences with considerable operational usefulness, as shown by studies on the use of social media in wildfires and other disasters (Sutton et al., 2008), but rumors, outdated information, and duplicate reports are constant possibilities that governance needs to anticipate. Clear mechanisms for triage, cross-confirmation, and feedback to the community are necessary, so that encouraging participation does not result in information overload for the teams responsible for analyzing these reports.

Post-event learning and communication auditing

Every emergency reveals aspects that formal plans drawn up under routine conditions cannot anticipate. Systematic audits carried out after each event should reconstruct the decisions made, response times at each stage, the channels actually used, the message's real reach, and the level of understanding achieved by the population. The purpose of this audit is not merely to assign responsibility for any failures, but to produce genuine organizational learning, in the sense developed by Argyris and Schön (1978), who distinguish between superficial corrections to procedure and deeper changes to the assumptions that guide institutional action. Records of messages issued, system logs, interviews with the teams involved, and emergency response data help identify bottlenecks that would otherwise go unnoticed in purely administrative reports.

Evaluation needs to systematically include the perspective of the receiving public, not only the institutional perspective of whoever issued the message. Knowing that a message was technically sent does not show that it was actually received, let alone correctly understood by the recipient. Post-event opinion surveys, community evaluation meetings, and systematic analysis of complaints and questions received make it possible to assess the real effectiveness of the communication carried out. Groups in more vulnerable situations need to be heard specifically and directly, since overall averages of satisfaction or understanding can easily conceal significant exclusion of population subgroups.

The recommendations produced by these audits must be formally incorporated into municipal plans, supplier contracts, ongoing training programs, and budget items, with named officials and defined deadlines for implementation. Evaluation reports without clear responsibility and without set deadlines systematically tend not to produce concrete change in institutional practice. Genuine institutional learning occurs when accumulated experience actually changes routines, protocols, and decision-making criteria, not merely when it is carefully documented in reports that remain filed away.

SOCIOTECHNICAL VULNERABILITIES AND THE LIMITS OF TECHNOCENTRISM

The main vulnerability identified in the analysis is the belief, still widespread among public managers, that sophisticated digital systems replace consolidated institutional capacities. Municipal control centers can display large quantities of data on screens and dashboards without that abundance translating into coherent, timely decisions. Information abundance can even hinder the prioritization of actions when there are no clear triage criteria, a phenomenon already documented by the information overload literature in other organizational contexts. Technology, in this sense, amplifies both the capacities and the weaknesses already present in the administrative structure that uses it; it rarely creates institutional capacity from scratch.

Another significant vulnerability is excessive dependence on private technology vendors. Proprietary platforms can restrict the municipality's own access to complete technical documentation, integration with other systems, and independent auditing of their functioning. Procurement contracts need to include explicit clauses on service continuity, guaranteed minimum technical support, the possibility of full data export, and an obligation to promptly report security incidents. The municipality must retain sufficient internal technical knowledge to operate alternatives in the event of contract discontinuation and to independently assess the results presented by the vendor, avoiding the situation, observed in various administrative contexts, in which only the contracted company fully understands how the system acquired by public authorities actually works.

The automation of decision-making processes can also introduce systematic biases that are hard to notice without a specific audit. Predictive models trained on incomplete historical records tend to better represent areas already monitored and populations already visible to existing official systems. Informal regions, precarious settlements, or territories with historically lower state presence may appear on automated risk dashboards as low-risk areas, when in reality there is only an absence of data, not an absence of real threat. Eubanks (2018) documents, in a different but conceptually applicable context, how automated systems can reproduce and even amplify pre-existing inequalities when implemented without adequate scrutiny of their training data. Municipal governance must, therefore, deliberately combine automated information with qualified field observation and accumulated community knowledge, treating these two types of knowledge as complementary rather than as hierarchically ordered substitutes.

Cybersecurity is necessarily part of contemporary communication resilience. Warning systems can be targeted by denial-of-service attacks, attempts to tamper with content, or misuse to spread false information under an official guise. Access control, robust authentication mechanisms, auditable logs of actions, and specific contingency plans for cyber incidents are necessary in any critical municipal system. At the same time, overly rigid security measures cannot prevent the rapid activation of an alert in a genuine emergency. Technical design needs to carefully balance protection against misuse with operability under time pressure, a balance that is rarely trivial to achieve in practice.

Financial sustainability also imposes concrete limits on municipal emergency communication systems. Equipment requires periodic maintenance, software licensing, continuous connectivity, and regular staff training. Projects funded only at the initial implementation stage, with no budget provision for subsequent maintenance stages, tend to systematically deteriorate within a few years. Municipal planning must explicitly consider the total life-cycle cost of each system component and prioritize solutions that are technically robust and compatible with the administrative and financial capacity actually available in the municipality, rather than necessarily the most sophisticated solutions found on the market.

Institutional fragmentation and authority conflicts

Institutional fragmentation can produce serious communication failures even when each agency involved adequately performs its own internal function, considered in isolation. Civil defense may correctly monitor meteorological risk, the communications department may competently control official channels, and the mobility department may manage traffic routes well, but the absence of a common procedure among these bodies prevents individually solid capacities from turning into an integrated response. Authority conflicts typically arise when different agencies interpret the appropriate moment to issue an alert, or the specific content to be released to the public, differently. In fast-moving events, improvised negotiation between agencies consumes scarce time and considerably increases the likelihood of contradictory messages reaching the population.

The solution to this problem does not simply consist of centralizing all communication in a single agency, a decision many municipalities adopt intuitively after a poorly managed crisis. Excessive centralization can slow response and ignore relevant information produced locally by territorial teams. Institutional design needs instead to clearly distinguish between strategic decisions, technical validation of content, and operational execution of communication. Central authority should ensure overall message coherence, while territorial and sectoral teams contribute updated data and adaptations needed for the specific local context. Escalation protocols become especially important when a threat crosses municipal boundaries or involves services managed by another level of government, a common situation in river basins shared by multiple municipalities.

Formalizing protocols must necessarily be accompanied by working relationships built before any crisis occurs. Regular intersectoral meetings, joint simulation exercises, and shared evaluation of results allow agents from different agencies to become personally familiar with one another's competencies and limitations. Interpersonal trust built between teams significantly reduces the cost of coordination during the emergency itself and facilitates the circulation of still-preliminary information, which might otherwise be withheld out of caution. Without this prior bond, agencies tend either to withhold data for fear of individual accountability or, at the opposite extreme, to release information without sufficient technical validation under perceived urgency.

Misinformation, rumors, and the contest for public attention

Contemporary digital environments allow reports, images, and personal interpretations to circulate widely before any official confirmation of an ongoing event. This speed of circulation can support the municipal administration's own initial identification of occurrences, but it also favors the spread of unfounded rumors, records taken out of their original context, and potentially dangerous guidance presented as though it were official. Public communication needs to compete for attention with informal sources and emotionally compelling content, which often spreads faster than more sober institutional statements. Slow institutional responses create an information vacuum that tends to be quickly filled by unverified versions of what is happening.

Active rumor management should formally be part of the municipal communication plan, not treated as a reactive, improvised response. Designated teams need to continuously monitor recurring public doubts, identify false information with real potential for harm at an early stage, and respond through recognized, established official channels. Correcting false information should be direct, immediately present the corresponding valid guidance, and avoid unnecessarily amplifying irrelevant content by simply repeating it in order to debunk it. Explicit transparency about what is already known with certainty, what remains uncertain, and when a new update will be provided strengthens institutional credibility over time, even when the information available at a given moment is limited.

Formal partnerships with local community radio stations, news outlets, schools, health units, and community organizations significantly expand the municipality's capacity to confirm and disseminate verified information. These institutions act as trust intermediaries between government and the population, able to adapt the language of the original message to their specific audience's context without altering the core guidance conveyed. The municipality should proactively make verifiable materials and updated official contacts available, so that these partners do not need to rely on fragmented interpretations or informally obtained second-hand information.

Data protection, security, and operational continuity

Municipal emergency communication systems frequently handle sensitive location data, registries of vulnerable people, and detailed information on the territory's critical infrastructure. Responsible use of this data must rigorously respect the principles of specific purpose, minimal necessity, and security appropriate to the risk involved. Indiscriminate data collection increases the risk of improper exposure without necessarily improving the quality of the institutional response. The municipality must clearly define which information is genuinely indispensable for the system's operation, exactly who can access it, and how long it will be kept before secure disposal.

The system's operational continuity requires regular backups, alternative power sources, readily available replacement equipment, and manual contingency procedures for the case of a complete failure of digital systems. Dependencies that are not obvious at first sight need to be carefully identified during planning. A municipal system may have technically redundant servers and still fail completely if all those servers rely on the same single internet connectivity provider, or if access to the system depends on centralized authentication that becomes unavailable precisely during a power outage. Mapping these hidden dependencies is an essential, and frequently neglected, part of municipal technological resilience planning.

Cyber incidents can also directly compromise the reliability of alerts issued. Tampering with an official message, whether through external intrusion or an undetected internal error, carries a high potential for harm to the population and for long-term damage to institutional credibility. Rigorous access controls, strong multi-factor authentication, auditable logs of every action taken, and a requirement for validation by more than one responsible person are necessary specifically for systems classified as critical. However, these security controls need to be carefully reconciled with operational urgency: excessively complex authentication procedures can, in practice, prevent the timely issuance of an alert exactly when it is most needed.

Communication for groups in more vulnerable situations

Mapping communication vulnerability must be both territorial and social, combining geographic data with the sociodemographic characteristics of the resident population. Areas with poor network coverage, established informal settlements, long-term care institutions, hospitals, schools, and places with heavy foot traffic require specific, differentiated communication strategies. Communication vulnerability does not stem only from a local lack of technological infrastructure; it can equally result from language barriers among migrant groups, sensory limitations not addressed by standard message design, low historical trust in local public institutions, or the concrete physical impossibility of complying with the guidance received, as is the case for older people without their own means of transportation.

Evacuation messages, for example, are structurally insufficient when the intended recipients have no available means of transportation, no nearby family or community support, or no known safe destination to go to. Effective communication needs to be linked, from its very conception, to the target population's actual material capacity to respond. Informing people without simultaneously offering concrete means of complying with the guidance can improperly shift responsibility for the risk itself onto the most vulnerable population, deepening existing social inequalities rather than mitigating them. Shelters with known locations, assisted transportation for people with reduced mobility, and direct support teams should be planned together with formal warning channels, not as additional, occasional measures.

The active participation of people with disabilities and community representatives in the actual design of the communication system, not only in its later evaluation, considerably improves the practical suitability of the messages produced. Usability testing conducted with real users and simulation exercises reveal concrete problems that technical documents drafted at a desk often fail to anticipate. Small changes in word choice, in the visual signage used, or in the order in which instructions are presented can make an important difference in the actual understanding achieved by the population, especially among groups less familiar with the administrative language habitually used by public authorities.

Administrative sustainability and bureaucratic capacity

The long-term maintenance of a municipal emergency communication system depends fundamentally on consolidated bureaucratic capacity. Municipalities need relatively stable teams, internalized technical knowledge, properly managed contracts, and guaranteed recurring budget, not only extraordinary resources obtained during moments of public outcry after a recent disaster. High staff turnover and the outsourcing of critical functions without genuine transfer of knowledge to permanent staff progressively weaken the municipality's institutional memory. When a system is deeply understood only by the external contracted vendor or by a single specific staff member, its continuity is dangerously exposed to changes in management or contracts.

Municipal plans must explicitly specify expected costs for ongoing maintenance, periodic equipment replacement, and regular staff training, incorporating these items into multi-year budget planning. Equipment installed without periodic testing or regular updates can create a false sense of institutional security, masking problems that only become apparent at the moment the system is actually needed. Long-term sustainability also involves a principle of deliberate simplification: overly complex systems may simply be incompatible with the administrative scale and technical capacity available in smaller municipalities. Solutions that are technically robust but understandable and operable by the local team tend to be more useful in practice than sophisticated platforms that require specialized knowledge unavailable within the municipality's actual staff.

Intermunicipal consortia and regional cooperation mechanisms can reduce individual costs, allow scarce specialists to be shared, and integrate warning systems for risks that, by their very physical nature, do not respect administrative boundaries, such as river basins or areas of geological instability shared among neighboring municipalities. Such regional cooperation must, however, preserve clearly defined local responsibilities and each participating municipality's own decision-making mechanisms, preventing cooperation from turning into an improper dilution of responsibility. Infrastructure sharing between municipalities should always be accompanied by formal, clear agreements on joint governance, funding allocation, and rules for shared use of the data produced.

MUNICIPAL APPLICATION AND MATURITY INDICATORS

The theoretical architecture proposed in this article can be operationalized through an institutional maturity diagnosis, allowing municipal managers to identify what stage their current system is at and which investment priorities make the most sense at each moment. A municipality at an early stage of maturity typically has poorly defined responsibilities among agencies, isolated communication channels, and a low frequency of practical protocol testing. At an intermediate stage, formal protocols already exist on paper, but effective integration between systems and community participation still remain uneven across different regions of the municipality. At an advanced stage, emergency communication is effectively governed as an integrated system, with tested redundancy, accessibility built into the design, continuous monitoring, and active institutional learning mechanisms.

Institutional authority indicators include the formal existence of a written protocol, the average time actually needed to authorize an alert, and the documented clarity of substitution criteria in the event the primary official is unavailable. Interoperability indicators can be assessed through the number of agencies actually integrated into the system, the frequency with which shared data is updated, and the average time needed to share relevant information between sectors. Redundancy indicators involve territorial coverage actually tested, the degree of technological independence among the available channels, and demonstrated capacity to function under conditions of partial infrastructure failure. Message quality indicators can be measured through comprehension rates assessed by survey, the level of actionability perceived by recipients, and the level of consistency across different channels used simultaneously.

Community participation indicators can be observed through the effective, active presence of organized community groups, the regular holding of simulation exercises with public participation, and the documented inclusion of vulnerable groups in system planning. Institutional learning indicators involve the systematic conduct of post-event audits, the actual implementation rate of the recommendations produced by those audits, and the frequency with which municipal plans are formally updated in light of accumulated experience. It is important to stress that these indicators should primarily support the continuous improvement of the system, not merely serve to produce comparative rankings among municipalities without considering relevant contextual differences. Comparisons between different municipalities must necessarily take into account differences in territory, available resources, and the specific risk profile faced by each locality.

Practical implementation of the architecture can begin in a focused way, prioritizing the threats of greatest local relevance rather than seeking simultaneous coverage of every possible risk. Municipalities subject to recurring flooding can start by mapping river basins, viable evacuation routes, and already-known exposed communities; cities with significant technological risks, such as proximity to hazardous industrial facilities, can prioritize integration with the companies responsible and with specialized health services. The architecture's conceptual structure remains common across different contexts, but the concrete application protocols must necessarily reflect the particularities of each territory. Excessive standardization of protocols, without adaptation to the local context, can ignore differences that actually determine the success or failure of the response in each specific case.

Simulation exercises are a central, irreplaceable instrument of this governance architecture. They allow the full decision chain, message formulation, the actual functioning of available channels, and the real reaction of the community to be tested under controlled conditions, without needing to wait for an actual disaster to discover flaws in the system. Well-designed simulations should deliberately include scenarios of power failure, temporary unavailability of mobile networks, and the unexpected absence of key decision-makers, thereby testing the system's robustness under adverse conditions and not merely its ideal functioning. The evaluation of each exercise needs to carefully record the times observed and the decisions actually made at each stage, ultimately producing a concrete correction plan with named officials and set deadlines, replicating the same institutional learning logic discussed in section 4.6.

FINAL CONSIDERATIONS

This article proposed a theoretical architecture for emergency communication governance in smart cities, built from the articulation of multilevel governance, crisis and risk communication theories, behavioral models of warning response, studies on smart cities and urban resilience, and the consolidated literature on early warning systems. The proposed model brings together six interdependent dimensions: clearly defined institutional authority, operational and technological interoperability, redundancy between digital and analog channels, accessible and actionable messages, effective community participation, and continuous institutional learning. The analysis carried out throughout the article consistently shows that communication resilience always depends on the combination of available technological infrastructure and the state's coordination capacity, and not on either of these factors considered in isolation.

The central contribution of this work is to deliberately shift the public and academic debate from the amount of technology available to the quality of governance actually practiced. Environmental sensors, integrated platforms, and analytical intelligence resources can certainly play a significant supporting role in protecting the population, but they do not replace clear protocols, tested interorganizational coordination, and public trust built over time. Genuinely resilient municipalities are those able to maintain useful, reliable communication even when significant parts of their technological infrastructure fail, precisely because their resilience does not depend on a single component, but on a deliberately redundant, well-coordinated system.

The proposed architecture also shows, in a way that deserves emphasis, that communication inclusion is not a peripheral or optional dimension of the system. A system that quickly reaches most of the population but systematically excludes groups already facing greater exposure to risk cannot reasonably be considered effective, regardless of its overall technical sophistication. Accessibility should guide the system's design from its initial conception, and community participation should be an organic part of municipal planning, not treated as a complementary step added at the end of the technological development process.

As a main limitation, it is important to acknowledge that the model presented here is theoretical in nature and requires subsequent empirical validation to confirm its practical applicability in different Brazilian municipal contexts. Future studies could apply this architecture in municipalities of different population sizes and administrative capacities, compare levels of institutional maturity among them, and retrospectively analyze real emergency events in light of the six proposed dimensions. Subsequent research could also develop more precise measurement scales for each dimension, systematically examine the actual costs of implementation in different contexts, and empirically investigate the relationship between prior institutional trust, effective understanding of the message received, and the population's actual response behavior during real emergencies.

For municipal public management, the most direct practical implication of this work is as follows: emergency communication should be treated as a permanent public policy, with its own budget, clearly assigned responsibilities, regular testing, and systematic evaluation of results, rather than as an episodic response mobilized only after a disaster has occurred. Institutional preparation deliberately built during periods of administrative normalcy ultimately determines the municipality's real capacity to adequately inform and effectively protect its population at the moment a crisis finally occurs.

REFERENCES

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

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

AUTHOR CONTRIBUTION

Moisés Figueiredo da Silva: conceptualization, methodology, investigation, formal analysis, writing of the original manuscript, review and editing, and supervision. Data curation and funding acquisition do not apply to this theoretical study.

EDITORIAL DECLARATIONS

Funding: the study received no external funding.

Conflict of interest: the author declares no conflict of interest.

Use of artificial intelligence: not declared by the author.