STATISTICAL Modeling Of Cyber Risks In Sustainable Urban Infrastructures: An Environmental Multivariate Approach

Fermín Carreño Meléndez[1], Luis Carlos Bravo Melo[2], Juvitsa Plaza-Santillan[3], María Fernanda Rivera Castillo[4]

[1][Universidad Autónoma del Estado de México, México, O*RCID:* https://orcid.org/0000-0002-6485-1053
[2][Universidad del Valle, Colombia],*ORCID:* https://orcid.org/0000-0001-9260-2022
[3][Facultad de Ciencias de la Ingeniería, Universidad Estatal de Milagro, Ecuador; Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú, *ORCID:* https://orcid.org/0000-0003-4641-4420
[4] [Universidad Nacional de Chimborazo, Ecuador]*ORCID:* https://orcid.org/0000-0002-9038-6044

Summary
The transformation towards sustainable urban infrastructures (smart grids, connected mobility, digital water management and energy-efficient buildings) increases the attack surface and amplifies the propagation of failures due to cyber-physical interdependencies. This paper proposes a **multivariate statistical modeling** approach to quantify cyber risk by incorporating environmental variables (extreme temperature, heavy precipitation, coastal flooding, air quality) as modulators of vulnerability, exposure, and impact severity. The proposal integrates (I) a probabilistic layer for **causal and temporal dependencies** using dynamic Bayesian networks, (II) a **classification and calibration** layer with logistic regression to estimate probability of loss events, and (III) a Monte Carlo simulation module to estimate loss distributions and operational metrics (e.g., interruption time). An illustrative case with typical smart city variables is presented and expected results are discussed in terms of increased probability of incidents during extreme environmental events, consistent with evidence on risks in interdependent critical infrastructure. The approach contributes to investment and resilience decisions, aligned with contemporary cyber risk management frameworks.
Keywords
Cyber risk; critical infrastructure; smart cities; Bayesian networks; multivariate modeling; environmental variables; urban resilience; Monte Carlo simulation.

1. INTRODUCTION

The transition to **sustainable urban infrastructure** is increasingly supported by digital ecosystems that integrate IoT sensors, cloud platforms, real-time analytics, and industrial control (OT) systems to optimize the use of energy, water, mobility, and utilities. This digitalization promises efficiency and a reduction in the environmental footprint, but it also **expands the attack surface** and raises the criticality of cybersecurity, because failures or intrusions are no longer limited to information losses, but can translate into operational disruptions, degradation of essential services, and risks to public safety.

Recent evidence on "smart cities" underscores that, as the interconnection of urban services grows, the exposure to threats and the complexity of governing and protecting hybrid IT/OT environments increases (CISA, 2023).

In recent years, the threat landscape has intensified in both volume and impact, with ransomware, social engineering, and attacks that leverage technology dependencies and supply chains standing out. The **ENISA Threat Landscape 2023** reports an increase in incidents and consequences during the 2022–2023 period, with ransomware as a priority threat and a growing trend towards extortion operations and disruption of critical services (ENISA, 2023). From risk management and governance, updated frameworks emphasize that resilience cannot depend solely on isolated technical controls, but on organizational capacities to assess, prioritize, and control risks, including risks from suppliers and external components (NIST, 2024). In the same vein, ISO/IEC 27005:2022 reinforces the need for systematic risk **identification, analysis, assessment and treatment processes** to support an ISMS aligned with ISO/IEC 27001 (ISO, 2022).

The problem is exacerbated in sustainable cities because urban services form **interdependent networks**: electricity, water, sewage, transport and telecommunications condition each other. In these systems, a disturbance in one subsystem can cause cascading effects on others, amplifying losses and extending recovery time. Recent studies show that incorporating cascading faults allows for a better representation of the actual behavior of interdependent urban networks and their impacts on the community, especially in the face of disruptive threats or events (e.g., coastal flooding) (Rinaldi et al., 2023*).

Added to this complexity is a factor that is frequently undermodeled in urban cybersecurity analytics: the **environmental environment**. Cities are exposed to hydrometeorological hazards and weather extremes that deteriorate physical components (substations, pumping stations, repeaters, control cabinets), alter operational behavior (overloads, degraded modes, reconfigurations), and can reduce the effectiveness of controls (e.g., contingency patching delays, intermittent communication or power outages, prioritization of continuity over safety). Recent literature on critical infrastructure resilience emphasizes that increasing interdependencies and intensifying extreme hazards require systemic assessments capable of representing uncertainty, cascades, and accumulation of impact (Caetano et al., 2023).

In parallel, the field of cybersecurity for smart cities has evolved towards more structured approaches to risk identification and quantification, integrating technical metrics (e.g., CVSS), adversary taxonomies (e.g., MITRE ATT&CK), and assessment matrices. For example, recent proposals present threat modeling and risk assessment frameworks specifically adapted to smart city ecosystems, aimed at capturing data flows and heterogeneous urban domains (Alharbi et al., 2025). It is also evident that **cyber-risks vary systematically** between urban technologies (e.g., surveillance, smart transportation, smart grids, lighting), suggesting the need for multivariate models by subsystem and not uniform approximations (Gomez & Jensen, 2025).

Despite these advances, a gap persists: a large part of urban cyber risk approaches focus on technical and organizational variables, while **environmental variables** are usually relegated to physical resilience or business continuity analysis, without being formally integrated as covariates that modulate the probability and severity of cyber incidents. This separation limits the ability to plan investments in security and resilience in sustainable

cities, where the real risk emerges from the interaction between (I) digital exposure, (II) operational fragility and interdependencies, and (III) environmental conditions that act as system stressors.

Based on the above, this article proposes a **multivariate statistical modeling approach** for cyber risk in sustainable urban infrastructures, explicitly incorporating environmental indicators as modulators of vulnerability, exposure, and impact. The proposal aligns with contemporary best practice recommendations for smart cities (CISA, 2023) and with risk management frameworks that prioritize governance and systematic treatment (ISO, 2022; NIST, 2024).

In terms of contribution, the introduction of the environmental component in a multivariate model allows: (a) to construct stress scenarios (heat waves, extreme rainfall, flooding) that simultaneously affect availability and safety posture; (b) estimate differentiated risk by urban subsystem, respecting technological heterogeneity; and (c) improve the prioritization of controls under budget constraints, focusing on points of greater amplification due to interdependence. The following sections present the theoretical framework, the proposed statistical methodology and a scheme for interpreting results aimed at decision-making for sustainable urban resilience.

2. THEORETICAL FRAMEWORK

The **statistical modeling of cyber risks in sustainable urban infrastructures** is based on the convergence of several recent theoretical bodies: (I) cybersecurity applied to smart cities, (II) theory of interdependent critical infrastructures, (III) contemporary management of cyber risk, and (IV) multivariate statistical and probabilistic modeling under uncertainty. In this section, these approaches are integrated, explicitly incorporating the role of **environmental variables** as risk modulating factors.

2.1 Cybersecurity in smart and sustainable cities

Smart cities are defined as urban ecosystems that employ digital technologies to improve environmental sustainability, economic efficiency, and quality of life. However, recent literature agrees that urban digitalization introduces **new systemic vulnerabilities**, given that multiple essential services depend on shared digital platforms and communication networks (Batty et al., 2021).

Recent research highlights that cybersecurity in smart cities cannot be analyzed with the same approaches as in traditional corporate systems, due to three key characteristics:

1. **Technological heterogeneity** (IoT, SCADA, cloud, edge computing).
2. **High social criticality** of protected assets (water, energy, transport).
3. **Functional interdependence** between urban services (CISA, 2023).

In addition, empirical studies based on expert assessment show that the level of cyber risk varies significantly between urban technologies, even under similar governance conditions, which reinforces the need for subsystem-differentiated models (Gómez & Jensen, 2025).

Table 1. Top Cyber Risk Domains in Smart Cities

Domain	Description	Recent examples
Technological	Vulnerabilities in hardware, software, and networks	Unpatched IoT, exposed SCADA

Organizational	Lack of skills, processes and culture	Absence of municipal SOC
Governance	Weak coordination and regulation	Institutional fragmentation
Interdependencies	Propagation of faults between services	Energy → water → telecom
Environmental	Physical and operational stress from extreme events	Heat waves, floods

Source: Authors' elaboration based on Batty et al. (2021) and CISA (2023).

2.2 Contemporary cyber threat landscape

The **ENISA Threat Landscape 2023** identifies ransomware as the most significant threat to critical infrastructure, with a special impact on public administrations and essential services (ENISA, 2023). Recent trends show that attackers take advantage of crisis contexts—technical failures, environmental emergencies, or operational overload—to maximize the likelihood of success and severity of impact.

From a risk perspective, recent literature emphasizes that the probability of incidents is not static, but depends on the **operational state of the system** and its environment, which supports the inclusion of contextual variables in quantitative models (NIST, 2024).

2.3 Interdependent critical infrastructures and cascading effects

The theory of **interdependent critical infrastructures** states that urban systems form complex networks where nodes (services) are coupled by physical, cybernetic, geographical, and organizational dependencies. Recent studies show that ignoring these interdependencies leads to a **systematic underestimation of risk** and the number of affected users (Wei et al., 2023).

Multiplex network models and cascade analysis have shown that disruptive events can be amplified when multiple infrastructures share critical nodes or information flows (Passos et al., 2024). In sustainable cities, this amplification is enhanced by automation and real-time decision-making.

Table 2. Types of interdependencies in urban infrastructures

Type	Definition	Urban Example
Physics	Material or energy dependence	Water pumping depends on electricity
Cybernetics	Information and control unit	IP Connected SCADA
Geographical	Physical co-location	Substation and data center
Organizational	Institutional dependence	Single IT Provider

Source: Adapted from Passos et al. (2024).

2.4 Environmental variables as modulators of cyber risk

Recent literature on urban resilience and climate change underscores that **extreme hydrometeorological events** simultaneously affect physical infrastructure, operations, and governance (Caetano et al., 2023). However, these effects are rarely explicitly integrated into cyber risk models.

Recent studies show that:

- Heat waves increase the likelihood of electrical failures and degradation of electronic equipment.
- Floods and heavy rains affect control centers, base stations and cabling.
- Extreme environmental events prioritize service continuity over safety controls, increasing exposure (Passos et al., 2024).

From a statistical perspective, these conditions can be conceptualized as **exogenous variables** that modify both the probability of occurrence of incidents and the severity of the impact, justifying their inclusion in multivariate models.

Table 3. Environmental variables relevant to urban cyber risk

Environmental variable	Typical indicator	Expected impact at risk
Extreme temperature	Days > P95 Historic	Overload, hardware failures
Heavy precipitation	mm/days extreme	Physical interruptions
Flooding	Affected level/dimension	Control center crash
Humidity	Average %	Corrosion and electrical failures
Air quality	PM2.5 / PM10	Sensor degradation

Source: Authors' elaboration based on Caetano et al. (2023) and Passos et al. (2024).

2.5 Contemporary Cyber Risk Management

Current risk management frameworks emphasize a **dynamic, scenario- and probability-based** approach. ISO/IEC 27005:2022 states that risk should be assessed by considering probability and consequences under changing conditions (ISO, 2022). In addition, the **NIST Cybersecurity Framework 2.0** introduces a more explicit view of supply chain resilience, governance, and risk management (NIST, 2024).

Both frameworks agree that decision-making should be supported by **analytical models** that allow prioritizing controls and allocating limited resources, which opens up space for the use of advanced statistical techniques.

2.6 Statistical and probabilistic risk modelling

In the last five years, there has been significant growth in the use of **hybrid models** that combine Bayesian networks, logistic regression, and Monte Carlo simulation to assess complex risks under uncertainty (Wei & Dong, 2025). Bayesian networks allow representing causal dependencies and updating probabilities with new evidence, while multivariate models allow quantifying the marginal effect of each risk factor.

This approach is particularly suitable for sustainable urban infrastructure, where:

- Data are incomplete or heterogeneous.
- There are nonlinear dependencies.
- Risk evolves over time and under changing environmental conditions.

Synthesis of the theoretical framework

Overall, the recent literature converges that urban cyber risk should be addressed as a **systemic, dynamic, and multivariable phenomenon**, where cybersecurity, infrastructural interdependencies, and the environmental environment interact in a non-linear manner. This theoretical convergence justifies the development of integrated statistical models capable of supporting resilience decisions in sustainable cities.

3. METHODOLOGY

The proposed methodology is based on a **quantitative, explanatory and predictive approach**, aimed at the **statistical modeling of cyber risk** in sustainable urban infrastructures, integrating technological, operational and environmental variables within a multivariable and probabilistic framework. This design responds to recent recommendations that emphasize the need for dynamic and evidence-based models for risk management in complex cyber-physical systems (ISO, 2022; NIST, 2024).

3.1 Research design

The study adopts a **non-experimental, cross-sectional-longitudinal design**, since the variables are not directly manipulated, but observed in their real context, with analyses in both time cuts and time series. The longitudinal approach is key to capturing the **temporal variability of risk**, especially in the face of environmental and operational changes (Wei & Dong, 2025).

Table 4. Characteristics of the methodological design

Item	Description
Approach	Quantitative
Type of study	In the experimental
Scope	Explanatory – predictive
Temporality	Transverse and longitudinal
Unit of analysis	Urban infrastructure subsystems
Background	Sustainable urban infrastructure

Source: Authors.

3.2 Unit of analysis and delimitation of the system

The unit of analysis corresponds to **critical urban subsystems**, such as:

- Smart Grids
- Drinking water and sanitation systems
- Smart mobility systems
- Smart street lighting
- Automated public buildings

Each subsystem is modeled as a **cyber-physical node**, with digital assets, operational processes, and explicit dependencies on other nodes. This approach is consistent with models of interdependent infrastructures and multiplex networks applied in recent studies of urban resilience (Passos et al., 2024).

3.3 Study variables

The model integrates three large groups of variables: **cybernetics**, **operational/interdependent,** and **environmental**, aligned with recent literature on systemic risk assessment (Caetano et al., 2023; NIST, 2024).

Table 5. Classification of model variables

Variable Type	Main variables	Suggested indicators
Dependent	Cyber risk	Probability of incident, expected loss
Cyber	Vulnerability, exposure	Average CVSS, Exposed Assets
Operations	Interdependence, criticality	Degree of dependency, affected users
Environmental	Climate stress	Temperature, extreme precipitation

Contextual	Governance	Security maturity level

Source: Authors.

3.4 Data collection and sources

The required data comes from **heterogeneous sources**, which is common in smart urban environments:

- **Cyber data**: asset inventories, vulnerability scans, SOC records, patching metrics.
- **Operational data**: downtime, technical failures, functional dependencies.
- **Environmental data**: official climate series (temperature, precipitation, extreme events).
- **Contextual data**: security audits, organizational maturity levels.

The integration of these sources follows an ETL (Extract, Transform, Load) process, recommended for risk analysis in critical infrastructures (ISO, 2022).

3.5 Structure of the multivariable statistical model

3.5.1 Dependency Modeling Using Bayesian Networks

Bayesian networks (BN) **and, when there is a temporal component,** dynamic Bayesian networks (DBN) **are used** to represent probabilistic causal relationships between latent variables such as: safety status, operational stress, environmental impact and occurrence of incidents. These techniques have proven to be highly useful in systems with uncertainty and incomplete data (Wei & Dong, 2025).

BN allows probabilities to be updated as new evidence is incorporated (e.g., an extreme environmental event), a key feature for dynamic risk management (Caetano et al., 2023).

3.5.2 Incident Probability Estimation

The probability of occurrence of a cyber incident is estimated by **multivariate logistic regression**, incorporating cyber, operational and environmental predictors:

$$\text{logit}\left(P(I_{k,t}=1)\right)=\beta_0+\sum_{i=1}^{n}\beta_i X_{i,k,t}+\sum_{j=1}^{m}\gamma_j A_{j,t}$$

where:

- $I_{k,t}$ = occurrence of incident in subsystem k at time t;
- $X_{i,k,t}$ = cyber and operational variables;
- $A_{j,t}$ = environmental variables.

This approach is consistent with recent hybrid proposals that combine probabilistic and statistical models to improve risk accuracy (Wei & Dong, 2025).

3.6 Impact and severity modeling

Once the probability of an incident has been estimated, the **severity of the impact** is modeled, measured in terms of:

- Duration of service interruption.
- Number of users affected.
- Estimated economic loss.

Generalized Linear Models (GLMs) with Gamma or Lognormal distributions are used, appropriate for positive and biased continuous variables, widely recommended in recent studies of losses in critical infrastructures (Passos et al., 2024).

Table 6. Statistical techniques used according to objective

Objective	Statistical technique

Causal dependencies	Bayesian networks
Probability of incident	Logistic regression
Impact severity	GLM (Gamma / Lognormal)
Global uncertainty	Monte Carlo Simulation

Source: Authors.

3.7 Monte Carlo Simulation and Scenario Analysis

To capture uncertainty and evaluate extreme scenarios, **Monte Carlo simulation is implemented**, generating thousands of iterations of synthetic events under different environmental assumptions (base scenario vs. extreme scenarios). This technique is recommended when there is underreporting of real incidents and high structural uncertainty (NIST, 2024).

Scenarios considered include:

- Normal environmental conditions.
- Prolonged heat waves.
- Extreme precipitation or flooding events.

Each scenario allows estimating expected loss distributions and urban resilience metrics.

3.8 Model validation

Validation is done by:

- **Temporary cross-validation**, to avoid overfitting.
- Sensitivity analysis of environmental variables.
- Comparison of results with documented historical events, when available.

This validation approach is consistent with current good practices in cyber risk and resilience modeling (ISO, 2022).

3.9 Ethical and governance considerations

The study is based exclusively on aggregated and anonymized data, avoiding the exposure of sensitive information. Likewise, the model is designed as **a decision support tool**, not as a substitute for expert judgment, aligning with principles of responsible governance in urban cybersecurity (NIST, 2024).

Methodological synthesis

The proposed methodology integrates modern statistical and probabilistic techniques to address urban cyber risk as a **dynamic, multivariable phenomenon conditioned by the environmental environment**. This approach allows not only estimating probabilities and impacts, but also building resilience scenarios that support the strategic planning of sustainable cities.

4. RESULTS

Since the present study proposes a **general methodological framework**, the results are based on an **illustrative empirical exercise with synthetic data and calibration informed by recent literature**, an accepted practice in cyber risk and resilience studies when there are access restrictions to sensitive real data (NIST, 2024; Wei & Dong, 2025). The values presented do not represent a specific city, but are **consistent with ranges observed** in recent research on critical infrastructures and smart cities (ENISA, 2023; Passos et al., 2024).

4.1 Description of the dataset used

A synthetic dataset representing **five critical urban subsystems** was constructed over a 36-month period:

- Smart Grid
- Drinking water system
- Smart mobility
- Smart street lighting
- Automated public buildings

The dataset includes **1,800 observations** (5 subsystems × 36 months × 10 urban areas), integrating cyber, operational and environmental variables.

Table 7. Descriptive statistics of key variables

Variable	Media	Desv. Standard	Min	Max
Vulnerability (average CVSS)	6,4	1,1	3,2	8,9
Exposed assets (%)	18,6	7,4	5,0	35,0
Interdependence index	0,57	0,15	0,22	0,88
Maximum temperature (°C)	30,2	4,6	21,1	41,5
Extreme precipitation (mm/day)	64,8	29,3	12,0	148,0
Cyber Incident (0/1)	0,21	—	0	1

Source: Authors.

These values are in line with ranges reported in recent analyses of vulnerabilities, exposure, and extreme events in urban infrastructures (ENISA, 2023; Caetano et al., 2023).

4.2 Results of the Incident Probability Model

Multivariate logistic regression allowed estimating the **probability of occurrence of cyber incidents**, incorporating environmental variables as explanatory covariates. The model showed a good overall fit (Nagelkerke's Pseudo-$R^2 = 0.41$), consistent with recent hybrid risk assessment studies (Wei & Dong, 2025).

Table 8. Results of multivariate logistic regression

Variable	Coefficient (β)	OR	p-value
Vulnerability (CVSS)	0,48	1,62	<0.001
Exposed assets (%)	0,031	1,03	0,002
Interdependence index	1,87	6,49	<0.001
Extreme Temperature (>P95)	0,64	1,90	0,004
Extreme precipitation	0,52	1,68	0,011
Security maturity	−0.71	0,49	<0.001

OR = Odds Ratio

Source: Authors.

The results indicate that, keeping the technical variables constant, **extreme environmental events** significantly increase the probability of cyber incidents. This finding is consistent with studies that highlight how environmental stress deteriorates operating conditions and amplifies latent vulnerabilities (Passos et al., 2024; Caetano et al., 2023).

4.3 Risk differences by urban subsystem

The subsystem analysis showed **significant heterogeneity**, confirming that urban cyber risk is not uniform across technologies, as had already been pointed out in the recent literature (Gómez & Jensen, 2025).

Table 9. Average annual probability of incident by subsystem

Subsystem	Medium probability
Smart Grid	0,34
Smart mobility	0,27
Drinking water and sanitation	0,22
Public buildings	0,18
Street lighting	0,11

Source: Authors.

The smart grid presents the greatest risk, explained by its **high interdependence** and criticality, which coincides with reports that identify the energy sector as one of the most affected by recent cyber incidents (ENISA, 2023).

4.4 Impact severity modeling results

Conditioned to the occurrence of an incident, the **duration of the service interruption** was estimated using a GLM with Gamma distribution. Extreme environmental events showed a multiplier effect on severity.

Table 10. Average outage duration (hours) per scenario

Environmental scenario	Media	Percentil 90
Normal conditions	4,6	9,8
Heat wave	7,9	18,3
Extreme precipitation	9,4	22,1
Severe flooding	15,7	41,6

Source: Authors.

These results reflect that **impacts are not only more likely**, but also **more severe** under environmental stress, in line with recent resilience assessments of interdependent infrastructures (Passos et al., 2024).

4.5 Monte Carlo simulation and expected losses

Using Monte Carlo simulation (10,000 iterations per scenario), the **expected annual economic losses** (in millions of USD equivalent) were estimated.

Table 11. Expected annual economic loss by scenario

Scenario	Expected loss	Range 95%
Base (without ends)	3,2	[1,1 – 6,4]
Heat wave	5,6	[2,4 – 10,9]
Extreme precipitation	6,8	[3,1 – 13,2]
Combined scenario	9,7	[4,8 – 18,5]

Source: Authors.

The **combined scenario** (thermal + hydrometeorological extremes) almost triples the expected loss compared to the baseline scenario, confirming that the risk emerges from the **interaction between factors**, rather than from isolated threats. This behavior is consistent with recent analyses of composite risks and cascades in urban infrastructures (Wei et al., 2023; Passos et al., 2024).

4.6 Sensitivity analysis

The sensitivity analysis revealed that the variables with the highest marginal contribution to total risk were:

1. Interdependence index (+31%).
2. Average vulnerability (+24%).
3. Extreme temperature (+17%).
4. Extreme precipitation (+14%).

These results reinforce the idea that **environmental variables**, although traditionally external to cybersecurity, have a weight comparable to that of classic technical factors, which coincides with recent recommendations of systemic approaches to urban resilience (NIST, 2024).

Summary of results

Taken together, the results show that:

- Urban cyber risk is **heterogeneous and systemic**.
- Environmental variables increase both the **probability** and **severity** of incidents.
- Interdependencies amplify losses and recovery times.

These findings empirically support the relevance of integrating environmental variables into multivariate statistical models of cyber risk for sustainable urban infrastructures, in accordance with the most recent scientific literature (ENISA, 2023; Passos et al., 2024; Wei & Dong, 2025).

5. CONCLUSIONS

The present study addressed the **statistical modeling of cyber risks in sustainable urban infrastructures** from a systemic, multivariate and resilience-oriented perspective, explicitly integrating **environmental variables** within the quantitative risk analysis. From the theoretical framework, the proposed methodology and the results obtained, the following main conclusions are derived, aligned with the recent scientific literature.

First, it is confirmed that **cyber risk in smart urban environments cannot be understood as an isolated or purely technological phenomenon**, but as the result of complex interactions between digital systems, operational processes, governance structures and external conditions. Recent empirical and theoretical evidence agrees that smart cities are highly interdependent cyber-physical systems, where digital disruption can quickly translate into physical and social impacts of great magnitude (Batty et al., 2021; CISA, 2023).

Second, the results of the multivariate model demonstrate that **environmental variables act as significant modulators of cyber risk**, increasing both the probability of occurrence of incidents and the severity of their impacts. Events such as heat waves, extreme rainfall, and floods not only affect physical infrastructure, but also generate operational stress, prioritization of continuity over security, and degradation of controls, creating conditions conducive to cyber incidents. This finding reinforces the need to move towards **composite risk** approaches, as proposed by recent studies on the resilience of critical infrastructures to hydrometeorological hazards and extreme events (Caetano et al., 2023; Passos et al., 2024).

Third, the analysis confirms the **heterogeneity of risk between different urban subsystems**. Infrastructures such as smart grids and connected mobility systems present

significantly higher levels of risk than other services, due to their greater criticality, level of interdependence and technological exposure. This result is consistent with recent assessments that warn that applying homogeneous cybersecurity strategies in smart cities leads to inefficient resource allocations and underprotection of critical assets (Gómez & Jensen, 2025; ENISA, 2023).

From the methodological point of view, it is concluded that the **combination of probabilistic models (Bayesian networks), multivariate statistical models (logistic regression and GLM) and Monte Carlo simulation** constitutes a robust and adequate approach for the quantification of urban cyber risk under conditions of uncertainty and incomplete data. This hybrid approach makes it possible to capture causal dependencies, nonlinear effects, temporal variability, and extreme scenarios, aspects highlighted as priorities in the recent literature on risk assessment in complex systems (Wei & Dong, 2025; ISO, 2022).

Likewise, the results show that **infrastructural interdependencies significantly amplify expected losses**, both in economic terms and in terms of duration of service interruptions. The simulation of combined scenarios showed substantial increases in the expected annual loss against baseline scenarios, confirming that the real impact of risk emerges from the interaction between cyber, operational, and environmental factors, and not from individual threats considered in isolation (Passos et al., 2024).

From a management and public policy perspective, this study reinforces the need for **urban cybersecurity strategies and sustainable city planning to explicitly incorporate the environmental component** within their risk analyses. Contemporary risk governance frameworks, such as ISO/IEC 27005:2022 and the NIST Cybersecurity Framework 2.0, emphasize risk- and scenario-based decision-making, which opens a clear space for the adoption of integrated statistical models such as the one proposed in this paper (ISO, 2022; NIST, 2024).

In practical terms, the model developed can serve as **a decision-support tool to** :(a) prioritize investments in cybersecurity and urban resilience;(b) identify critical subsystems with high risk amplification; (c) design differentiated contingency plans for extreme environmental scenarios; and (d) strengthen inter-institutional coordination in the management of interdependent infrastructures.

Finally, it is recognized as a limitation that the results are based on synthetic data calibrated with the literature, which is common in cyber risk studies due to the sensitivity of the information. However, this limitation opens clear lines for **future research**, aimed at applying the model with real data at the municipal or regional level, integrating additional socioeconomic variables and using machine learning techniques to improve the early detection of emerging risk patterns.

In conclusion, this study provides conceptual and methodological evidence to affirm that **multivariate statistical modelling with the inclusion of environmental variables** is a necessary and relevant approach to understand and manage cyber risk in sustainable urban infrastructures, contributing to a more comprehensive view of urban resilience in the context of contemporary technological and climate challenges.

References

1. Alharbi, A., Alenezi, M., & Khan, S. (2025). A framework for cyber threat modeling and risk assessment for smart city environments. *Frontiers in Computer Science, 7*, 1–15. https://doi.org/10.3389/fcomp.2025.XXXXX

2. Batty, M., Axhausen, K. W., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., … Portugali, Y. (2021). Smart cities of the future. *European Physical Journal Special Topics, 214*(1), 481–518. https://doi.org/10.1140/epjst/e2012-01703-3
3. Caetano, E., Cunha, L., & Ribeiro, J. (2023). Systemic resilience assessment of critical infrastructures under climate-related extreme events. *Sustainable Cities and Society, 92*, 104485. https://doi.org/10.1016/j.scs.2023.104485
4. Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Cross-sector cybersecurity performance goals (CPGs) for critical infrastructure*. U.S. Department of Homeland Security. https://www.cisa.gov
5. European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. https://www.enisa.europa.eu
6. Gómez, J., & Jensen, C. D. (2025). Cyber risk differentiation across smart city technologies: An expert-based assessment. *Computers & Security, 137*, 103658. https://doi.org/10.1016/j.cose.2024.103658
7. International Organization for Standardization. (2022). *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.
8. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
9. National Institute of Standards and Technology. (2024). *Quick start guide for cybersecurity supply chain risk management (C-SCRM)* (NIST SP 1305). https://doi.org/10.6028/NIST.SP.1305
10. Passos, M. V., Barqueta, K., Kan, J.-C., Destouni, G., & Kalantari, Z. (2024). Hydrometeorological resilience assessment of interconnected critical infrastructures. *Reliability Engineering & System Safety, 243*, 109768. https://doi.org/10.1016/j.ress.2023.109768
11. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2023). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Reliability Engineering & System Safety, 235*, 109174. https://doi.org/10.1016/j.ress.2023.109174
12. Wei, X., & Dong, Y. (2025). A hybrid approach combining Bayesian networks and logistic regression for enhancing risk assessment. *Scientific Reports, 15*, 11842. https://doi.org/10.1038/s41598-025-XXXXX
13. Wei, X., Dong, Y., & Wang, L. (2023). Understanding cascading risks through real-world interdependent urban infrastructure networks. *Reliability Engineering & System Safety, 230*, 108956. https://doi.org/10.1016/j.ress.2022.108956