University of New Mexico

AHP-TOPSIS-Based Cybersecurity Control Prioritization for Local E-Government: Integrating COBIT 2019 and ISO/IEC 27001:2022 in Ecuador

Gabriel Neptalí Bailón Arcentales, Jair Andrés Semblantes Pinto, and Noel Batista Hernández

Universidad Bolivariana del Ecuador (UBE), Guayaquil, Ecuador

gnbailona@ube.edu.ec; jasemblantesp@ube.edu.ec; nbatistah@ube.edu.ec

Abstract—Local governments in Ecuador manage critical citizen services yet operate with limited cybersecurity maturity. This paper presents MPEC-GAD, a cybersecurity governance model integrating COBIT 2019 strategic alignment with ISO/IEC 27001:2022 technical controls, using AHP-TOPSIS multi-criteria prioritization. Applied to GAD Jaramijó (Manabí, Ecuador), the model uses a reported baseline MIL of 1.0 and treats 2.8 within 36 months as a planning target, not an observed outcome (+1.8 points). The four decision criteria weight risk reduction at 48.24%, implementation cost at 27.18%, deployment time at 15.75%, and technical complexity at 8.83% (AHP Consistency Ratio CR = 0.0054 < 0.10). The TOPSIS ranking directs scarce resources toward the 47 mandatory EGSI controls with highest risk-reduction per investment unit. The model addresses LOPDP compliance requirements (up to 3% revenue penalties) and aligns with Ecuador's EGSI v3.0. A single-round structured review by seven experts rated pertinence, viability and completeness with mean scores ≥4.0/5.0.

Index Terms—cybersecurity governance, AHP-TOPSIS, COBIT 2019, ISO 27001, local e-government, MCDM, EGSI Ecuador

1. Introduction

Local governments worldwide face escalating cybersecurity threats. According to Sophos [1], ransomware attacks against government entities increased from 58% to 69% between 2022 and 2023, with average recovery costs exceeding USD 2.8 million per incident. Kaspersky [2] reported 1.15 million ransomware attempts targeting Latin American organizations in 2023 alone, with municipalities and sub-national entities disproportionately represented among victims. In Ecuador, the Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) exposes institutions to penalties of up to 3% of annual revenues for data breaches, increasing the financial risk of inaction.

GAD Jaramijó, a cantonal local government in Manabí province, serves approximately 20,000 inhabitants and administers an annual budget of ~USD 8 million. It is representative of the other small Ecuadorian cantonal GADs that operate with fewer than 5 full-time IT staff and no dedicated cybersecurity function [3]. Critical digital services—including property tax collection (4,500 monthly transactions) and the cadastral registry (10,050 parcels)—operate on legacy infrastructure without formal risk management.

Despite the existence of COBIT 2019 for governance alignment [4] and ISO/IEC 27001:2022 for technical controls [5], no published model articulates how small Latin American municipalities can jointly operationalize both frameworks under real resource constraints. Ecuador's mandatory EGSI v3.0 [6] defines 47 mandatory controls for revenue systems but provides no prioritization guidance, leaving GAD administrators without a decision basis for investment sequencing.

This paper addresses that gap through MPEC-GAD, a three-layer cybersecurity governance model that (1) aligns COBIT 2019 governance objectives with institutional strategy; (2) applies AHP-TOPSIS multi-criteria prioritization to rank ISO 27001:2022 controls by risk-reduction per investment unit; and (3) provides a case-specific implementation roadmap. The main contributions are: (i) the MPEC-GAD framework integrating governance and technical layers; (ii) an empirical case study at GAD Jaramijó including AHP weight elicitation (CR = 0.0054) and TOPSIS ranking of 47 EGSI controls; and (iii) expert validation via a 7-member Delphi panel confirming pertinence, viability and completeness (mean ≥4.0/5.0).

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 presents the MPEC-GAD framework. Section 4 describes the GAD Jaramijó case study. Section 5 discusses results and transferability. Section 6 concludes.

2. Related Work

2.1. COBIT 2019 and ISO 27001 Integration

COBIT 2019 provides a governance and management framework organizing objectives into five domains: Evaluate, Direct and Monitor (EDM); Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). ISO/IEC 27001:2022 restructures the information security management system (ISMS) into 93 controls across 4 themes. Hendry et al. [7] formally characterized the complementarity: COBIT 2019 defines "what" governance objectives to pursue, while ISO/IEC 27001:2022 specifies "how" to implement corresponding security controls. Their Integrated Governance and Security Framework (IGSF) demonstrated that joint deployment reduces residual risk by 31% compared with either framework alone.

Schmidt et al. [8] studied COBIT-ISO integration in three European small municipalities and identified five critical success factors: top-management commitment, incremental scoping, budget-aware control selection, staff competency development, and continuous monitoring. Hossain et al. [9] conducted a systematic review of 84 cybersecurity maturity studies in local governments, finding that MCDM-based prioritization reduces average implementation timelines by 28% versus expert-judgment-only approaches.

2.2. AHP-TOPSIS in Cybersecurity

The Analytic Hierarchy Process (AHP), introduced by Saaty [10], provides a structured method for deriving priority weights from pairwise comparisons using a 1–9 scale. A Consistency Ratio CR < 0.10 validates that judgments are acceptably consistent. TOPSIS (Hwang & Yoon [11]) ranks alternatives by their Euclidean distance from the positive ideal solution (PIS) and negative ideal solution (NIS), selecting alternatives simultaneously closest to the PIS and farthest from the NIS.

Md Hanafiah et al. [12] applied AHP-TOPSIS to prioritize cybersecurity controls in port information systems, reporting that the combined method produces rankings 40% more stable under sensitivity analysis than pure AHP. Their finding that cost and risk-reduction criteria dominate rankings in resource-constrained contexts directly informed the criterion selection for MPEC-GAD. A TOPSIS framework has likewise been used to choose among machine-learning models using multiple performance criteria [21], reinforcing the method's role as a transparent selection layer rather than a domain-specific score.

2.3. Cybersecurity Maturity in Ecuador

López Loja et al. [13] developed a Maturity Implementation Level (MIL) model for Ecuadorian critical infrastructure, calibrated against C2M2 v2.1 and NIST CSF 2.0. Their five-level scale (1.0–5.0) has been validated against 14 public institutions and provides the baseline measurement instrument used in this study. Ecuador's EGSI v3.0 (MINTEL, 2024) [6] mandates 47 controls specifically for revenue-collection systems in public institutions, grouping them into five categories: access control, cryptography, incident management, business continuity, and supplier relationships. Non-compliance triggers LOPDP sanctions and SERCOP procurement restrictions [14].

3. MPEC-GAD Framework

3.1. Three-Layer Architecture

MPEC-GAD organizes cybersecurity governance into three integrated layers (Fig. 1). The —Strategic Layer—is governed by COBIT 2019 through a goal-cascade mechanism that maps enterprise objectives to governance and management objectives. For GAD Jaramijó, six COBIT objectives were activated: EDM01 (Governance Framework), APO12 (Risk Management), APO13 (Security Management), BAI06 (IT Changes), DSS05 (Security Services), and MEA02 (Internal Control). The —Tactical Layer—employs AHP for criterion weighting and TOPSIS for control ranking, interfaced with MAGERIT v3.0 threat catalogues to estimate residual risk reduction per control. The —Operative Layer—implements ISO/IEC 27001:2022 controls, ensuring alignment with EGSI v3.0 mandatory requirements and LOPDP compliance obligations.

3.2. AHP Criteria Weighting

Four criteria were defined through structured expert elicitation: C_1 Risk Reduction (RR) — percentage decrease in residual risk for critical assets; C_2 Implementation Cost (IC) — normalized investment including labor and licensing; C_3 Deployment Time (DT) — weeks required for full implementation; C_4 Technical Complexity (TC) — composite indicator of staff skill requirements and integration effort. Seven experts (mean experience 12.4 years in public-sector IT governance) completed pairwise comparison matrices via structured questionnaire.

TABLE 1. AHP PAIRWISE COMPARISON MATRIX AND CRITERIA WEIGHTS

Criterion	C_1 RR	C_2 IC	C_3 DT	C_4 TC	Weight (w_i)
C_1 Risk Reduction	1	2	3	5	0.4824

Criterion	C_1 RR	C_2 IC	C_3 DT	C_4 TC	Weight (w_i)
C_2 Implementation Cost	1/2	1	2	3	0.2718
C_3 Deployment Time	1/3	1/2	1	2	0.1575
C_4 Technical Complexity	1/5	1/3	1/2	1	0.0883
$\lambda_{max} = 4.0145$ | $IC = 0.0048$ | $IA = 0.90$ | $CR = 0.0054 < 0.10$					$\sum = 1.0000$

The AHP Consistency Index (CI) and Consistency Ratio (CR) are computed as follows:

$$CI = (\lambda max - n) / (n - 1) = (4.0145 - 4) / 3 = 0.0048 \quad (1)$$

$$CR = IC / RI = 0.0048 / 0.90 = 0.0054 < 0.10 \quad (2)$$

where λ_{max} is the principal eigenvalue of the comparison matrix, n = 4 is the number of criteria, and RI = 0.90 is the random consistency index for n = 4 (Saaty, 1980). CR = 0.0054 ≪ 0.10 confirms full consistency.

3.3. TOPSIS Ranking Procedure

Let D be the m × n decision matrix where rows represent controls and columns represent criteria. The TOPSIS procedure follows four steps: (1) normalize D to obtain $r_{ij} = d_{ij} / (\sum_i d_{ij}^2)^{½}$; (2) multiply by AHP weights to form $v_{ij} = w_j \cdot r_{ij}$; (3) identify PIS $A^+ = \{\max(v_{ij})\}$ and NIS $A^- = \{\min(v_{ij})\}$ for benefit criteria; (4) compute Euclidean distances D^+ and D^- to PIS and NIS; and (5) rank by closeness coefficient C_i^*:

$$C_i^* = D^- / (D^+ + D^-) \quad (3)$$

where $C_i^* \in [0, 1]$; higher values indicate controls closer to the ideal solution (maximum benefit per unit investment). Controls with $C_i^* \geq 0.70$ are classified as Priority 1 (immediate implementation within 6 months).

4. Case Study: GAD Jaramijó

4.1. Institutional Profile and Critical Systems

GAD Jaramijó is a Type-D cantonal government (population ~20,000; annual budget ~USD 8M) in Manabí province, Ecuador. The institution employs 142 civil servants, with 3 FTE in IT (0 dedicated to cybersecurity). Three critical digital systems were identified through the MAGERIT v3.0 asset inventory: (i) the Revenue Collection System (4,500 transactions/month; 72% of own-source revenues; MAGERIT risk score 8.7/10); (ii) the Cadastral Registry System (8,200 urban parcels + 1,850 rural parcels; risk score 7.3/10); and (iii) the Human Resources and Payroll System (142 employees; risk score 6.1/10). These three systems collectively handle personal data covered by LOPDP and are subject to all 47 EGSI v3.0 mandatory controls.

4.2. As-Is Security Diagnosis

The security assessment combined technical inspection, document review, and structured interviews with all 3 IT staff and 12 department heads. Infrastructure findings revealed critical obsolescence: VMware ESXi 6.5 (end-of-support since October 2022), FortiGate 60D firewall with firmware 14 months out-of-date (CVE exposure window), and SQL Server 2008 without extended security updates. No encryption at rest is implemented for the revenue database. Backup procedures are manual and untested (last recovery drill: never documented).

The López Loja MIL instrument [13] was applied across six COBIT domains (Table 3). The composite As-Is MIL score is 1.0 (range 0–5), indicating initial/ad-hoc practices with no formal policies or documented procedures. The weakest domains are Business Continuity (MIL = 0.3) and Incident Management (MIL = 0.5), where no formal plans exist. A SWOT analysis identifies as key strengths: committed IT leadership and recent LOPDP awareness training. Key weaknesses include zero security budget allocation and no CISO role.

4.3. AHP-TOPSIS Results

TABLE 2. AHP CRITERIA WEIGHTS — SUMMARY AND EIGENVALUE VERIFICATION

Criterion	Abbreviation	Weight (w_i)	λ_i	Rank
Risk Reduction	C_1 RR	0.4824 (48.24%)	4.0148	1
Implementation Cost	C_2 IC	0.2718 (27.18%)	4.0147	2
Deployment Time	C_3 DT	0.1575 (15.75%)	4.0144	3

Criterion	Abbreviation	Weight (w_i)	λ_i	Rank
Technical Complexity	C_4 TC	0.0883 (8.83%)	4.0141	4
—	$\lambda_{max} = 4.0145$	$\sum = 1.0000$	CR = 0.0054	✓

TABLE 3. TOP-5 ISO/IEC 27001:2022 CONTROLS BY TOPSIS RANKING (C_i^*)

Rank	ISO 27001:2022 Control	EGSI Cat.	C_i^*	D^+	D^-
1	A.8.3 — Information access restriction	Access Ctrl.	0.8907	0.041	0.334
2	A.8.24 — Use of cryptography	Cryptography	0.8444	0.063	0.342
3	A.5.24 — IS incident mgmt. planning	Incident Mgmt.	0.8040	0.088	0.361
4	A.8.13 — Information backup	Continuity	0.7780	0.097	0.340
5	A.5.2 — Information security roles	Governance	0.7647	0.108	0.351

Note: $C_i^* \geq 0.70 \rightarrow$ Priority 1 (implementation within 6 months)

5. Results and Discussion

Applying the TOPSIS-ranked implementation sequence to GAD Jaramijó's 36-month roadmap projects a To-Be MIL of 2.8 (+1.8 points from baseline 1.0). This increment is based on the López Loja et al. [13] calibration table, which maps completed control sets to expected MIL gains. Specifically, full implementation of the 47 EGSI mandatory controls (Priority 1–2) is projected to raise MIL to 2.5 by month 24, with the additional 0.3 gain derived from COBIT MEA02 continuous monitoring practices activated in months 25–36.

Four quantitative outcomes targets are defined: (i) residual risk reduction ≥40% for the three critical systems (Revenue, Cadastral, HR/Payroll) as computed by MAGERIT risk re-assessment post-implementation; (ii) EGSI compliance ≥85% for all High priority controls; (iii) cybersecurity investment ≤12% of annual IT budget over 24 months (projected USD 67,200 against a USD 560,000 IT envelope); and (iv) documented incident response capability (MTTR ≤48 hours) for ransomware scenarios by month 18.

Expert validation was conducted via a single-round structured expert review with 7 specialists (3 cybersecurity practitioners, 2 COBIT-certified auditors, 2 public-sector CISOs; mean professional experience 12.4 years). Using a 5-point Likert scale across three dimensions, results confirmed: Pertinence 4.6/5.0 ($\sigma = 0.31$), Viability 4.2/5.0 ($\sigma = 0.42$), and Completeness 4.1/5.0 ($\sigma = 0.38$). All mean scores exceed the 4.0 threshold established a priori. The experts specifically endorsed the AHP weight for Risk Reduction (48.24%) as appropriate for institutions facing LOPDP penalty exposure.

The framework's transferability extends to the estimated other small Ecuadorian cantonal GADs with profiles similar to Jaramijó (budget USD 5–15M, IT staff ≤5 FTE, current MIL ≤1.5). The AHP weights are parameterizable: municipalities with larger IT budgets may re-weight C_2 downward; those with shorter electoral cycles may prioritize C_3. No full sensitivity matrix was preserved for independent audit; robustness beyond the reported case is therefore not claimed.

Limitations include the single-site case study (internal validity strong, external validity inferred), the absence of longitudinal post-implementation data, and the manual nature of the AHP elicitation. Future work should address these through multi-site validation across at least 10 GADs of varying sizes.

5.1. Neutrosophic Uncertainty Extension

For the five displayed controls, Table 5 adds a limited neutrosophic reporting-precision audit: T is the recomputed TOPSIS closeness, I is the width induced by rounding the displayed distances to three decimals, and F = 1 − T. This I component measures numerical reporting precision only; it is not a substitute for the unavailable per-expert uncertainty matrix. The top-five order remains stable at the

displayed precision. A future deployment should separately elicit expert support, indeterminacy and counterevidence [16–20].

Table 4. Neutrosophic Reporting-Precision Audit for the Five Leading Controls

TOPSIS rank	T = Ci	I = rounding interval	F = 1 − Ci
1	0.8907	0.0027	0.1093
2	0.8444	0.0025	0.1556
3	0.8040	0.0022	0.1960
4	0.7780	0.0023	0.2220
5	0.7647	0.0022	0.2353

6. Conclusion

This paper presented MPEC-GAD, a three-layer cybersecurity governance model for small Latin American local governments. Three principal conclusions emerge from the GAD Jaramijó application. First, the AHP-TOPSIS prioritization produces a consistent, transparent investment sequence (CR = 0.0054) that directs ≤12% of the IT budget toward the 47 EGSI-mandatory controls with highest risk-reduction per unit cost, more transparent than the current ad-hoc approach at the institution.

Second, the COBIT 2019 goal-cascade mechanism provides a governance accountability structure (EDM01 through MEA02) that bridges strategic intent and operational implementation, enabling GAD administrators without cybersecurity backgrounds to own the security agenda. The 36-month roadmap projecting MIL 1.0 → 2.8 is operationally realistic given the institution's resource envelope and was rated as pertinent in a single-round review by seven experts (pertinence 4.6/5.0).

Third, the model's transferability to the 65% of comparable Ecuadorian cantonal GADs motivates testing MPEC-GAD in a broader multi-municipality study for subnational e-government cybersecurity. Future work will focus on: (i) automating the AHP-TOPSIS engine as a web-based decision support tool; (ii) extending the framework to intermediate GADs (budget > USD 30M); and (iii) integrating real-time SIEM telemetry to enable dynamic MIL reassessment.

Acknowledgment

The authors thank GAD Jaramijó authorities and IT staff for their cooperation during the field assessment. This work was conducted within the Research Program on Intelligent Systems and Digital Governance at Universidad Bolivariana del Ecuador.

References

[1] Sophos, "The State of Ransomware in Government 2023," Sophos Ltd., Oxford, UK, Tech. Rep., 2023. [Online]. Available: https://www.sophos.com/en-us/content/state-of-ransomware

[2] Kaspersky Lab, "Cyberthreat Landscape in Latin America 2023," Kaspersky Global Research & Analysis Team, Moscow, Russia, Tech. Rep., 2023.

[3] MINTEL, "Diagnóstico de Capacidades Digitales de Gobiernos Autónomos Descentralizados," Ministerio de Telecomunicaciones del Ecuador, Quito, Rep. Téc., 2023.

[4] ISACA, COBIT® 2019 Framework: Governance and Management Objectives. Schaumburg, IL: ISACA, 2018.

[5] ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva: ISO, 2022.

[6] MINTEL, "Esquema Gubernamental de Seguridad de la Información v3.0 (EGSI)," Ministerio de Telecomunicaciones del Ecuador, Acuerdo Ministerial N° 023-2024, Quito, 2024.

[7] J. Hendry, P. McDermott, and A. Williamson, "Integrated Governance and Security Framework (IGSF): Bridging COBIT 2019 and ISO/IEC 27001:2022," J. Inf. Secur. Appl., vol. 82, p. 103698, 2025.

[8] T. Schmidt, L. Fischer, and M. Weber, "Lessons Learned from COBIT-ISO 27001 Integration in Small European Municipalities," Gov. Inf. Q., vol. 42, no. 1, p. 101892, 2025.

[9] M. A. Hossain, R. Kumar, and S. Al-Farsi, "Cybersecurity Maturity in Local Governments: A Systematic Review," Comput. Secur., vol. 138, p. 103645, 2025.

[10] T. L. Saaty, The Analytic Hierarchy Process. New York, NY: McGraw-Hill, 1980.

[11] C. L. Hwang and K. Yoon, Multiple Attribute Decision Making: Methods and Applications. Berlin: Springer, 1981.

[12] N. H. Md Hanafiah, M. Z. Jamaludin, and R. A. Hamdan, "Cybersecurity Control Prioritization for Port Information Systems Using AHP-TOPSIS," IEEE Access, vol. 13, pp. 45210–45225, 2025.

[13] J. C. López Loja, F. Suquí Romero, and A. Narváez Pérez, "Modelo de Madurez MIL para Infraestructuras Críticas Ecuatorianas," Rev. Iberoam. Autom. Inform. Ind., vol. 20, no. 3, pp. 245–258, 2023.

[14] Asamblea Nacional del Ecuador, Ley Orgánica de Protección de Datos Personales (LOPDP). Quito: Registro Oficial Suplemento 459, 2021.

[15] Ministerio de Hacienda de España, MAGERIT v3.0 — Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: MINHAC, 2012.

[16] L. G. Lopezdominguez Rivas, S. D. Lopezdominguez Rivas, D. M. Lopezdominguez Rivas, and F. Parrales-Bravo, "How Much of a Multicriteria Ranking Is the Data and How Much Is the Arithmetic? A Neutrosophic Stress Test on Stakeholder Perception Data," accepted manuscript, CITIS 2026, paper 241, 2026.

[17] M.-E. Puebla-Martínez, "HERA 2.0: Human-Governed Agentic Software Development with External Cognitive Orchestration -- An Industrial Experience Report on AI-DLC with ChatGPT Web as Cognitive Continuity Layer," Neutrosophic Sets and Systems, vol. 101, 2026, forthcoming.

[18] V. Vega Falcón, "Which operation moves the ranking? Single-operation contrasts for a neutrosophic TOPSIS model with ordered weighted distances," Journal of Evidential and Paraconsistent Reasoning, vol. 1, no. 1, 2026. https://doi.org/10.5281/zenodo.22712873

[19] M. Leyva-Vázquez, E. Santos-Baquerizo, M. Peña-González, L. Cevallos-Torres, and A. Guijarro-Rodríguez, "The Extended Hierarchical Linguistic Model in Fuzzy Cognitive Maps," in Technologies and Innovation, CCIS, vol. 658, Springer, Cham, 2016, pp. 39–50, doi: 10.1007/978-3-319-48024-4_4.

[20] G. A. Álvarez Gómez, M. Y. Leyva Vázquez, and J. Estupiñán Ricardo, "Application of Neutrosophy to the Analysis of Open Government, its Implementation and Contribution to the Ecuadorian Judicial System," Neutrosophic Sets and Systems, vol. 52, pp. 215–224, 2022. https://digitalrepository.unm.edu/nss_journal/vol52/iss1/23

[21] M. Y. Leyva Vázquez, L. A. Briones Peñafiel, S. X. Sanchez Muñoz, and M. A. Quiroz Martinez, "A Framework for Selecting Machine Learning Models Using TOPSIS," in Advances in Artificial Intelligence, Software and Systems Engineering, AISC, vol. 1213, Springer, 2021, pp. 119–126, doi: 10.1007/978-3-030-51328-3_18.