

Cybersecurity as a mediator between e-government and control of corruption: Evidence from a panel study in Latin America and the Caribbean

Willy Alejo-Ramírez, *Pontificia Universidad Católica del Perú, Lima-Peru*, walejo@pucp.edu.pe

Christian Fernando Libaque-Saenz, *Universidad del Pacífico, Lima-Peru*, cf.libaques@up.edu.pe

Abstract

The literature on the relationship between e-government and control of corruption remains inconclusive, as it does not clearly explain how e-government reduces corruption. This issue is critical, given that approximately one quarter of global public expenditure is lost to corruption, with limited progress in controlling it over the past decade. This study examines the mediating role of cybersecurity in the relationship between e-government and control of corruption. A quantitative, correlational, non-experimental, exploratory design was employed, using a panel-structured dataset from 31 countries in Latin America and the Caribbean over the period 2014–2024. Regression-based models were used to examine the relationships between e-government and control of corruption. Grounded on the Principal-Agent and Institutional Theories, this study's proposed research model incorporates cybersecurity as a mechanism linking e-government to control of corruption. Findings suggest that cybersecurity not only directly influences control of corruption but also serves as a key mechanism through which e-government influences it, by enhancing the integrity of digital systems and reducing opportunities for manipulation and abuse. However, the results also reveal inconsistent mediation, in which cybersecurity simultaneously reinforces and constrains the positive effects of e-government on control of corruption, suggesting a more complex relationship conditioned by institutional and governance dynamics. The study contributes by clarifying this mechanism, providing regional empirical evidence, and offering policy-relevant insights for the design of secure and effective e-government strategies.

Keywords: Cybersecurity, e-government, control of corruption, inconsistent mediation, panel data analysis

Introduction

Information and communication technologies (ICTs) have revolutionized the way the public sector delivers its services, opening a wide range of new opportunities (Chen & Aklikokou, 2021). Their increasing application has driven the development of e-government, a concept defined as the provision of government services through ICTs to strengthen the interaction between public organizations and society, including stakeholders, associations, and citizens (Rose et al., 2018; Todisco et al., 2021). The potential benefits of e-government include transparency, accountability, and the strengthening of democratic processes, thereby contributing to the control of corruption (Bertot et al., 2010; Krishnan et al., 2017; Sung & Park, 2021).

Corruption generally occurs when private wealth and public power overlap (Cappelli et al., 2022). In this regard, corruption is defined as any conduct that deviates from generally accepted norms in the exercise of

public office for the purpose of obtaining private benefit (Cappelli et al., 2022; Khan & Krishnan, 2021; Wawrosz, 2019). Such conduct is a universal phenomenon that has persisted from ancient times to the modern era (Choi, 2007). The 2025 Corruption Perceptions Index revealed that 82.9% of the 181 countries assessed showed no significant progress in reducing corruption in the public sector over the past 13 years (Transparency International, 2026).

Corruption generates adverse effects in countries, both in socioeconomic and organizational terms. In the socioeconomic domain, corruption undermines sustainable and inclusive economic growth (Andersen, 2009; Jameel et al., 2019), hinders investment (Cieřlik & Goczek, 2018; Habib & Zurawicki, 2001), and compromises socio-political stability (Cappelli et al., 2022; Schumacher, 2013). It is estimated that 25% of global public expenditure is lost to corruption (United Nations, 2023). In organizational terms, corruption limits the effectiveness of public policies (Ramirez-Madrid et al., 2022; Roseth et al., 2018), is associated with increased operational costs and practices of misallocation and misappropriation of funds (Silal & Saha, 2021), and undermines citizens' trust in government (E. Chang & Chu, 2006).

In response to the need to strengthen control of corruption, researchers in the field of e-government have intensified their studies on this topic over the past decade (Khan et al., 2021). E-government has been described as a potential means to control corruption and transform corrupt institutions (Alam et al., 2023; Srivastava et al., 2016). However, the existing literature remains insufficient, as it does not clarify when e-government effectively reduces corruption and when it does not (Wang et al., 2022). The identified gap highlights the need to examine additional variables that help explain the management of control of corruption through e-government. In this regard, Khan et al. (2021) argue that prior studies have not sufficiently established the mechanisms through which e-government affects corruption, highlighting the need for a deeper understanding of mediating factors. This need is grounded in the fact that mediating variables help explain the mechanism through which an independent variable influences a dependent variable (Baron & Kenny, 1986).

In response, Silal et al. (2023) proposed evaluating the impact of government quality measures on the abovementioned relationship. Among these, cybersecurity stands out as a potential explanatory factor (Al-Hawamleh, 2024; Bořa-Avram, 2024; Güler & Büyükközkın, 2023). Cybersecurity is understood as the integrated use of technologies, policies, and proactive practices to protect the digital assets of organizations and users in both local systems and Internet-connected networks (Asamblea Mundial de Normalización de las Telecomunicaciones, 2008; Lezzi et al., 2018). The implementation of cybersecurity measures can reinforce the integrity of government operations, serving as a mechanism through which e-government translates into improved control of corruption.

The present study addresses a gap in the literature by seeking to explain the relationship between e-government and control of corruption across countries. The purpose guiding this research is to identify the extent to which cybersecurity explains the relationship between e-government and control of corruption. In contrast to prior studies that adopt a broad cross-country perspective, this study focuses on Latin American and Caribbean countries, providing a more context-specific analysis. This objective follows the recommendation for future research by Chen and Aklikokou (2021), who suggest that this type of analysis should adopt panel-data approaches to better capture temporal and cross-sectional dynamics.

Literature Review

Corruption is understood as a universal phenomenon, persistent across time and space, and pathological, as it undermines the effectiveness and legitimacy of governments and political and market systems (Choi,

2007). Chen and Aklikokou (2021) highlighted that effective control of corruption requires accountability and transparency processes, less regulation, and greater openness to public and media scrutiny. Likewise, Hancu-Budui and Zorio-Grima (2023) found that public institutions attempt to legitimize themselves through the implementation of e-government, a mechanism described as a potential means to control corruption and transform corrupt institutions (Alam et al., 2023; Srivastava et al., 2016). Elbahnasawy (2014), for example, found causality-based evidence on the impact of e-government on corruption. Consistent with these results, prior empirical studies indicate a positive relationship between e-government and control of corruption (e.g., Cappelli et al., 2022; Seiam & Salman, 2024; Silal et al., 2023).

On the other hand, another group of studies suggests that a negative relationship between e-government and control of corruption may exist, implying that e-government can facilitate corruption rather than prevent it. For example, Bertot et al. (2010) argued that ICTs have created new means and opportunities for corrupt behavior. Wescott (2001) argued that e-government could provide corrupt officials with additional tools, thereby facilitating their involvement in illicit activities. Bhatnagar (2003) suggested that technological adoption could, paradoxically, accelerate corrupt processes within government. This perspective was supported by the study by Park and Kim (2020), which found that increased e-government development may be associated with higher levels of corruption, calling for further research in this area. In this respect, Boța-Avram (2024) emphasizes that the role of digitalization and technology in reducing corruption remains debated and may vary depending on the institutional and governance context.

These non-conclusive results in the literature highlight the complexity of this issue and the importance of examining how other factors may help explain the relationship between e-government and control of corruption (Arayankalam et al., 2021; Kalesnikaitė et al., 2023). Likewise, Wang et al. (2022) indicate that the literature linking e-government to control of corruption remains inconclusive because it has not fully explained the conditions under which e-government reduces corruption and the conditions under which it does not. In response, Silal et al. (2023) suggested evaluating the effect of government quality measures on the relationship between e-government and control of corruption, and cybersecurity was identified as one such potential measure (Al-Hawamleh, 2024; Boța-Avram, 2024). Similarly, Güler and Büyüközkan (2023) identified limitations in the current e-government literature, highlighting a lack of studies proposing practices to strengthen government cybersecurity and arguing that government cybersecurity systems and the sustainability of trust in public services are major research gaps on this topic.

In Latin America and the Caribbean (LAC), the relationship between e-government and control of corruption is particularly relevant given the persistent challenges in governance and institutional effectiveness across the region. LAC has historically been regarded as one of the most unequal regions in the world (Economic Commission for Latin America and the Caribbean, 2016). This condition can exacerbate vulnerabilities to corruption and weaken institutional capacity. In this context, the 2025 Corruption Perceptions Index reports a lack of progress in combating corruption in the region, with an average decline of 2.37 points from 2016 levels, and highlights that corruption negatively affects people's lives and exacerbates violence (Transparency International, 2026).

This article addresses the existing gap in the literature in explaining the relationship between e-government and control of corruption across countries, with a particular focus on LAC, specifically regarding the potential mediating role of cybersecurity. This study also contributes to the field of strategic management in both academic and practical domains by expanding theoretical understanding of this relationship through empirical evidence that strengthens the existing literature. From a methodological perspective, it proposes and validates a model that integrates cybersecurity, offering a reference framework for future research. In practical terms, its findings can inform decision-making and the implementation of secure e-government strategies, fostering more effective management of corruption control in the public sector.

Theoretical Framework and Hypotheses

In this section, the main theoretical lenses will be discussed in order to understand the relationship between e-government, cybersecurity, and control of corruption.

Relationship between E-Government and Control of Corruption

Principal-Agent Theory is one of the seminal theories that clarifies the relationship between e-government and corruption (Norris & Moon, 2005). This theory emphasizes how public officials (agents) represent citizens (principals). Klitgaard (1991) argues that effective anti-corruption strategies within the principal-agent framework should focus on reducing officials' discretionary power and strengthening oversight and accountability mechanisms. From this perspective, e-government facilitates the scrutiny of government actions and promotes accountability by increasing transparency and providing access to information (Zhao & Xu, 2015).

Empirical studies have linked both variables. For example, Nam (2018) analyzed data from 191 countries in 2016 and found a significant, positive correlation between e-government development and control of corruption. Similarly, Chen and Aklirikou (2021) found a significant, positive correlation between the two variables using data from 191 countries. On the other hand, Abbas et al. (2022) analyzed 42 Asian countries over 2015–2021. They identified a significant, negative correlation between e-government and the prevalence of corruption, the latter being an inverse measure of control of corruption, which explains the observed negative relationship. Silal et al. (2023) analyzed 102 countries over 2008–2019 and found a significant, positive correlation between e-government development and a reduction in citizens' perceived corruption. Similar results were obtained by Seiam and Salman (2024), who analyzed 110 countries between 2003 and 2021 and found a significant, positive association between e-government development and the prevention of corruption. However, some studies, as in Arayankalam et al. (2021), failed to find evidence of a relationship between e-government and three dimensions of corruption: legislative, executive, and judicial.

Cybersecurity in the Relationship Between E-Government and Control of Corruption

Institutional Theory has been applied in studies on ICTs in governmental settings (Luna-Reyes & Gil-Garcia, 2011; Ramirez-Madrid et al., 2022; Zheng et al., 2013). This theory is complemented by Principal-Agent Theory, which has helped clarify the relationship between e-government and corruption (Norris & Moon, 2005). The adoption of new technologies raises regulatory and ethical dilemmas, such as those related to data security and privacy (V. Chang et al., 2020). Institutional Theory focuses on how structures, norms, and rules—both formal and informal—influence the behavior of individuals and organizations, and thus this theory offers a valuable perspective for understanding the challenges associated with implementing e-government (Kim et al., 2009). It highlights the role of social and cultural contexts in shaping institutions and, in turn, practices and behaviors. Both theories help explain these dynamics within governmental organizations in the context of control of corruption.

The risk of cybercrime and cyberattacks increases as governance and service systems become more digital, representing a significant barrier to the efficient delivery of e-government services (Al-Hawamleh, 2024; Bokhari, 2023). This situation may lead to broader access to databases, making them susceptible to manipulation by officials with advanced technical skills, thereby empowering a new bureaucratic elite (Cappelli et al., 2022). Hence, the implementation of ICTs can both build and undermine trust (Smith, 2011). A robust cybersecurity system will protect organizational databases and public processes, promoting the efficient delivery of e-government services and strengthening citizens' trust in government (Al-Hawamleh, 2024). Boța-Avram (2024) argues that technologies aimed at improving the control of

interactions between citizens and public officials should be supported by robust security protocols to manage cybersecurity risks and potential cyberattacks.

In this regard, Abbas et al. (2022) assessed 42 Asian countries between 2015 and 2021 and identified a significant, positive correlation between e-government and cybersecurity. Similarly, the authors found a significant correlation between cybersecurity and corruption-free government systems. Likewise, Krishna and Sebastian (2021) analyzed 127 countries and identified a significant, positive correlation between e-government and cybersecurity. In addition, Al-Hawamleh (2024) found, through an analysis of 285 questionnaires administered to employees of the Saudi Electronic University in the Kingdom of Saudi Arabia, a significant, positive correlation between cybersecurity practices and the quality of e-government services.

Research Model

Based on the above discussion, the research model of this study (see Figure 1) integrates concepts from Principal-Agent and Institutional Theories. Principal-Agent Theory has facilitated the study of the relationship between e-government and control of corruption over the past decade. Institutional Theory, on the other hand, explains how structures, norms, and rules influence the behavior of individuals and organizations behavior. Accordingly, this theory explains that e-government implementation involves challenges such as data security and privacy (V. Chang et al., 2020), which supports the inclusion of cybersecurity as a mediator in the relationship. Cybersecurity refers to the set of institutional, technical, and operational capabilities aimed at protecting digital systems and infrastructures, which may influence the relationship between e-government and control of corruption. Hence, the research model proposes that cybersecurity acts as a mediating mechanism linking e-government to control of corruption. E-government (EGOV) is considered the independent variable. In turn, cybersecurity (CSEC) functions as both an independent and a dependent variable, as it is a mediating variable in the model. Finally, Control of Corruption (CC) is defined as the outcome variable. In short, this study proposes:

- H1: EGOV positively influences CC
- H2: EGOV positively influences CSEC
- H3: CSEC positively influences CC
- H4: CSEC mediates the relationship between EGOV and CC by transmitting part of the effect of EGOV on CC

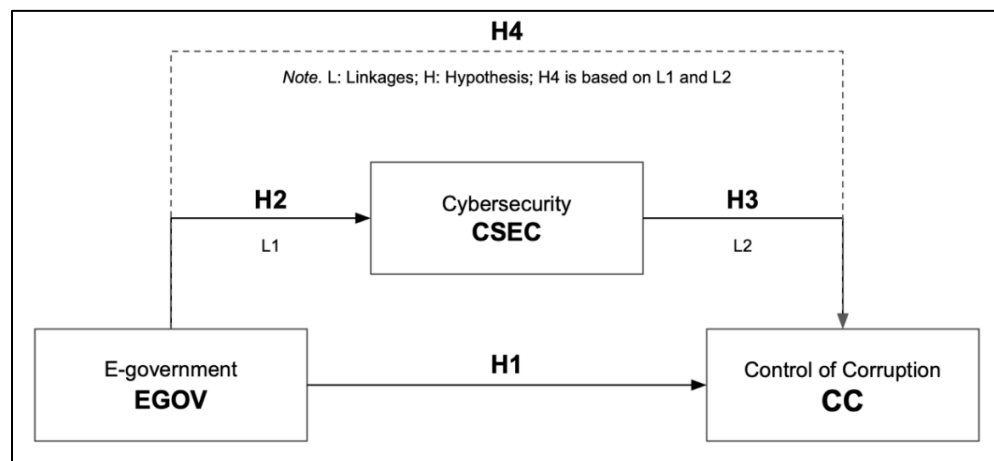


Figure 1. Research Model

Research Methodology

This study adopted a quantitative, correlational, non-experimental, and panel design. This approach is appropriate for analyzing patterns and relationships among variables over time and across countries using secondary data (e.g., Abbas et al., 2022; Khan & Krishnan, 2021; Srivastava et al., 2016).

Measurement of Variables and Data Collection

This study used secondary data sources covering LAC countries over the period 2014–2024, where countries constitute the unit of analysis. Furthermore, the target population comprises all countries assessed by the selected international data sources for the LAC region during the specified period, providing a regional framework for the comparative analysis of the variables under study. To assess EGOV, the study used the E-Government Development Index developed by the United Nations and applied across countries in the region between 2003 and 2024 (United Nations, 2022). This index has been widely referenced in the relevant scientific literature (e.g., Abbas et al., 2022; Chen & Aklikokou, 2021; Khan & Krishnan, 2021). To measure CSEC, the Global Cybersecurity Index developed by the International Telecommunication Union was used, covering the 2014–2024 period (International Telecommunication Union, 2021). This index has been employed in similar studies, such as those by Abbas et al. (2022) and Krishna and Sebastian (2021). Finally, to assess CC, the World Governance Indicator of the World Bank was used, which covers the same set of countries from 1996 to 2023 (Kaufmann & Kraay, 2024). This indicator was also used in similar studies (e.g., Chen & Aklikokou, 2021; Silal & Saha, 2021).

The delimitation of the units of analysis is based on the observable population, defined as the set of countries with complete and comparable secondary data for the variables under study. Consequently, the analysis adopts an incomplete census relative to the theoretical population, with coverage of the observable population determined by the availability of secondary data, in accordance with the distinction between theoretical and empirical populations in research based on secondary data (Daniels, 2012; Malhotra, 2016). The review of available data enabled the selection of 31 LAC countries with complete and comparable information across the three study variables. El Salvador was excluded from the analysis due to incomplete data across all study variables. The data cover the three study variables for the years 2014, 2018, 2020, 2022, and 2024.

Analytical Technique

This study employs multiple regression as its analytical technique. Accordingly, this study analyzed the relationships among the dependent, independent, and mediating variables, all measured as metric variables, in the context of national governments, understood as countries' organizational entities. The data used in this analysis were drawn from secondary sources, forming a panel-structured dataset that allows for the observation of both longitudinal and cross-sectional variations across countries. Given the exploratory and pilot nature of this study, the empirical analysis was conducted using regression-based models applied to this panel-structured dataset. Although the data include both cross-sectional and temporal variation, the purpose of the analysis is to provide an initial assessment of the relationships between EGOV, CSEC, and CC in the LAC context, rather than to estimate a fully specified panel econometric model. Finally, a multicollinearity analysis was conducted among the independent variables using variance inflation factors (VIFs); values below 5 would indicate the absence of problematic collinearity (Kerlinger & Lee, 2002).

Results

Two multiple linear regression models were estimated to analyze the relationships between EGOV, CSEC, and CC, and to evaluate the potential mediating effect of CSEC on the relationship between EGOV and

CC. The first regression was conducted with EGOV and CSEC as independent variables and CC as the dependent variable. The second regression was conducted with EGOV as the independent variable and CSEC as the dependent variable. Before the analysis, the assumptions required for the proper application of this statistical technique were verified. First, the potential presence of multicollinearity among the independent variables was assessed using the Variance Inflation Factor (VIF). The results showed values below the recommended threshold of 5: 1.821 for EGOV and CSEC (first regression), and 1 for the second regression, confirming the absence of problematic collinearity among the independent variables (Kerlinger & Lee, 2002).

Second, the assumptions of homoscedasticity, normality, and linearity of the residuals were visually assessed, revealing patterns consistent with the linear model's requirements in both regressions. In particular, the residuals exhibited approximately constant dispersion across the predicted values, a distribution close to normality, and linear relationships between the independent and dependent variables, indicating compliance with the assumptions required for multiple linear regression in both cases.

In the first regression, results indicate that the overall model is statistically significant ($F = 26.950$, $p < 0.001$) and explains 30.8% of the observed variance in CC ($R^2 = 0.308$), suggesting moderate explanatory power and an adequate fit to the analyzed data. Regarding the individual effects (standardized coefficients), EGOV shows a positive, statistically significant effect on CC ($\beta = 0.748$, $p < 0.001$), providing empirical support for H1. This result suggests that higher levels of EGOV are associated with higher levels of CC in the countries analyzed, highlighting the potential of government digitalization initiatives to strengthen transparency and reduce opportunities for corruption. On the other hand, CSEC has a negative and significant effect on CC ($\beta = -0.472$, $p < 0.001$), contrary to the initial hypothesis (H3). The negative sign of the coefficient suggests that, after controlling for EGOV, higher levels of CSEC are associated with lower levels of CC in the countries analyzed. This result reveals a more complex dynamic between CSEC and CC in the LAC context, differing from the initially expected positive relationship.

In the second regression, the overall model was also statistically significant ($F = 100.110$, $p < .001$), explaining 45.1% of the observed variance in CSEC ($R^2 = 0.451$), indicating adequate explanatory power. In terms of standardized coefficients, the results show that EGOV presents a positive and significant effect on CSEC ($\beta = 0.671$, $p < .001$), providing empirical support for H2. This finding indicates that higher levels of EGOV are associated with higher levels of CSEC, suggesting that the advancement of e-government initiatives is accompanied by the strengthening of national capacities to protect digital infrastructure, systems, and services. Figure 2 summarizes the empirical results of the proposed research model.

Finally, the potential mediating effect of CSEC on the relationship between EGOV and CC was evaluated. The results show that EGOV has a positive direct effect on CC, whereas the indirect effect transmitted through CSEC is negative. Taken together, these findings show inconsistent mediation, characterized by the coexistence of direct and indirect effects with opposite signs. In substantive terms, the results suggest that EGOV contributes directly to strengthening CC; however, part of this positive effect is partially offset by the negative indirect effect associated with CSEC. This finding indicates that the relationship between EGOV and CC is neither linear nor uniform, but rather depends on institutional dynamics and complementary capacities for cybersecurity management.

Consequently, the results provide empirical support for H1 and H2, whereas H3 presents a behavior opposite to that initially expected under certain institutional controls. Likewise, H4 receives partial support under an inconsistent mediation framework, revealing a more complex dynamic between EGOV, CSEC, and CC in the LAC context.

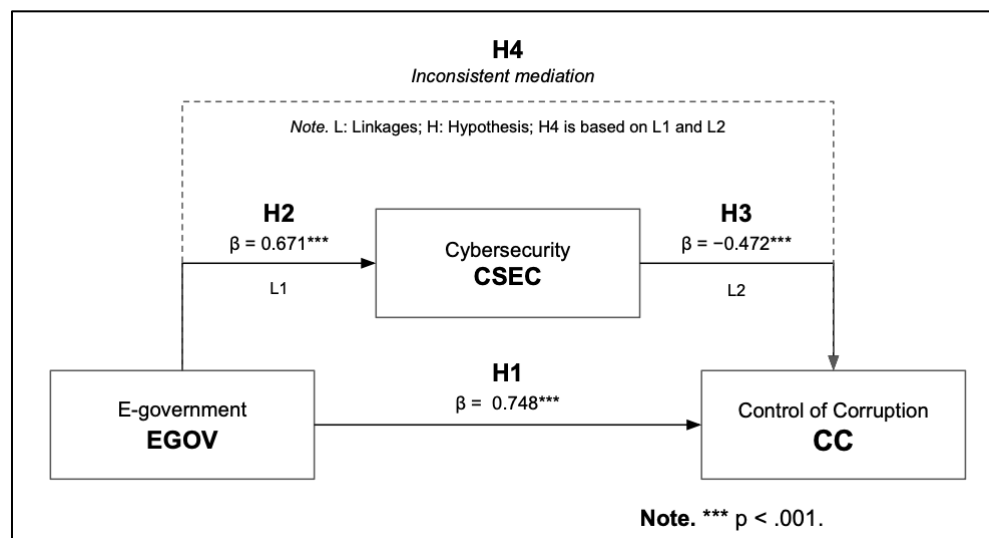


Figure 2. Empirical Results of the Research Model

Discussion and Implications

The results obtained provide partial empirical support for the proposed model and contribute new evidence regarding the relationships between EGOV, CSEC, and CC in the LAC context. Overall, the findings clarify the mechanisms by which EGOV influences CC, addressing a gap in the literature regarding the limited understanding of how e-government effectively translates into improvements in control of corruption (Khan et al., 2021; Wang et al., 2022).

First, the results confirm that EGOV presents a positive and significant effect on CC, providing empirical support for H1. This finding is consistent with previous studies that identify e-government as a mechanism for strengthening transparency, accountability, and public oversight (Andersen, 2009; Chen & Aklikokou, 2021; Nam, 2018). Likewise, the results support the arguments of Srivastava et al. (2016), who suggest that process automation and the reduction of discretionary interactions between public officials and citizens can reduce opportunities for corrupt practices. From the perspective of Principal-Agent Theory, this finding suggests that EGOV reduces information asymmetries between citizens and public officials by strengthening monitoring mechanisms and limiting opportunities for administrative discretion.

Second, the results show that EGOV exerts a positive and highly significant effect on CSEC, providing empirical support for H2. This result is consistent with studies that identify a growing alignment between the advancement of e-government and the strengthening of national cybersecurity capabilities (Güler & Büyükožkan, 2023; Krishna & Sebastian, 2021). Likewise, from the perspective of Institutional Theory, the finding supports the idea that adopting digital technologies promotes the development of complementary structures, capabilities, and mechanisms to ensure the functioning and sustainability of governmental digital ecosystems (Luna-Reyes & Gil-Garcia, 2011). In this sense, the growth of EGOV in the analyzed countries tends to be accompanied by greater institutional efforts to strengthen the protection of digital infrastructure, systems, and services.

Nevertheless, the results show that CSEC has a statistically significant negative effect on CC, contrary to the initial hypothesis (H3). The negative coefficient indicates a more complex dynamic between CSEC and CC in the LAC context. This result partially aligns with Boța-Avram's (2024) arguments, which suggest

that the effects of digitalization on corruption remain subject to debate and may yield heterogeneous results depending on the institutional context analyzed. The rejection of H3 further reinforces the heterogeneous and context-dependent nature of the relationship between cybersecurity and control of corruption in LAC countries.

The findings suggest a gap between strengthening national CSEC capabilities and their effective translation into CC outcomes. Although the strengthening of CSEC accompanies the growth of EGOV and contributes to the protection, resilience, and operational sustainability of the governmental digital ecosystem, there is no evidence that these capabilities are directly translated into institutional mechanisms that strengthen public integrity, accountability, oversight, or anti-corruption enforcement. Consequently, CSEC emerges as a necessary condition for sustaining the State's digital transformation, but is not, by itself, sufficient to guarantee observable improvements in CC. This finding underscores the need to reflect on the degree of articulation between operational cybersecurity capabilities and public governance mechanisms that support transparency, traceability, and institutional control.

Most importantly, the results reveal inconsistent mediation by CSEC in the relationship between EGOV and CC, providing partial support for H4. This type of mediation is characterized by the coexistence of direct and indirect effects with opposite signs: EGOV maintains a positive direct effect on CC, while the indirect effect transmitted through CSEC is negative. This finding has theoretical and empirical relevance, as it helps explain why prior literature has reported inconclusive results on the impact of EGOV on control of corruption (Boța-Avram, 2024; Wang et al., 2022).

In substantive terms, the results suggest that EGOV directly strengthens CC through mechanisms associated with digitalization, automation, and reduced administrative discretion. However, this positive effect is partially offset by dynamics associated with CSEC that, in the LAC context, do not show sufficient evidence of being translated into institutional capacities to strengthen CC. This finding suggests that the effectiveness of EGOV depends not only on digital adoption but also on the degree of articulation between technological capabilities, governance structures, and institutional mechanisms oriented toward public control.

Overall, the findings contribute to shifting the discussion from whether EGOV reduces corruption toward a deeper understanding of the mechanisms and conditions under which such effects occur. In this sense, the study directly responds to calls for research to incorporate mediating variables and complementary institutional capacities into the analysis of the relationship between EGOV and corruption (Khan et al., 2021; Silal et al., 2023).

Theoretical Implications

These findings generate relevant implications for both research and practice in the fields of e-government, cybersecurity, and control of corruption. From a theoretical perspective, the study contributes to the literature on the relationship between EGOV and CC by incorporating CSEC as a mediating variable, thereby moving beyond approaches that focus exclusively on direct effects. In particular, the identification of inconsistent mediation demonstrates that complementary technological and institutional capacities may act as catalysts that simultaneously enhance and constrain the expected effects of e-government initiatives.

Likewise, the results suggest that strengthening CSEC capabilities does not automatically guarantee improvements in CC, especially in contexts characterized by heterogeneous institutional capacities. In this sense, the study highlights the need to examine not only the adoption of digital technologies but also the articulation among technological capabilities, governance structures, and institutional mechanisms of public control. Similarly, this study opens avenues for future research to explore further the role of cybersecurity within digital governance ecosystems. Consequently, future studies are encouraged to

incorporate mediating or moderating variables related to transparency, accountability, e-participation, institutional trust, or regulatory quality to better understand the mechanisms linking EGOV, CSEC, and CC. Additionally, future research should expand the analysis to a larger number of countries and incorporate institutional differences across regions.

Practical Implications

From a practical perspective, these findings suggest that public sector digital transformation strategies should not focus exclusively on expanding digital services or strengthening technological protection capabilities. Although CSEC constitutes a necessary condition for sustaining governmental digital ecosystems, the findings indicate that such capabilities alone do not guarantee observable improvements in CC unless they are articulated with mechanisms of transparency, traceability, oversight, and institutional control.

Accordingly, the empirical evidence suggests that public institutions and policymakers should promote integrated digital governance approaches by aligning cybersecurity strategies with broader objectives related to public integrity and control of corruption. In line with prior studies on digital transformation and improved public services, the findings also suggest that technological capabilities should be accompanied by citizen-centered governance approaches that strengthen transparency, reliability, and institutional trust within digital public service environments (Diaz-Parra & Libaque-Saenz, 2025).

More specifically, governments should align cybersecurity and anti-corruption policies through concrete governance mechanisms. First, cybersecurity strategies should be designed not only to protect digital infrastructure, but also to strengthen transparency, traceability, and accountability in public processes. This implies incorporating audit trails, access controls, data integrity mechanisms, and real-time monitoring tools into e-government platforms, particularly in high-risk areas such as public procurement, licensing, tax administration, subsidies, and social programs. Second, cybersecurity institutions and anti-corruption bodies should establish formal coordination mechanisms, including shared risk assessments, protocols for reporting cyber-enabled manipulation of public records, and joint incident response procedures. Third, policymakers should ensure that digital government projects include integrity-by-design and security-by-design principles from the planning stage, so that cybersecurity controls are directly connected to the prevention, detection, and investigation of corruption risks. As a further policy recommendation, governments should develop performance indicators that measure not only cybersecurity readiness or digital service availability, but also the contribution of secure digital systems to transparency, institutional oversight, and corruption control outcomes.

Finally, the study provides relevant evidence for LAC, a region characterized by accelerated digital transformation alongside persistent institutional and corruption-related challenges. In this context, the findings highlight the importance of aligning cybersecurity capabilities with broader governance and accountability mechanisms to strengthen the effectiveness of e-government initiatives.

Limitations

The study presents certain limitations related to data availability and the scope of the analysis. First, the research relies on secondary data sources, which limits the coverage of the theoretical population to the extent that international indicators are available and consistent. Consequently, the findings should be interpreted within the context of the study's observable population.

Second, the analysis focuses specifically on the mediating role of CSEC in the relationship between EGOV and CC, without incorporating other institutional, political, or socioeconomic factors that could also influence corruption control outcomes. In particular, the model does not include additional country-level

control variables, such as economic development, education, institutional quality, political stability, or other governance-related factors. The absence of these variables may limit the ability to isolate the specific effects of EGOV and CSEC on CC, particularly in cross-country panel analyses where institutional, socioeconomic, and political differences may influence the observed relationships. Therefore, future research should consider incorporating relevant control variables to reduce potential omitted variable bias and provide a more comprehensive explanation of the mechanisms linking EGOV, CSEC, and CC.

Likewise, while this study applies regression-based logic to assess the mediating role of CSEC, future studies could complement this approach with more robust mediation testing techniques. Such techniques would allow for a more precise estimation of indirect effects and would strengthen the empirical validation of CSEC as a mediating mechanism in the relationship between EGOV and CC. Additionally, although the study uses a panel-structured dataset, the empirical strategy does not estimate fixed effects or random effects panel models. This decision is consistent with the exploratory and pilot nature of the study, which seeks to provide an initial assessment of the proposed relationships in the LAC context. Future research could extend this analysis by applying fixed effects, random effects, or other longitudinal panel-data techniques to better account for unobserved country-specific heterogeneity and temporal dynamics. Moreover, the study adopts a quantitative approach without integrating qualitative perspectives or subnational analyses that could provide a deeper contextual understanding of the observed mechanisms.

Finally, the study is limited to the LAC context, which may limit the generalizability of its findings to regions with different institutional, political, and technological conditions. In this sense, future research could expand the geographical scope and incorporate mixed-method approaches to provide a more comprehensive understanding of the relationship between EGOV, CSEC, and CC.

Conclusions

This study examined the relationship between e-government, cybersecurity, and control of corruption in the Latin American and Caribbean context, providing partial empirical support for the proposed model. The findings confirm that e-government exerts a positive and significant effect on both control of corruption and cybersecurity capabilities, reinforcing the role of digital government as a driver of institutional modernization and public sector transparency. However, the results also reveal that cybersecurity capabilities present a significant negative effect on control of corruption, suggesting that strengthening cybersecurity does not necessarily translate into observable improvements in corruption control outcomes. In this regard, the study identifies inconsistent mediation, suggesting that cybersecurity capabilities may simultaneously reinforce and constrain the expected effects of e-government on control of corruption.

Overall, the findings suggest that the effectiveness of e-government depends not only on technological adoption but also on the articulation between cybersecurity capabilities, governance structures, and institutional mechanisms oriented towards transparency, accountability, and public control. Consequently, the study contributes to advancing the understanding of the complex mechanisms linking digital government, cybersecurity, and control of corruption in emerging institutional contexts.

References

- Abbas, H. S. M., Qaisar, Z. H., Ali, G., Alturise, F., & Alkhalifah, T. (2022). Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *PLoS ONE*, 17(11), e0274550. <https://doi.org/10.1371/journal.pone.0274550>

- Alam, T., Aftab, M., Abbas, Z., Ugli, K. M. M., & Bokhari, S. A. A. (2023). Impact of e-government initiatives to combat corruption mediating by behavioral intention: A quantitative analysis from emerging economies. *Sustainability*, 15(3), 2694. <https://doi.org/10.3390/su15032694>
- Al-Hawamleh, A. M. (2024). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. *Digital Policy, Regulation and Governance*, 26(3), 317–336. <https://doi.org/10.1108/dprg-11-2023-0168>
- Andersen, T. B. (2009). E-Government as an anti-corruption strategy. *Information Economics and Policy*, 21(3), 201–210. <https://doi.org/10.1016/j.infoecopol.2008.11.003>
- Arayankalam, J., Khan, A., & Krishnan, S. (2021). How to deal with corruption? Examining the roles of e-government maturity, government administrative effectiveness, and virtual social networks diffusion. *International Journal of Information Management*, 58, 102203. <https://doi.org/10.1016/j.ijinfomgt.2020.102203>
- Asamblea Mundial de Normalización de las Telecomunicaciones. (2008). *Recomendación UIT-T X.1205. Aspectos generales de la ciberseguridad*. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-S&type=items
- Baron, R. M., & Kenny, D. A. (1986). The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, 51(6), 1173–1182. <https://doi.org/10.1037/0022-3514.51.6.1173>
- Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 27(3), 264–271. <https://doi.org/10.1016/j.giq.2010.03.001>
- Bhatnagar, S. (2003). *Global Corruption Report 2003: Access to Information*. https://issuu.com/transparencyinternational/docs/2003_gcr_accessinfo_en
- Bokhari, S. A. A. (2023). A Quantitative Study on the Factors Influencing Implementation of Cybersecurity Laws and Regulations in Pakistan. *Social Sciences*, 12(11), 629. <https://doi.org/10.3390/socsci12110629>
- Boța-Avram, C. (2024). Examining the white and dark sides of digitalisation effects on corruption: unveiling research patterns and insights for future research. *Journal of Risk Finance*, 25(2), 181–223. <https://doi.org/10.1108/jrf-10-2023-0256>
- Cappelli, L., Pisano, A., Iannucci, E., Papetti, P., D’Ascenzo, F., & Ruggieri, R. (2022). Digitalization and prevention of corruption: Opportunities and risks—Some evidence from the Italian university system. *Business Strategy and the Environment*, 33(1), 81–94. <https://doi.org/10.1002/bse.3332>
- Chang, E., & Chu, Y. H. (2006). Corruption and trust: Exceptionalism in asian democracies? *The Journal of Politics*, 68(2), 259–271. <https://doi.org/10.1111/j.1468-2508.2006.00404.x>
- Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, 158, 120166. <https://doi.org/10.1016/j.techfore.2020.120166>

- Chen, L., & Aklikokou, A. K. (2021). Relating e-government development to government effectiveness and control of corruption: a cluster analysis. *Journal of Chinese Governance*, 6(1), 155–173. <https://doi.org/10.1080/23812346.2019.1698693>
- Choi, J. W. (2007). Governance structure and administrative corruption in Japan: An organizational network approach. *Public Administration Review*, 67(5), 930–942. <https://doi.org/10.1111/j.1540-6210.2007.00779.x>
- Cieřlik, A., & Goczek, Ł. (2018). Control of corruption, international investment, and economic growth – Evidence from panel data. *World Development*, 103, 323–335. <https://doi.org/10.1016/j.worlddev.2017.10.028>
- Daniels, J. D. (2012). Técnicas de muestreo. In *Investigación de mercados* (4th ed., 4). Pearson Educación.
- Diaz-Parra, R., & Libaque-Saenz, C. F. (2025). The impact of digitalization on peruvian public services. *Issues in Information Systems*, 26(3), 220–236. https://doi.org/10.48009/3_iis_2025_2025_118
- Economic Commission for Latin America and the Caribbean. (2016). *The social inequality matrix in Latin America*. <https://hdl.handle.net/11362/40710>
- Elbahnasawy, N. G. (2014). E-Government, internet adoption, and corruption: An empirical investigation. *World Development*, 57, 114–126. <https://doi.org/10.1016/j.worlddev.2013.12.005>
- Güler, M., & Büyüközkan, G. (2023). A survey of digital government: Science mapping approach, application areas, and future directions. *Systems*, 11(12), 563. <https://doi.org/10.3390/systems11120563>
- Habib, M., & Zurawicki, L. (2001). Country-level investments and the effect of corruption — some empirical evidence. *International Business Review*, 10(6), 687–700. [https://doi.org/10.1016/S0969-5931\(01\)00038-5](https://doi.org/10.1016/S0969-5931(01)00038-5)
- Hancu-Budui, A., & Zorio-Grima, A. (2023). Supreme audit institutions in Europe: synergies, institutional transparency, gender equality and sustainability engagement. *Journal of Public Budgeting, Accounting and Financial Management*, 35(4), 451–473. <https://doi.org/10.1108/jpbafm-07-2021-0116>
- International Telecommunication Union. (2021). *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity*. <https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E>
- Jameel, A., Asif, M., Hussain, A., Hwang, J., Sahito, N., & Bukhari, M. H. (2019). Assessing the moderating effect of corruption on the e-government and trust relationship: An evidence of an emerging economy. *Sustainability*, 11(23), 6540. <https://doi.org/10.3390/su11236540>
- Kalesnikaite, V., Neshkova, M. I., & Ganapati, S. (2023). Parsing the impact of e-government on bureaucratic corruption. *Governance*, 36(3), 827–842. <https://doi.org/10.1111/gove.12707>
- Kaufmann, D., & Kraay, A. (2024). *The Worldwide Governance Indicators: Methodology and 2024 update* (10952; Policy Research Working Paper; 10952). <https://doi.org/10.1596/1813-9450-10952>

- Kerlinger, F., & Lee, H. (2002). *Investigación del Comportamiento* (L. Pineda & I. Mora, Trans.; 4th ed.). McGraw-Hill. <https://padron.entretemas.com.ve/INICC2018-2/lecturas/u2/kerlinger-investigacion.pdf>
- Khan, A., & Krishnan, S. (2021). Moderating effects of business-systems corruption on corruption in basic national institutions and electronic government maturity: Insights from a dynamic panel data analysis. *International Journal of Information Management*, 59, 102349. <https://doi.org/10.1016/j.ijinfomgt.2021.102349>
- Khan, A., Krishnan, S., & Dhir, A. (2021). Electronic government and corruption: Systematic literature review, framework, and agenda for future research. *Technological Forecasting and Social Change*, 167, 120737. <https://doi.org/10.1016/j.techfore.2021.120737>
- Kim, S., Kim, H. J., & Lee, H. (2009). An institutional analysis of an e-government system for anti-corruption: The case of OPEN. *Government Information Quarterly*, 26(1), 42–50. <https://doi.org/10.1016/j.giq.2008.09.002>
- Klitgaard, R. (1991). *Controlling Corruption* (1st ed.). University of California Press. <https://www.ucpress.edu/book/9780520074088/controlling-corruption>
- Krishna, B., & Sebastian, M. P. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis. *Information and Computer Security*, 29(5), 737–760. <https://doi.org/10.1108/ics-12-2020-0205>
- Krishnan, S., Teo, T. S. H., & Lymm, J. (2017). Determinants of electronic participation and electronic government maturity: Insights from cross-country data. *International Journal of Information Management*, 37(4), 297–312. <https://doi.org/10.1016/j.ijinfomgt.2017.03.002>
- Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, 103, 97–110. <https://doi.org/10.1016/j.compind.2018.09.004>
- Luna-Reyes, L. F., & Gil-Garcia, J. R. (2011). Using institutional theory and dynamic simulation to understand complex e-Government phenomena. *Government Information Quarterly*, 28(3), 329–345. <https://doi.org/10.1016/j.giq.2010.08.007>
- Malhotra, N. K. (2016). *Sampling design and procedures*. In *Marketing research: An applied orientation* (Pearson, Ed.; 7th ed., 9).
- Nam, T. (2018). Examining the anti-corruption effect of e-government and the moderating effect of national culture: A cross-country study. *Government Information Quarterly*, 35(2), 273–282. <https://doi.org/10.1016/j.giq.2018.01.005>
- Norris, D. F., & Moon, M. J. (2005). Advancing e-government at the grassroots: Tortoise or hare? *Public Administration Review*, 65(1), 64–75. <https://doi.org/10.1111/j.1540-6210.2005.00431.x>
- Park, C. H., & Kim, K. (2020). E-government as an anti-corruption tool: panel data analysis across countries. *International Review of Administrative Sciences*, 86(4), 691–707. <https://doi.org/10.1177/0020852318822055>

- Ramirez-Madrid, J. P., Escobar-Sierra, M., Lans-Vargas, I., & Montes Hincapie, J. M. (2022). Government influence on e-government adoption by citizens in Colombia: Empirical evidence in a Latin American context. *PLoS ONE*, 17(2), e0264495. <https://doi.org/10.1371/journal.pone.0264495>
- Rose, J., Flak, L. S., & Sæbø, Ø. (2018). Stakeholder theory for the E-government context: Framing a value-oriented normative core. *Government Information Quarterly*, 35(3), 362–374. <https://doi.org/10.1016/j.giq.2018.06.005>
- Roseth, B., Reyes, A., Farias, P., Porrúa, M., Villalba, H., Acevedo, S., Peña, N., Estevez, E., Lejarraga, S. L., & Fillottrani, P. (2018). El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital. In B. Roseth, A. Reyes, & C. Santiso (Eds.), *Banco Interamericano de Desarrollo (BID)*. Inter-American Development Bank. <https://doi.org/http://dx.doi.org/10.18235/0001150>
- Schumacher, I. (2013). Political stability, corruption and trust in politicians. *Economic Modelling*, 31(1), 359–369. <https://doi.org/10.1016/j.econmod.2012.11.047>
- Seiam, D. A., & Salman, D. (2024). Examining the global influence of e-governance on corruption: a panel data analysis. *Future Business Journal*, 10(1). <https://doi.org/10.1186/s43093-024-00319-3>
- Silal, P., Jha, A., & Saha, D. (2023). Examining the role of e-government in controlling corruption: A longitudinal study. *Information and Management*, 60(1). <https://doi.org/10.1016/j.im.2022.103735>
- Silal, P., & Saha, D. (2021). Impact of national e-participation levels on inclusive human development and environmental performance: The mediating role of corruption control. *Government Information Quarterly*, 38(4). <https://doi.org/10.1016/j.giq.2021.101615>
- Smith, M. L. (2011). Limitations to building institutional trustworthiness through e-government: A comparative study of two e-services in Chile. *Journal of Information Technology*, 26(1), 78–93. <https://doi.org/10.1057/jit.2010.17>
- Srivastava, S. C., Teo, T. S. H., & Devaraj, S. (2016). You can't bribe a computer: Dealing with the societal challenge of corruption through ICT. *MIS Quarterly*, 40(2), 511–526. <https://doi.org/https://doi.org/10.25300/misq/2016/40.2.14>
- Sung, C. S., & Park, J. Y. (2021). Understanding of blockchain-based identity management system adoption in the public sector. *Journal of Enterprise Information Management*, 34(5), 1481–1505. <https://doi.org/10.1108/JEIM-12-2020-0532>
- Todisco, L., Tomo, A., Canonico, P., Mangia, G., & Sarnacchiaro, P. (2021). Exploring social media usage in the public sector: Public employees' perceptions of ICT's usefulness in delivering value added. *Socioeconomic Planning Sciences*, 73, 100858. <https://doi.org/10.1016/j.seps.2020.100858>
- Transparency International. (2026). *Corruption Perceptions Index 2025*. <https://files.transparencycdn.org/images/CPI-2025-Report-EN.pdf>
- United Nations. (2022). *E-Government Survey 2022: The Future of Digital Government*. <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022>
- United Nations. (2023, May 2). *25% of global public spending is lost to corruption*. <https://news.un.org/es/story/2023/05/1520592>

- Wang, L., Luo, X. R., & Jurkat, M. P. (2022). Understanding Inconsistent Corruption Control through E-government Participation: Updated Evidence from a Cross-Country Investigation. *Electronic Commerce Research*, 22(3), 979–1006. <https://doi.org/10.1007/s10660-020-09444-x>
- Wawrosz, P. (2019). Productive of the Service Sector: Theory and Practice of Corruption Declining. *Marketing and Management of Innovations*, (4), 269–279. <https://doi.org/10.21272/mmi.2019.4-21>
- Wescott, C. G. (2001). E-Government in the Asia-Pacific region. *Asian Journal of Political Science*, 9(2), 1–24. <https://doi.org/10.1080/02185370108434189>
- Zhao, X., & Xu, H. D. (2015). E-government and corruption: A Longitudinal analysis of countries. *International Journal of Public Administration*, 38(6), 410–421. <https://doi.org/10.1080/01900692.2014.942736>
- Zheng, D., Chen, J., Huang, L., & Zhang, C. (2013). E-government adoption in public administration organizations: integrating institutional theory perspective and resource-based view. *European Journal of Information Systems*, 22(2), 221–234. <https://doi.org/10.1057/ejis.2012.28>