SCIENTIFIC CULTURE

www.sci-cult.com

*SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 15221-15237*
*Open Access. Online & Print*

**DOI: 10.5281/zenodo.20573342**

# RISK GOVERNANCE IN THE DIGITAL CULTURE OF COLOMBIAN SMART UNIVERSITIES

**Jovani Alberto Jiménez-Builes[1], Maria Antonia Nuñez[2] and Juan Alejandro Peña-Palacio[3]**

*[1]Research Group: Artificial Intelligence in Education, Department of Computer and Decision Sciences, Faculty of Mines, Universidad Nacional de Colombia, Email: jajimen1@unal.edu.co*
*[2]Research Group: Information and Management, School of Administration, EAFIT University, Email: mnunezpa@eafit.edu.co*
*[3]Research Group: Information and Management, School of Administration, EAFIT University, Email: japena@eafit.edu.co*

*Received: 04/04/2026*
*Accepted: 20/05/2026*

*Corresponding Author: Jovani Alberto Jiménez-Builes (jajimen1@unal.edu.co)*

## ABSTRACT

***This article examines the role of digital risk governance in shaping the transformation of higher education institutions into Smart Universities within the Colombian context. Grounded in a conceptual and documentary analysis of literature (2018-2025), international standards, and national public policies, the study explores how digital culture influences institutional exposure to technological, ethical, legal, organizational, and reputational risks. The research adopts a systemic perspective of risk governance, understood as a framework of decisions, actors, processes, and norms that enable the identification, assessment, management, and communication of risks in complex digital environments. It argues that digital transformation in universities cannot be reduced to technological adoption; rather, it involves a deep reconfiguration of organizational culture, leadership, and institutional capabilities. In this sense, digital culture is conceptualized as both an enabler of innovation and a source of new vulnerabilities, particularly in areas such as data governance, cybersecurity, artificial intelligence ethics, and institutional trust. The article identifies key challenges associated with fragmented digitalization, resistance to organizational change, lack of digital competencies, and insufficient alignment between institutional strategies and national regulatory frameworks. To address these challenges, it proposes a set of operational governance guidelines structured around policies, roles, control mechanisms, and performance metrics, enabling traceability between risk exposure and institutional decision-making. Furthermore, the study highlights the need for a human-centered and participatory governance approach aligned with emerging paradigms such as Industry 5.0, emphasizing ethical responsibility, sustainability, and stakeholder engagement. The findings contribute to bridging the gap between policy and practice by offering a contextualized framework for strengthening digital risk governance in Colombian higher education institutions, supporting resilient, inclusive, and accountable digital transformation processes.***

**KEYWORDS:** Digital Risk Governance; Smart Universities; Digital Culture; Higher Education; Artificial Intelligence Ethics; Digital Transformation; Industry 5.0.

## 1. INTRODUCTION

Smart universities represent an institutional response to broad processes of digital transformation. Their development implies incorporating advanced technologies to strengthen connectivity, automate tasks, and improve academic, research, and administrative management (Min-Allah & Alrashed, 2020). In higher education, this change requires organizational adjustments, governance structures capable of anticipating and managing emerging digital risks, and an institutional culture that places people, rather than platforms, at the center of transformation (Farrell et al., 2024; Gkrimpizi et al., 2023). This human-centered orientation is consistent with the principles of Industry 5.0, which emphasize human-machine collaboration and the use of technology to enhance creativity, well-being, and human capabilities (Nahavandi, 2019).

Even so, the transition towards smart university models does not advance uniformly. Institutions invest considerably in digital infrastructure, but organizational culture tends to change more slowly than technological adoption. This difference leaves relevant governance gaps in fields such as cybersecurity, data ethics, interoperability and institutional accountability (Brdesee & Alsaggaf, 2022). These gaps express deeper organizational vulnerabilities, which formal risk governance frameworks seek to address (Renn, 2008; Van Asselt & Renn, 2011). Recent literature on digital governance shows that governance outcomes depend largely on institutional response capacity, more than on technological capacity itself, and that this relationship varies according to regional and organizational contexts (Lund & Vildåsen, 2022; Zhu et al., 2025).

In Colombia, documented university experiences allow for the observation of this divergence in concrete institutional contexts. The Universidad Nacional de Colombia advanced in a participatory strategic model that reorganized the institutional vision and decision-making culture around digital transformation (Arango Serna et al., 2019). For its part, the Universidad Popular del Cesar shows that many Colombian higher education institutions still rely on fragmented use of information technologies (IT), with limited strategic orientation and persistent gaps in risk governance capacity (Molina, 2020). During the COVID-19 pandemic, universities in Medellín faced a significant increase in academic fraud in virtual environments, a situation that exposed the lack of systematic institutional controls against digital risk (Ríos-Avendaño et al., 2024).

This divergence between technological advancement and governance capacity leads to two central questions: (1) How does digital risk governance manifest in documented cases of university digital transformation, with special attention to the Colombian context? (2) What systematic lessons can be derived from the published evidence?

These questions acquire special relevance in Colombia, where the regulatory framework for digital transformation has advanced more rapidly than the institutional capacity to implement it. National policy instruments, including Decree 767 of 2022 and the Ministry of National Education's guidelines, assign explicit digital governance responsibilities to institutional committees and ICT units (MinTIC, 2022; MEN, 2021). Existing studies suggest that compliance with these frameworks remains irregular, while the organizational and cultural dimensions of digital transformation receive less institutional investment than that destined for technological infrastructure (Cardenas Ruiz et al., 2023; Gkrimpizi et al., 2023;).

Recent research has examined digital transformation in higher education from organizational (Faraj & Leonardi, 2022), pedagogical (Farrell et al., 2024), and public policy (Castañeda et al., 2023) perspectives. Digital risk governance has developed more in corporate and public administration settings (Sivan-Sevilla, 2021; Hassan et al., 2022; Stein & Wiedemann, 2016), whereas its analysis in universities of emerging economies remains less consolidated. In Colombia and Latin America, existing contributions concentrate on specific dimensions, such as strategic formulation, IT governance models and academic integrity risks. These experiences offer relevant contributions, but a synthesis that explains how digital risk governance is configured in different institutional cases and what patterns of challenge and response are repeated among them is still lacking (Arango Serna et al., 2019; Molina, 2020; Paredes Barrigas & Negrete Costales, 2025; Ríos-Avendaño et al., 2024).

To address this gap, the present study develops a systematic documentary analysis of published cases on digital transformation in Colombian universities, together with evidence from comparable Latin American institutional contexts. Based on risk governance theory (Renn, 2008; Stein & Wiedemann, 2016; Van Asselt & Renn, 2011), this analysis examines how institutional, cultural, and regulatory conditions influence digital risk governance in higher education. From this analysis, the study identifies common patterns of risk exposure, governance

response, and organizational outcomes.

## 2. THEORETICAL BACKGROUND

### *2.1. Smart Universities and Digital Transformation*

We can understand smart universities as higher education institutions that integrate digital infrastructures and services, data, and processes with governance structures and an organizational culture oriented towards the responsible use of digital technologies. This integration seeks to improve academic and administrative outcomes and sustain changes in teaching and management practices (Farrell et al., 2024; Gkrimpizi et al., 2023). In this perspective, the smart campus constitutes an operational subset of the smart university, in which technologies, policies, processes, and cultural values mediate the institutional effects of digitalization in seven dimensions: smart buildings, smart environment, smart mobility, smart life, smart people, smart governance, and smart data (Chagnon-Lessard et al., 2021; Min-Allah & Alrashed, 2020). Therefore, technological adoption depends on organizational capacities, explicit role definitions, and measurement systems that link risk exposure to decision-making (Chacón-Henao & Arias-Pérez, 2024; Faraj & Leonardi, 2022; Samara et al., 2025).

Digital transformation in higher education institutions is a sociocultural and organizational process that entails more than the mere incorporation of technological infrastructure (Benavides et al., 2020; Farias-Gaytan et al., 2023). Existing systematic reviews identify three successive levels of institutional change: the digital conversion of analog processes, the digitalization of organizational functions, and digital transformation, understood as an integral reconfiguration of institutional models, culture, and value creation (Gkrimpizi et al., 2023; Benavides et al., 2020). In higher education, these transformations are oriented towards improving service delivery and operational efficiency.

However, research consistently documents that the transition towards smart university models faces persistent organizational, strategic, and cultural barriers. A systematic review of 44 studies identified 20 specific barriers to digital transformation in higher education institutions, organized into six categories: environmental, strategic, organizational, technological, skills-related, and cultural (Gkrimpizi et al., 2023). Among the most documented barriers are the lack of digital literacy, resistance to change and risk aversion, insufficient strategic planning, and fragmented data architectures, including cybersecurity concerns and system integration challenges (Luo et al., 2024; Yucel, 2018). These elements provide the basis for examining institutional strategy and digital vision, as well as the organizational and cultural conditions that shape digital transformation in higher education.

### *2.2. Digital Risk Governance*

This study defines risk governance as the institutional configuration of policies, responsibilities, and processes through which institutions identify, assess, address, monitor, and communicate risks (Hassan et al., 2022; Renn, 2008; Stein & Wiedemann, 2016; UNDRR, 2023; Van Asselt & Renn, 2011). The literature defines it in two complementary ways: as a critical examination of complex networks of risk decision-making, and as a set of normative principles that guide relevant actors in the responsible management of risk (Renn & Graham, 2005; Van der Vegt, 2018). Unlike risk assessment, which operates at a technical-scientific level to identify and quantify risks, and risk management, which implements specific measures at the strategic-operational level, risk governance constitutes the institutional and regulatory framework that grants legitimacy, responsibility, and direction to both processes, by integrating stakeholder participation, transparency, and accountability mechanisms (Agarwal & Kallapur, 2018; Hassan et al., 2022; Klinke & Renn, 2002; Stein et al., 2019). Table 1 presents the operational definitions and controls associated with each type of digital risk in higher education institutions.

***Table 1: Typology Of Digital Risks in Heis: Operational Definitions, Controls, And Metrics.***

| Risk Type | Operational Definition | Measures / Controls | Metric |
|---|---|---|---|
| Technological (International Organization for Standardization, 2022) | Failures/threats to digital infrastructure and services | Information Security Management System, Business Continuity Plan / Disaster Recovery Plan, incident management | Incidents and recovery time |
| Ethical / AI (UNESCO, 2022) | Damage resulting from the use of AI / data without ethical standards | AI guidelines for teaching / research, Data Protection Impact Assessment – ethics | Percentage of courses with guidelines; bias reviews |
| Ethical (Hassan et al., 2022) | Mismatch in roles/processes / culture | Digital Governance Committee, RACI matrix (Responsible, Accountable, Consulted, Informed), training | Percentage of processes with designated responsible parties |

| | | | |
|---|---|---|---|
| Legal/Privacy (Renn, 2008; Van Asselt & Renn, 2011) | Non-compliance with regulations and personal data protection | Data policy, access controls, activity logging | Compliance findings; audits |
| Institutional Image (Heeks, 2022) | Erosion of trust due to digital incidents | Incident reporting protocol | Response time; impact on reputation |
| Financial | Losses due to disruptions / inefficiency | Cyber insurance, segregation of duties | Avoided losses / benefits |

**Source: Author's Own Work.**

The literature on data governance broadens the risk governance perspective by addressing the specific challenge of governing institutional data as a strategic asset exposed to risks. Abraham et al. (2019), in a structured review of 145 publications, identify six central dimensions of data governance applicable to organizations: governance mechanisms (structural, procedural, and relational), organizational scope, data scope, domain scope, antecedents, and consequences. In higher education, this framework operationalizes risk governance through measurable constructs: decision rights and data accountability; data policies and standards; compliance monitoring; and mechanisms to manage problems (Stojanov & Daniel, 2024). In the Colombian context, studies such as Arango Serna et al. (2019) show that the maturity of digital culture requires aligning internal guidelines with specific sectoral regulations, for example, the policies of the Ministry of Information and Communications Technologies (MinTIC) and the Ministry of National Education (MEN), and with the actual capacities of higher education institutions.

Digital risk governance in higher education institutions operates in a space of uncertainty where institutions must balance openness, security, and autonomy. From the risk governance perspective, this balance requires well-reasoned decisions, clear roles, and measurable processes (Renn, 2008; Van Asselt & Renn, 2011). This perspective supports the analysis of digital risk exposure, institutional response, and the governance arrangements through which universities assign responsibilities, monitor compliance, and manage institutional vulnerabilities.

### *2.3. Artificial Intelligence in Higher Education*

The integration of artificial intelligence and learning analytics in university environments introduces particular governance challenges that exceed conventional risk frameworks. A meta-systematic review of 66 evidence syntheses on AI in higher education identifies a recurring need for greater ethical consideration, methodological rigor, and contextual sensitivity, particularly regarding student data, algorithmic bias, and institutional accountability (Bond et al., 2024). For the Colombian context, AI governance has evolved from the initial framework of CONPES 3975 towards the recent roadmap established in CONPES 4144 (DNP, 2025). Despite these regulatory advances, the risk persists of adopting standards from developed countries while ignoring local regulatory, cultural, and infrastructure particularities, which hinders their effective implementation in institutions (Thaldar et al., 2025).

A systematic review of FATE (Fairness, Accountability, Transparency, and Ethics) in AI and higher education finds that the majority of empirical research focuses on algorithmic fairness. In contrast, accountability and transparency have received less comparative attention (Memarian & Doleck, 2023; Jobin et al., 2019). The FATE framework offers an operative vocabulary to translate abstract ethical principles into institutional governance structures: fairness requires that AI systems do not systematically discriminate based on demographic attributes; accountability assigns institutional responsibility for decisions generated by AI; transparency requires that institutions make both the use and the decision logic of these systems accessible to affected actors; and ethics articulates these elements within an organizational culture oriented towards the responsible use of AI.

A case study on AI governance guidelines in fourteen Big Ten universities in the United States shows that the most effective governance approaches combine the participation of various units, such as IT departments, teaching and learning units, university libraries and AI-dedicated centers; role-specific guidance, with differentiated expectations for faculty, students, researchers and administrative staff; and a formative and guiding approach that emphasizes digital literacy more than strict enforcement of rules (Wu et al., 2024). This result contrasts with purely prescriptive frameworks and suggests that institutional governance of AI in higher education works better when it strengthens organizational capacity while also defining institutional rules.

The three reviewed literature blocks converge on a common point: digital risk governance in higher education requires technical controls, formal policies, and, simultaneously, institutional strategic guidance, organizational capacity to manage specific risks, cultural conditions that enable change, and ethical principles that regulate the use of data and AI. This

convergence informs the four analytical dimensions of the present study, structures the documentary analysis, and underpins the governance framework discussed in the following sections.

Figure 1 below presents a classification of the categories associated with digital challenges, followed by a detailed description of the key elements to consider within each category, with the aim of strengthening a university's risk management system and, consequently, defining guidelines and directives for its governance. The identified elements were consolidated as a result of the literature review conducted (Brdesee & Alsaggaf 2022; Faraj & Leonardi, 2022; Farrell et al., 2024; Nugraha & Syaidah, 2022; Samara et al., 2025).

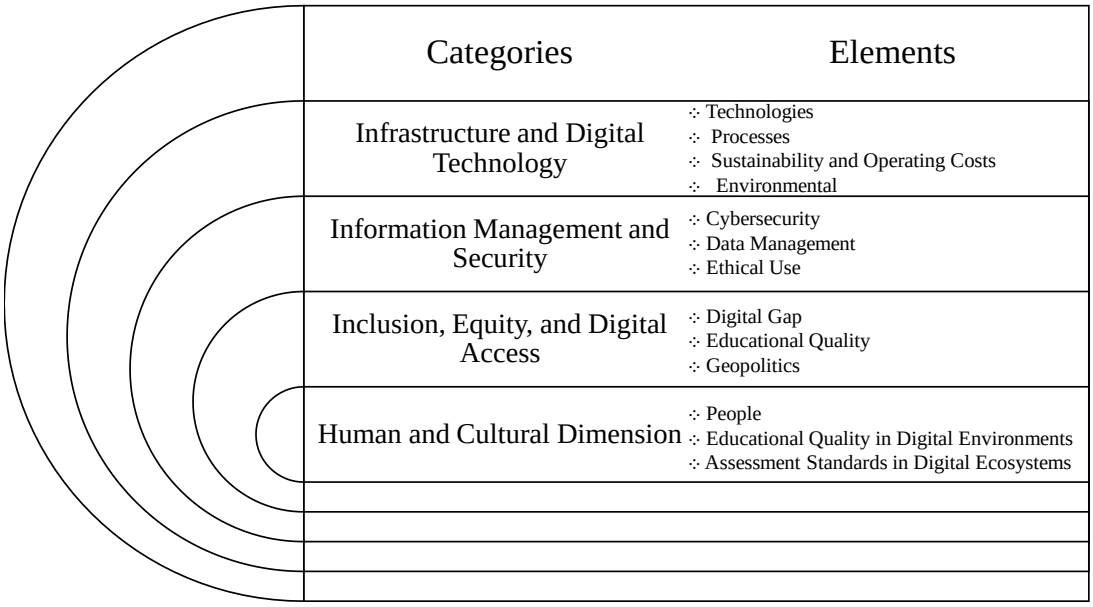


***Figure 1: Classification Of Digital Risk Categories.***
**Source: Author's Own Work.**

## 3. MATERIALS AND METHOD

### *3.1. Research Design*

This study adopts a systematic documentary analysis and intentional case selection as its research design. This approach combines a structured search of academic and policy-related literature with the deliberate identification of institutional cases that meet criteria of empirical soundness and analytical relevance (Benavides et al., 2020; Gkrimpizi et al., 2023). Following this design, the study examines patterns of digital risk governance in documented institutional contexts, drawing on evidence from case studies, institutional reviews, and public policy evaluations. The analytical procedure applies explicit criteria for search, selection, inclusion, exclusion, and coding to ensure methodological consistency across cases.

### *3.2. Search Strategy*

We conducted a structured search in Scopus and Web of Science (WoS) for the period 2018–2025. Four complementary search strings were designed through a keyword reconstruction process based on the study's conceptual framework, covering four thematic groupings: (1) digital governance and institutional transformation in higher education; (2) empirical and documentary evidence on digital transformation in universities; (3) studies focused on the Colombian and Latin American regional context; and (4) ethical governance of artificial intelligence and learning analytics in higher education. For each string, the search strategy combined English- and Spanish-language terms related to risk governance, higher education, digital transformation, learning analytics, artificial intelligence ethics, and personal data protection. For String 4, we restricted the search to the title field in both databases to avoid including studies that referenced ethical concepts only peripherally in their abstracts.

To broaden the documentary corpus, we complemented the search with international standards from the International Organization for Standardization (ISO) and ethical frameworks from the United Nations Educational, Scientific and Cultural Organization (UNESCO), as well as relevant Colombian policies, such as CONPES 3975/2019, Decree 767/2022, Law 1581/2012, and guidelines from the Ministry of National Education (MEN). The four search strings yielded a combined total of 454

records across both databases: 328 in Scopus and 126 in Web of Science. After eliminating duplicates through cross-database comparison, we retained 341 unique records for the screening phase.

### 3.3. Inclusion And Exclusion Criteria

Inclusion criteria were defined in advance and included the following: peer-reviewed status; direct relevance to higher education or public-sector digitalization; focus on governance arrangements, digital risk, organizational culture, or artificial intelligence ethics in institutional contexts; and full-text availability. For case-level selection, we applied an additional criterion. We included studies as analytical cases only when they reported documented institutional experiences with sufficient detail to examine governance dimensions, outcomes, or lessons learned.

We excluded documents that consisted primarily of opinion pieces, essays without analytical or empirical grounding, or texts not substantively related to digital governance, digital transformation, or risk management in higher education settings.

We conducted the screening process in two phases. In the first phase, we reviewed the titles and abstracts of the 341 unique records to assess their alignment with the inclusion criteria, excluding 271 records and retaining 70 for full-text assessment. In the second phase, we reviewed the full text of the retained records to confirm their analytical relevance and assess the quality and specificity of the reported evidence. This phase excluded 34 records, yielding a final corpus of 36 peer-reviewed studies that informed the analytical framework and discussion.

Figure 2 illustrates the document selection process following the PRISMA protocol, adapted for systematic documentary analysis.

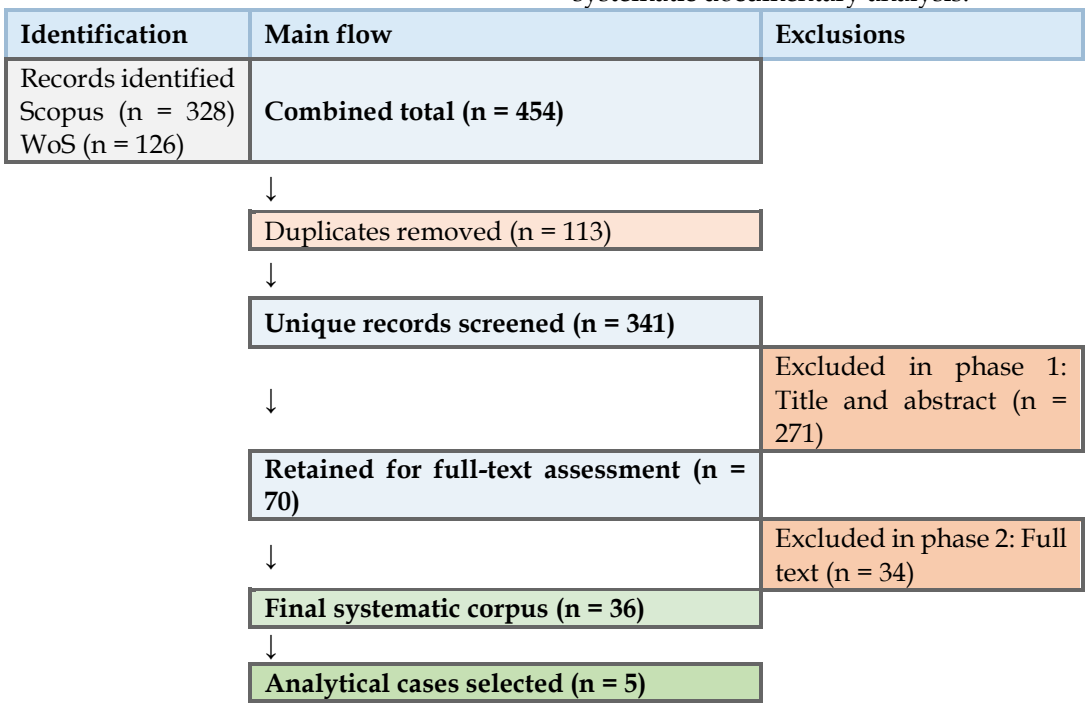


*Figure 2: Flow Diagram of the Document Selection Process (Adapted From PRISMA).*
**Source: Author's Own Work.**

### 3.4. Case Selection Criteria and Selected Cases

From the corpus of studies retained after full-text review, an intentional selection process identified the studies we would analyze as institutional cases. Six explicit criteria guided this selection: (a) Availability of published peer-reviewed evidence describing institutional experiences. (b) Explicit documentation of at least one governance dimension: institutional strategy, digital risk exposure and response, organizational culture and resistance to change, or ethical governance of data and artificial intelligence. (c) Higher education institutional context: public or private universities. (d) Publication within the search window 2018–2025. (e) For Colombian cases, the source study referenced or allowed verification of alignment with the regulatory frameworks of the Ministry of Information and Communications Technologies (MinTIC) and the Ministry of National Education (MEN). (f) For comparative cases: Latin American institutional context presenting governance challenges structurally comparable to those of Colombian higher education institutions, as described in the source study.

Five studies met all applicable criteria; therefore, we selected them as analytical cases. Three correspond to the Colombian context, which constitutes the main focus of the study, and two contribute regional comparative evidence from Ecuador and Peru. Four sources are peer-reviewed publications, while one source — Molina (2020) — corresponds to a master's thesis deposited in an institutional repository. We retained it as grey literature because it provides the only documented operational assessment of IT governance maturity at a Colombian public university. Table 2 presents the selected cases with their main institutional characteristics.

***Table 2: Cases Selected for Systematic Documentary Analysis.***

| University | Country | Documented initiative | Period | Governance dimension | Source |
|---|---|---|---|---|---|
| Universidad Nacional de Colombia | Colombia | Gran Partenón model: participatory digital governance | 2019 | DA1, DA3 | Arango Serna et al. (2019) |
| Universities in Medellín | Colombia | Academic fraud risk management in virtual environments | 2024 | DA2, DA4 | Ríos-Avendaño et al. (2024) |
| Universidad Popular del Cesar | Colombia | IT governance diagnosis and risk management model | 2020 | DA1, DA2 | Molina (2020) |
| Universidad Nacional de Chimborazo | Ecuador | Institutional digital transformation plan | 2025 | DA1, DA2, DA3 | Paredes Barrigas and Negrete Costales (2025) |
| Two private universities | Peru | Knowledge management and organizational digitalization | 2021 | DA3, DA4 | Arias Velásquez and Mejía Lara (2021) |

**Source: Author's Own Work.**

### *3.5. Analytical Dimensions of the Study*

This study examines digital risk governance in higher education through a systematic documentary analysis of published cases. The analytical framework structures the analysis around four dimensions derived from the convergence between risk governance theory (Renn, 2008; Van Asselt & Renn, 2011), data governance frameworks (Abraham et al., 2019; Garcés-Ordóñez & González-Zabala, 2021), and the literature on artificial intelligence (AI) ethics and digital transformation reviewed in Section 2. We read each case in its entirety and coded it according to the four analytical dimensions.

**Coding procedure.** Coding proceeded in two rounds after a full reading of each case. In the first round, source text segments associated with institutional decisions, mechanisms, outcomes, or challenges corresponding to the four analytical dimensions were identified and recorded. In the second round, the consistency of the initial coding was reviewed, and the classification of evidence was refined in relation to the theoretical framework. Only elements explicitly documented in the analyzed sources were recorded. Sections 4 and 5 present the synthesis of cross-case patterns.

Analytical Dimension 1 (DA1): institutional strategy and digital vision. Examines whether each institution articulates an explicit strategic orientation towards digital transformation and in what way it does so, as well as what role governance structures play in that orientation. The absence of holistic strategic planning is among the most frequently documented barriers to effective digital transformation in higher education institutions (Gkrimpizi et al., 2023), and effective governance requires alignment between senior management and digital strategy (Cardenas Ruiz et al., 2023). This analysis allows for diagnosing institutional governance capacity.

Analytical Dimension 2 (DA2): digital risk exposure and institutional response. DA2 identifies the specific categories of digital risk documented in each case—technological, ethical, organizational, legal, or reputational—and examines the formal mechanisms each institution deploys to identify, assess, address, and monitor those risks, following the typology established in Table 1 of the theoretical framework.

Analytical Dimension 3 (DA3): organizational culture and resistance to change. Examines the human and cultural dimensions of digital transformation, including documented patterns of resistance, digital literacy gaps, and the degree to which institutional processes support meaningful stakeholder participation (Deacon et al., 2025; Gkrimpizi et al., 2023).

Analytical Dimension 4 (DA4): ethical governance of data and artificial intelligence. Examines the degree to which institutions integrate FATE principles into their operational governance of data and artificial intelligence systems, including the presence of data protection policies, algorithmic oversight arrangements, and frameworks for the

responsible use of AI (Memarian & Doleck, 2023; UNESCO, 2022; Wu et al., 2024).

We read each case in its entirety and coded it according to the four analytical dimensions. We recorded evidence when a study explicitly described institutional decisions, mechanisms, outcomes, or challenges associated with a given dimension. Sections 4 and 5 present the synthesis of cross-case patterns.

## 4. RESULTS

### *4.1. Institutional Strategy and Digital Vision (DA1)*

The two Colombian cases examined under this dimension show a pattern: digital transformation efforts develop without a general institutional governance framework that integrates technological adoption with organizational and cultural change.

In the Colombian context, the Universidad Nacional de Colombia recognized the importance of promoting participatory digital governance as a strategy to anticipate emerging risks (Arango Serna et al., 2019). The Gran Partenón model represents one of the few documented cases in the Colombian higher education system that explicitly frames digital transformation as an institutional strategic process that involves prospective analysis, stakeholder prioritization, and leadership alignment. Arango Serna et al. (2019) report that the model organized the university's digital vision around five axes (connectivity, digital culture, data governance, innovation, and institutional services) and assigned explicit responsibilities to academic units for its implementation. Relevantly, the model treated organizational culture as a governance variable that requires active management. This experience shows that digital transformation strategies go beyond technological adoption, as they imply a deep reconfiguration of organizational culture, and these processes require governance structures capable of integrating digital innovation with institutional strategic vision.

In contrast, the diagnosis conducted at the Universidad Popular del Cesar reveals what occurs in the absence of such a framework. Molina (2020) documents that the majority of higher education institutions in Colombia use information technology in a fragmented manner and with limited strategic direction, which underscores the need for IT governance models with risk management to advance beyond basic use and create academic and organizational value. The study found no unified data governance structure, no explicit assignment of decision-making authority over digital resources, and no performance indicators linking technological investments with institutional outcomes — conditions that correspond directly with the structural and strategic barriers identified by Gkrimpizi et al. (2023) in their systematic review of 44 cases of higher education institutions at the international level.

The comparative case of the Universidad Nacional de Chimborazo in Ecuador confirms this pattern from a different institutional trajectory. Paredes Barrigas and Negrete Costales (2025) document what they describe as "digitalization islands": isolated advances in infrastructure and systems that lacked coordination due to the absence of an institutional digital transformation plan and change management capacities. The institution had invested in technology across multiple units without a governance framework that aligned these investments with a shared institutional vision, which produced operational fragmentation rather than strategic transformation. This evidence suggests that the challenge is both technical and organizational, as well as cultural.

Across the three cases, the evidence points to a common governance gap: institutions that advance in digital infrastructure without a corresponding development of institutional architecture for decision-making (formal committees, role matrices, performance cycles) lack the coordination mechanisms necessary to manage digital risks as they emerge.

### *4.2. Digital Risk Exposure and Institutional Response (DA2)*

The evidence reviewed in DA2 shows that, in the Colombian cases, institutions recognize different digital risks, but do not yet have sufficiently consolidated mechanisms to manage them. While these institutions identify risks in institutional documents, policies, or diagnoses, they have yet to fully develop actions for assessing, monitoring, communicating, and responding to them.

The most detailed empirical account of risk exposure in a Colombian higher education institution comes from Ríos-Avendaño et al. (2024), whose qualitative study on risk management practices in universities in Medellín examined academic fraud as a category of digital risk that increased with the transition to virtual environments during the COVID-19 pandemic. The study identified seven recurring typologies of fraud (plagiarism, hiring third parties to carry out academic work, identity impersonation, false certification, answer exchange, simulated virtual

attendance, and unauthorized use of technology). It documented their associated causes, ranging from the normalization of improper conduct and the insufficient application of regulations to specific cultural factors in the Medellín context. The study classified institutions' controls into preventive, corrective, and review controls, and included plagiarism-detection tools, pedagogical diversification of assessments, and institutional integrity campaigns. However, the study found that the analysis and assessment phase represented the most significant governance gap: institutional decisions on fraud risks were handled intuitively, rather than through formal instruments, and no systematic monitoring mechanisms existed to evaluate whether the deployed controls effectively reduced exposure to inherent risk (Ríos-Avendaño et al., 2024). Academic regulations proved reactive and punitive rather than adaptive and had not been updated to address the specific fraud patterns enabled by technology-mediated learning environments.

The IT governance diagnosis at the Universidad Popular del Cesar documents a different, but structurally related, pattern of risk exposure. Molina (2020) reports that the institution had assessed thirteen risk categories through an institutional risk matrix, covering infrastructure obsolescence, unauthorized access to systems, errors in production code, data loss due to malware, inadequate operation, service interruption due to communication failures (connectivity), misuse of administrator roles, and business continuity interruption, among others. The maturity assessment in five phases (identification, detection, protection, response, and recovery) showed that the identification phase reached the highest maturity level, while the remaining phases revealed significant gaps. Critically, the study concludes that the institution lacks a robust structural risk management framework to raise maturity in subsequent phases. Currently, IT governance is limited to an operational role, with no indicators linking technological investments with institutional objectives.

In both cases, the evidence points to a governance gap that goes beyond simple risk identification. Although Colombian institutions catalog digital threats and implement specific controls, they lack the analytical infrastructure — probabilistic instruments, responsibility matrices, and alert protocols — necessary for continuous and adaptive management. This finding is consistent with Renn's (2008) distinction: institutions locate hazards (identification), but omit the structured assessment of probability and impact (evaluation).

### *4.3. Organizational Culture and Resistance to Change (DA3)*

The cultural and organizational dimension of digital transformation constitutes one of the most persistent governance challenges in the reviewed cases. The evidence shows that resistance to change is primarily associated with institutional conditions, such as resource constraints, insufficient change management strategies, and difficulties in coordination and trust between areas during accelerated digitalization processes.

The most detailed analysis of cultural barriers in the reviewed cases is by Paredes Barrigas and Negrete Costales (2025) at the Universidad Nacional de Chimborazo. Based on interviews, the study shows that budget constraints, insufficient infrastructure, and low institutional priority for digital spending constrained digital transformation. Although the university implemented technologies over approximately 20 years, these advances were incremental and lacked a specific digital transformation plan that articulated investment, leadership, and governance. The study also links resistance to change with available training, suggesting that technological adoption depended on sustained training, socialization, and induction processes, in addition to institutional leadership commitment.

The evidence from Arias Velásquez and Mejía Lara (2021) shows that digitalization can strengthen some dimensions of organizational capital while weakening others. In two Peruvian private universities, the COVID-19 pandemic strengthened the faculty collaboration network: connections increased 2.5 times, and organizational learning indicators improved. However, the links between students and the university weakened. Student loyalty and commitment decreased, and only 40% of students expressed intention to continue in the following semester. This finding shows that digital transformation governance frameworks that focus primarily on operational efficiency often omit interpersonal bonds and community fabric, elements that are fundamental to ensuring student retention and knowledge transfer.

Resistance to change, associated with work overload, fear of losing pedagogical control, and disagreements over teaching autonomy, poses a latent risk that can weaken the effectiveness of digital initiatives when institutions do not address it through participation and recognition strategies

(Deacon et al., 2025). The evidence supports Gkrimpizi et al.'s (2023) finding that cultural barriers are among the most frequent obstacles to digital transformation in higher education institutions, particularly conservative institutional cultures, weak links between academic units, and teaching-workload constraints. However, these obstacles tend to receive less formal attention in institutional governance documents.

### *4.4. Ethical Governance of Data and Artificial Intelligence (DA4)*

This dimension presents the least documented evidence in the reviewed cases. This absence constitutes a relevant finding, because it shows that institutions have advanced more in security, operational continuity, and technological management than in explicit criteria to guide the ethical use of data and intelligent systems.

None of the five case reports has an explicit institutional framework to govern data and artificial intelligence in line with the FATE principles (fairness, accountability, transparency, and ethics). The closest approximation appears in Molina (2020), which includes the ethical use of information systems as a risk category in the institutional matrix, alongside unauthorized access and data loss. However, the study does not document specific mechanisms to address that category. The reviewed documents do not identify data protection policies with assigned responsibilities, oversight schemes for digital systems, or criteria to evaluate whether the institutional use of technology protects user rights or produces equitable outcomes. In digital culture, openness contributes public value but increases exposure to privacy and service continuity risks when not accompanied by impact assessments and proportional controls (ISO, 2022). For its part, academic autonomy coexists with the need for standardization to ensure traceability, compliance, and security (Hassan et al., 2022; UNESCO, 2022).

Paredes Barrigas and Negrete Costales (2025) document that the Universidad Nacional de Chimborazo adopted ISO 27001 as the reference standard for information security and implemented internal data protection policies. Nevertheless, the study shows that these measures primarily focus on cybersecurity and operational continuity rather than ethical governance. The institution's expert informant acknowledged that, although information security exists as an institutional concept, more robust security requires external evaluation. The informant also noted that the digital divide among users raises pending questions about equitable access and use of digital systems. Recent data from the region show concerns among faculty and students about privacy, transparency, and algorithmic biases of AI, reinforcing the need for specific governance frameworks (Marín et al., 2025).

This gap in the reviewed evidence coincides with findings in institutions with greater resources. A study on artificial intelligence governance guidelines at 14 Big Ten universities in the United States found that, even in well-funded institutions, accountability and transparency remain the least operationally developed FATE dimensions. Governance documents tend to define principles but often fail to specify who implements them, who monitors compliance, or which redress mechanisms are available to affected users (Wu et al., 2024). A systematic literature review on FATE in higher education confirms this tendency: the majority of empirical work concentrates on algorithmic fairness, while accountability and transparency receive less institutional attention (Memarian & Doleck, 2023). In contexts such as Colombia, where regulatory frameworks on data protection (Law 1581 of 2012) and digital transformation (Decree 767 of 2022) assign explicit institutional responsibilities, the absence of documented mechanisms for the ethical use of data suggests that compliance remains more formal than operational (CRC, 2012).

The governance gap in this dimension persists as Colombian universities intensify the implementation of learning management platforms, educational analytics, and artificial intelligence-assisted assessment systems. Without explicit frameworks on who authorizes these tools, what data they process, who audits their results, and how students and faculty can question decisions that affect them, institutions remain exposed to reputational, legal, and ethical risks. The literature identifies these risks as emerging threats to the digitalization of higher education (Bond et al., 2024; Thaldar et al., 2025; Williamson et al., 2020).

### *4.5. Cross-Case Analysis and Propositions for Digital Governance*

The comparison among the five cases allows for the formulation of four analytical propositions. These propositions emerge from each dimension in a connected manner, with relationships between institutional strategy, risk management, organizational culture, and ethical governance in the examined contexts.

First proposition: A more mature digital strategic vision does not guarantee more developed ethical governance.

Among the five cases, the Universidad Nacional de Colombia is the only one to document an explicit institutional architecture for digital transformation, with defined axes, assigned responsibilities, and the treatment of organizational culture as a governance variable (DA1). However, the institution did not translate that strategic advance into operational frameworks to guide the ethical use of data or artificial intelligence (DA4). The absence of documented ethical governance appears in all cases, even in those with greater strategic development. This decoupling suggests that strategic governance and ethical governance can advance through different institutional paths. The former appears to depend on leadership decisions and planning; the latter requires normative conditions, internal demands, or specialized capacities that, in the reviewed cases, are not yet clearly observable.

Second proposition: Identifying digital risks does not guarantee the institutional capacity to assess and monitor them.

The Universidad Popular del Cesar and the universities in Medellín show that institutions can catalog risks through institutional matrices or academic fraud typologies, but do not yet have instruments to estimate their probability, monitor controls, or adjust institutional responses (DA2). In these cases, the main limitation does not appear to be technical, but organizational. When formal decision structures, defined responsible parties, and performance cycles linked to risk management do not exist (DA1), systematic assessment lacks a clear space to become institutionalized. The case of the Universidad Popular del Cesar illustrates this situation: the institution had a risk matrix with 13 categories but lacked sufficient governance processes to advance beyond identification.

Third proposition: cultural resistance to digital change is related to organizational conditions, especially when institutional strategy is weak.

The cases of the Universidad Nacional de Chimborazo and the Peruvian universities show two expressions of this problem. At the Universidad Nacional de Chimborazo, the evidence links resistance to budget constraints, leadership gaps, and the absence of a transformation plan that articulated investment and governance (DA3 conditioned by DA1). At the Peruvian universities, accelerated digitalization strengthened faculty collaboration networks but weakened the links between students and the university, with effects on retention and institutional commitment. In both cases, strategies focused only on individual training proved insufficient because they did not address the organizational conditions that sustained or limited change. This relationship connects DA3 with DA1: when the governance architecture does not actively manage cultural change, resistance remains as a poorly controlled institutional risk.

Fourth proposition: Advances in cybersecurity do not substitute ethical governance of data and digital systems.

The Universidad Nacional de Chimborazo adopted ISO 27001 and implemented internal data protection policies oriented towards operational continuity and cybersecurity. These measures constitute the most documented advance in DA2 among the reviewed cases. Nevertheless, the same case acknowledges that the digital divide among users raises questions about equitable access and use that those controls do not resolve. Information security protects systems, data, and infrastructure; ethical governance, in contrast, defines criteria on rights, transparency, equity, and responsibility in the institutional use of technology. This difference shows that existing regulatory frameworks, such as Law 1581 of 2012 in Colombia or ISO standards, guide formal compliance but do not always offer sufficient criteria for determining who authorizes analytics or artificial intelligence systems, what data they process, who reviews their results, and who can question decisions derived from those systems.

By connecting these propositions, weakness in DA1 limits management capacity in DA2; insufficient organizational conditions reduce the effectiveness of strategies in DA3; and advances in technical security do not replace the ethical frameworks required in DA4. This reading has practical implications: intervening in a single dimension without attending to its relationships with the others can reproduce the fragmentation shown by the reviewed cases.

## 5. DISCUSSION

### *5.1. Research Findings*

The systematic documentary analysis of five cases shows that digital risk governance in Colombian and Latin American higher education institutions generally operates as a reactive function, centered on regulatory compliance and risk categorization. The evidence shows a lesser consolidation of institutional capacities to anticipate, assess, and adjust responses to those risks. In the digital era, mitigating risk requires more than technical solutions: it requires distributed governance, ethical leadership, and institutional commitment to digital transformation. In the examined cases, this change still appears incomplete and, in some cases, incipient.

The four analytical propositions identified in

section 4.5 are consistent with what Gkrimpizi et al. (2023) document in 44 cases of higher education institutions at the international level. In the reviewed cases, strategic weakness (DA1) limits risk assessment (DA2); organizational conditions influence cultural resistance (DA3); and greater strategic maturity does not ensure more developed ethical governance (DA4). These relationships appear in both the international literature and the Colombian and Latin American cases examined. The study also shows that the main gap is not in recognizing digital risks, but in having mechanisms to assess, monitor, and adjust institutional responses over time. Given that no single balance among openness, security, and autonomy exists, each institution must define its approach based on its risk exposure and periodically review it through performance metrics (Hassan et al., 2022).

### *5.2. Theoretical Contributions*

This study contributes to the regional literature on digital governance in higher education in two specific ways. First, it applies the risk governance framework of Renn (2008) and Van Asselt and Renn (2011), developed primarily in the context of environmental and public policy risk, to the analysis of institutional digital transformation in higher education. This application allows distinguishing between governance understood as compliance and governance understood as adaptive capacity. The four analytical dimensions used in the study — institutional strategy, risk exposure and response, organizational culture, and ethical governance of data and artificial intelligence — offer a framework that can guide similar analyses in other institutional contexts in the region.

Second, the study shows how the gap between digital policy and institutional practice manifests itself in Colombia, a context in which national instruments assign explicit responsibilities for digital governance. However, compliance with those instruments does not always translate into the organizational and cultural changes that effective governance requires. This finding aligns with the observations of Zhu et al. (2025) and Lund and Vildåsen (2022) on the uneven territorial diffusion of digital governance. It situates them in the institutional domain of higher education. In this context, differences in governance capacity between institutions depend not only on available resources but also on organizational readiness and cultural conditions.

### *5.3. Practical Implications*

The findings point to three priority areas for institutional action. The first is the articulation between policy and practice. The evidence supports the need for institutional digital transformation plans aligned with national strategies, such as CONPES 3975, Decree 767 of 2022, and the MEN guidelines, with interoperability as an architectural criterion and the systematic evaluation of projects within governance cycles (DAFP, 2024; DNP, 2019; MinTIC, 2022; Paredes Barrigas & Negrete Costales, 2025). When institutions do not connect risk prioritization, resource allocation, change management, and accountability through verifiable indicators, they produce fragmented forms of digitalization and reinforce technological dependence.

The second area corresponds to academic integrity and digital risk. The evidence from Ríos-Avendaño et al. (2024) suggests that institutional programs that combine policies, verification procedures, and ethical training are more effective than responses that focus solely on sanctions or technological tools. At this point, the main weakness in many Colombian institutions appears to be the lack of concrete monitoring indicators.

The third area relates to data and artificial intelligence governance. Institutional oversight arrangements, such as committees with defined responsibilities, algorithmic review protocols, and digital literacy programs for faculty and students, can reduce exposure to legitimacy and legal risks associated with learning analytics and artificial intelligence-assisted assessment (Osorio et al., 2024; UNESCO, 2022; Wu et al., 2024). Furthermore, organizational evidence shows that resistance to change requires participatory processes and institutional recognition of staff who lead technological adoption, rather than top-down mandates (Deacon et al., 2025).

Table 3 summarizes the three priority action areas, the analytical dimensions from which they derive, the recommended mechanisms, and the suggested monitoring indicators, to support their adoption as an institutional diagnostic and planning instrument.

***Table 3: Digital Risk Governance Framework for Smart Universities: Action Areas, Mechanisms, And Indicators.***

| Action area | Source AD | Recommended mechanism | Suggested indicator |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Policy–practice articulation | AD1, AD2 | Digital governance committee; annually reviewed risk matrix | % of digital processes with an assigned responsible party; no. of IT indicators linked to institutional objectives |
| Academic integrity and digital risk | AD2, AD4 | Incident monitoring protocol; revision of academic regulations | No. of incidents recorded by typology; effectiveness rate of preventive controls |
| Ethical governance of data and AI | AD4 | FATE criteria for AI authorization; redress mechanisms; impact assessments | % of platforms with completed impact assessment; no. of algorithmic reviews per period |

**Source: Authors Own Work.**

### *5.4. Limitations And Future Research*

This study presents several limitations. We selected the five cases for their evidential richness and not for their institutional representativeness. Furthermore, the sources vary in methodological depth, especially Molina (2020), which we retained as grey literature in the absence of a peer-reviewed equivalent for that governance dimension. Therefore, the findings do not allow generalization to the Colombian higher education system as a whole. The evidence allows describing recurring relationships across different institutional types, national contexts, and study periods, as well as pointing to gaps where further research is required.

Primary data collection, through institutional document audits, interviews with governance actors, or longitudinal surveys on risk management maturity, would allow evaluating the depth of governance beyond what is reported in published sources. Cross-country comparisons within Latin America would also be useful for establishing whether the identified gaps are driven by Colombia-specific regulatory conditions or by broader regional dynamics in the digital governance of higher education. Finally, given the advances of generative artificial intelligence in university environments, future studies could analyze how institutions develop, adapt, or leave pending ethical governance frameworks for these tools in real time (Osorio et al., 2024).

## 6. CONCLUSIONS

Digital transformation strategies in Colombian universities, oriented towards adopting smart models, entail more than simply incorporating technology. Their scope depends on the institutional capacity to adapt organizational culture, reorganize internal structures, and strengthen an integral, adaptive, and participatory risk governance. The systematic documentary analysis conducted in this study shows that the most recurring governance gaps across the five cases are primarily related to organizational and cultural conditions that technical frameworks, on their own, are unable to resolve.

The study shows that Colombian higher education institutions have the capacity to identify digital risks and formulate regulatory compliance mechanisms. However, they have not yet consolidated a monitoring and evaluation infrastructure sufficient to sustain effective governance. Cultural resistance to change is associated with budget constraints and leadership gaps, as well as with individual attitudes towards technology. Likewise, the ethical governance of data and artificial intelligence (AI), exposed to emerging risks arising from learning analytics and generative AI, appears to be the least developed dimension in the reviewed cases. In the Colombian context, Arango Serna et al. (2019) document advances towards participatory strategic models that can guide this type of transformation. Even so, these developments reveal gaps in the assessment of vulnerabilities and their impact, in the active inclusion of students, and in the systematization of documented institutional experiences.

Three policy recommendations derive from these findings. First, Colombian universities should develop specific digital transformation plans, distinct from general strategic plans, that include explicit governance cycles: risk prioritization, resource allocation, change management, and accountability through verifiable indicators aligned with CONPES 3975 and Decree 767 of 2022. Second, institutional risk management should go beyond catalog-based approaches and incorporate instruments to estimate probability and impact, monitoring protocols on the effectiveness of controls, and periodic review mechanisms that connect governance decisions with observed outcomes. Third, as AI adoption expands in university environments, institutions should establish formal oversight frameworks for data and AI systems, including defined roles, transparency requirements, and audit procedures, before deploying them at scale and not only reactively in response to already materialized problems.

This governance requires transforming technocratic visions into ethical, contextually grounded management models. Its strength demands institutional capacity to integrate the human factor, organizational dialogue, and sustainability as guiding principles. These lessons are not exclusive to the Colombian context. Institutions in comparable Latin American environments with similar regulatory and organizational conditions will

likely exhibit similar governance patterns.

## 7. DECLARATIONS

### *7.1. Declaration Of Conflicts Of Interest*

The authors declare that there are no conflicts of interest related to the research, authorship, or publication of this article.

### *7.2. Ethical Considerations*

This article is conceptual in nature and is based on public and academic documentary sources; it did not involve interaction with individuals or the collection of personal data. Consequently, it did not require approval from an ethics committee. The principles of academic integrity (attribution of authorship, citation, and honest use of information) were respected, and data protection was observed by avoiding the processing of sensitive or identifiable information.

## REFERENCES


Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

Agarwal, R., & Kallapur, S. (2018). Cognitive risk culture and advanced roles of actors in risk governance: A case study. *The Journal of Risk Finance*, 19(4), 327-342. https://doi.org/10.1108/JRF-11-2017-0189

Arango Serna, M. D., Branch, J. W., Castro Benavides, L. M., & Burgos, D. (2019). Un modelo conceptual de transformación digital. Openergy y el caso de la Universidad Nacional de Colombia. *Education in the Knowledge Society* (EKS), 19(4), 95–107. https://doi.org/10.14201/eks201819495107

Arias Velásquez, R.M. & Mejía Lara, J.V. (2021). Knowledge management in two universities before and during the COVID-19 effect in Peru. *Technology in Society*, 64, 101479. https://doi.org/10.1016/j.techsoc.2020.101479

Beck, U. (1998). La sociedad del riesgo: hacia una nueva modernidad (J. Navarro, Trad.). Paidós

Benavides, L., Arias, J., Serna, M., Bedoya, J., & Burgos, D. (2020). Digital transformation in higher education institutions: A systematic literature review. Sensors, 20(11), 3291. https://doi.org/10.3390/s20113291

Bond, M., Khosravi, H., De Laat, M., Bergdahl, N., Negrea, V., Oxley, E., Pham, P., Chong, S. W., & Siemens, G. (2024). A meta systematic review of artificial intelligence in higher education: A call for increased ethics, collaboration, and rigour. International Journal of Educational Technology in Higher Education, 21(1), 4. https://doi.org/10.1186/s41239-023-00436-z

Brdesee, H., & Alsaggaf, W. (2022). Decision-Making Strategy for Digital Transformation: A Two-Year Analytical Study and Follow-Up Concerning Innovative Improvements in University e-Services. *Journal of Theoretical and Applied Electronic Commerce Research*, 17(1), 138-164. https://doi.org/10.3390/jtaer17010008

Cardenas Ruiz, H. A., Rubiano Lopez, S. H. A., & Cabra Naranjo, L. C. (2023). Liderazgo, gobernanza y transformación digital en el diseño organizacional de la educación superior colombiana. Una revisión sistémica. *Miradas*, 18(2), 164–189. https://doi.org/10.22517/25393812.25468

Castañeda, L., Esteve-Mon, F., & Adell, J. (2023). La universidad digital: aproximación a un análisis crítico de los planes de transformación digital de las universidades públicas españolas. *Profesorado*, *Revista de Currículum y Formación del Profesorado*, 27(1), 175–198. https://doi.org/10.30827/profesorado.v27i1.23870

Chacón-Henao, J., & Arias-Pérez, J. (2024). Apoyo de la gestión como impulsor del Capital Intelectual (CI) en Instituciones de Educación Superior (IES). *Desarrollo Gerencial*, 16(1), 1–16. https://doi.org/10.17081/dege.16.1.6605

Chagnon-Lessard T., Gosselin L., Barnabe S., Bello-Ochende T., Fendt S., Goers S., Silva LCPD, Schweiger B., Simmons R., Vandersickel A., & Zhang P. (2021). Smart campuses: extensive review of the last decade of research and current challenges. IEEE Access 9:124200–124234. https://doi.org/10.1109/ACCESS.2021.3109516

CRC. (2012). Ley 1581 de 2012. Congreso de la República de Colombia. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

DAFP. (2024). Manual operativo del Modelo Integrado de Planeación y Gestión (MIPG). Departamento Administrativo de la Función Pública. https://www1.funcionpublica.gov.co/documents/28587410/56548624/2024-12-18_Manual_operativo_mipg_6V-publicada.pdf/0a5653af-7639-bda1-ec7a-6cded14d7da4

Deacon, B., Laufer, M., Mende, M. A., Tschache, T., & Schäfer, L. O. (2025). Resisting digital change at the university: an exploration into triggers and organisational countermeasures. European *Journal of Higher Education*, 15(sup1), 119–142. https://doi.org/10.1080/21568235.2025.2512735

DNP. (2019). Documento CONPES 3975: Política nacional para la transformación digital y la inteligencia artificial Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf

DNP. (2025). Documento CONPES 4144: Política Nacional de Inteligencia Artificial. Departamento Nacional de Planeación. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4144.pdf

Faraj, S., & Leonardi, P. M. (2022). Strategic organization in the digital age: Rethinking the concept of technology. *Strategic Organization*, 20(4), 771–785. https://doi.org/10.1177/14761270221130253

Farias-Gaytan, S., I. Aguaded, & M.-S. Ramirez-Montoya. (2023). Digital Transformation and Digital Literacy in the Context of Complexity Within Higher Education Institutions: A Systematic Literature Review. Humanities and Social Sciences Communications 10, 1: 1–11. https://doi.org/10.1057/s41599-023-01875-9

Farrell, R., Rice, M., & Qualter, D. (2024). Navigating the digital transformation of education: Insights from collaborative learning in an Erasmus+ Project. *Education Sciences*, 14(9), pp. 1023. https://doi.org/10.3390/educsci14091023

Garcés Ordóñez, M., & González Zabala, M. P. (2021). Caracterización de marcos de referencia que apoyan la implementación del gobierno de datos propuesto por MinTIC para entidades públicas. *Investigación E Innovación En Ingenierías*, 9(2), 42–58. https://doi.org/10.17081/invinno.9.2.4467

Gkrimpizi, T., Peristeras, V., & Magnisalis, I. (2023). Classification of barriers to digital transformation in higher education institutions: Systematic literature review. *Education Sciences*, 13(7), 746. https://doi.org/10.3390/educsci13070746

Hassan, M. K., Abdulkarim, M. E., & Ismael, H. R. (2022). Risk governance: exploring the role of organisational culture. *Journal of Accounting & Organizational Change,* 18(1), 77–99, doi: https://doi.org/10.1108/JAOC-01-2021-0003

Heeks, R. (2022). Digital inequality beyond the digital divide: conceptualizing adverse digital incorporation in the global South. *Information Technology for Development*, *28*(4), 688–704. https://doi.org/10.1080/02681102.2022.2068492

International Organization for Standardization. (2022). Information security management systems – Requirements (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence,* 1(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Klinke, A., & Renn, O. (2002), A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Analysis*, 22: 1071-1094. https://doi.org/10.1111/1539-6924.00274

Lund, H. B., & Vildåsen, S. S. (2022). The influence of Industry 4.0 narratives on regional path development. *Regional Studies, Regional Science*, 9(1), 82–92. https://doi.org/10.1080/21681376.2022.2029552

Luo, W., Y. Yu, & M. Deng. 2024. The Impact of Enterprise Digital Transformation on Risk-Taking: Evidence from China. *Research in International Business and Finance,* 69:102285. https://doi.org/10.1016/j.ribaf.2024.102285

Marín Y. R., Caro O. C., Rituay A. M. C., Llanos K. A. G., Perez D. T., Bardales E. S., Tuesta J. N. A., & Santos R. C. (2025). Ethical challenges associated with the use of artificial intelligence in university education, *Journal of Academic Ethics.* 23(4), 2443–2467, https://doi.org/10.1007/s10805-025-09660-w

Memarian, B., & Doleck, T. (2023). Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (A.I.) and higher education: A systematic review. Computers and Education: Artificial Intelligence, 5, 100152. https://doi.org/10.1016/j.caeai.2023.100152

MEN. (2021). Plan de transformación digital del Ministerio de Educación Nacional. https://www.mineducacion.gov.co/1759/articles-409015_recurso_11.pdf

Min-Allah, N., & Alrashed, S. N. (2020). Smart campus—A sketch. *Sustainable Cities and Society*, 59, 102231. https://doi.org/10.1016/j.scs.2020.102231

MinTIC. (2022). Decreto 767 de 2022. Ministerio de Tecnologías de la Información y las Comunicaciones. https://gobiernodigital.mintic.gov.co/692/articles-272977_Decreto_767_2022.pdf

Molina O., A. (2020). Modelo de gobierno y gestión de riesgos TI para las universidades públicas de Colombia:

Caso de estudio Universidad Popular del Cesar (Tesis de maestría, Universidad del Norte). https://manglar.uninorte.edu.co/bitstream/handle/10584/10394/1065814294.pdf

Nahavandi, S. (2019). Industry 5.0—A human-centric solution. Sustainability, 11(16), 4371. https://doi.org/10.3390/su11164371

Nugraha, R., & Syaidah, R. (2022). Smart campus governance design for XYZ Polytechnic based on COBIT 2019. *International Journal on Informatics Visualization*, 6(3), pp. 718-725. https://doi.org/10.30630/joiv.6.3.1257

Osorio, A. M., Úsuga, L. F., Restrepo-Carmona, J. A., Rendón, I., Sierra-Pérez, J., & Vásquez, R. E. (2024). Methodology for stakeholder prioritization in the context of digital transformation and society 5.0. *Sustainability*, 16(13), 5317. https://doi.org/10.3390/su16135317

Paredes Barrigas, S. L., & Negrete Costales, O. P. (2025). Políticas públicas para la transformación digital en el sector público: un estudio de caso en la Universidad Nacional de Chimborazo. *Esprint Investigación*, *4*(1), 498–514. https://doi.org/10.61347/ei.v4i1.125

Renn, O. (2008). Risk governance: Coping with uncertainty in a complex world. Earthscan

Renn, O., & P. Graham. (2005). White paper on risk governance. towards an integrative approach. International Risk Governance Council

Ríos-Avendaño, C., Ocampo-Salazar, C., & Nuñez, M.-A. (2024). Gestión del riesgo de fraude académico en educación superior. Un análisis en universidades de Medellín, Colombia, en tiempos de COVID-19. *Revista Iberoamericana De Educación Superior*, 15(42), 152–173. https://doi.org/10.22201/iisue.20072872e.2024.42.1670

Samara K., Mulholland G., & Aluko A. O. (2025), Impact of technology driven change on individuals' readiness in higher education: grounded in micro-foundations. *International Journal of Organizational Analysis*, 33(5), 1096–1113, doi: https://doi.org/10.1108/IJOA-03-2024-4388

Sivan-Sevilla, I. (2021). Framing and governing cyber risks: comparative analysis of U.S. Federal policies [1996–2018]. *Journal of Risk Research*, 24(6), 692–720. https://doi.org/10.1080/13669877.2019.1673797

Stein, V., & Wiedemann, A. (2016), Risk governance: Conceptualization, tasks and research agenda. *Journal of Business Economics*, 86(8), 813-836. https://doi.org/10.1007/s11573-016-0826-4

Stein, V., Wiedemann, A., & Bouten, C. (2019). Framing risk governance. *Management Research Review*, 42(11), 1224-1242. https://doi.org/10.1108/MRR-01-2019-0042

Stojanov, A., & Daniel, B.K. (2024). A decade of research into the application of big data and analytics in higher education: A systematic review of the literature. *Education and Information Technologies*, 29(5), 5807–5831. https://doi.org/10.1007/s10639-023-12033-8

Thaldar D., Botes M., Badru A., Chenia H., Duma S., Dlamini S.B., Amin N., Hugo W., Govender R., Bruce-Brand J., Vosloo A., Koorbanally N.A., & Chuturgoon A. (2025). Generative AI governance in higher education: a case study from Africa. Frontiers in Political Science. 7:1666661. https://doi.org/10.3389/fpos.2025.1666661

UNDRR. (2023). Governance of systemic risk: An initial exploration. United Nations Office for Disaster Risk Reduction. https://www.undrr.org

UNESCO. (2022). Recommendation on the ethics of artificial intelligence. UNESCO. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

van Asselt, M. B. A., & Renn, O. (2011). Risk governance. *Journal of Risk Research*, 14(4), 431–449. https://doi.org/10.1080/13669877.2011.553730

van der Vegt, R. G. (2018). A literature review on the relationship between risk governance and public engagement in relation to complex environmental issues. *Journal of Risk Research,* 21(11), 1–18. https://doi.org/10.1080/13669877.2017.1351466

Williamson, B., S. Bayne, and S. Shay. 2020. The Datafication of Teaching in Higher Education: Critical Issues and Perspectives. Teaching in Higher Education 25 (4): 351–365. https://doi.org/10.1080/13562517.2020.1748811.

Wu, C., H. Zhang, and J. M. Carroll. (2024). AI Governance in Higher Education: Case Studies of Guidance at Big Ten Universities. Future Internet 16 (10): 354. https://doi.org/10.3390/fi16100354

Yucel, S. (2018). Estimating the benefits, drawbacks and risk of digital transformation strategy. In: 2018 International Conference on Computational Science and Computational Intelligence CSCI, pp. 233-238, IEEE. https://doi.org/10.1109/CSCI46756.2018.00051

Zhu, J., Shi, C., & Dong, R. K. (2025). Digital governance and natural resource efficiency: evidence from China.

*Regional Studies, Regional Science*, 12(1), 721–739. https://doi.org/10.1080/21681376.2025.2542444