Journal of Posthumanism

2025
Volume: 5, No: 5, pp. 2701–2718
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i5.1664

Perspectives on a Cybersecurity Governance Framework Integrating Blockchain, Artificial Intelligence, and Legal Base for one Organization

Moisés Toapanta T.[1], Jeanette Jordán Buenaño[2], Santiago Vayas C.[3], Rubén Nogales, P.[4], Rodrigo Del Pozo D.[5], Antonio Orizaga T.[6], Diego Andrade A.[7]

Abstract

Cybersecurity governance issues remain persistent worldwide. One of the key causes is the lack of appropriate models, prototypes, or guidelines that effectively incorporate emerging technologies such as blockchain and artificial intelligence, while being grounded in national legal frameworks or aligned with international standards. The objective of this research is to analyze and define a prototype for the integration of a "Framework for Cybersecurity Governance Based on Blockchain, Artificial Intelligence, and Legal Foundations for Organizations." A deductive method and exploratory research approach were employed to analyze scholarly articles, standards, laws, regulations, and official websites related to the topic. The study resulted in the identification of relevant actors for the development of a cybersecurity governance framework, an algorithm for its analysis, and a prototype framework. The findings suggest that all organizations, based on simulations involving the identified actors, should aim for a performance level above 75%. Organizations scoring 75% or lower must seek strategies to reach a higher range—between 76% and 95%—to effectively mitigate risks, threats, and vulnerabilities in cybersecurity governance management.

Keywords: *Cybersecurity Framework, Cybersecurity Governance, Legal Framework, Legal Basis, Artificial Intelligence, Blockchain.*

Introduction

Cybersecurity governance management continues to face persistent challenges worldwide, particularly within public and private organizations in Ecuador. A key contributing factor is the lack of a well-defined cybersecurity governance framework that effectively integrates emerging technologies such as blockchain, specialized software, security policies, and standards underpinned by a robust legal foundation.

Companies today are seeking to be competitive through the use of information technologies and

[1] Carrera de Derecho, Universidad Técnica de Ambato, Ambato, Ecuador. Email: sm.toapanta@uta.edu.ec, (Correspondence Author)
[2] Carrera de Derecho, Universidad Técnica de Ambato, Ambato, Ecuador Email: je.jordan@uta.edu.ec
[3] Prof. MSc. Guillermo Santiago Vayas Castro, Carrera de Derecho, Universidad Técnica de Ambato, Ambato, Ecuador Email: gs.vayas@uta.edu.ec
[4] Carrera Ingeniería en Sistemas, Electrónica e Industrial, Universidad Técnica de Ambato, Ambato, Ecuador, Email: re.nogales@uta.edu.ec
[5] Carrera de Ingeniería de Sistemas, Universidad Estatal de Bolívar, Guaranda, Ecuador Email: rdelpozo@ueb.edu.ec
[6] Doctorado en Tecnologías de Información, Universidad de Guadalajara, San Isidro, México Email: jose.orizaga@academicos.udg.mx
[7] Subsistema de posgrados, U Centro de Estudios de Seguridad (CESEG), Universidad de Santiago de Compostela (USC) Compostela, España Email: diegoandradea@hotmail.com

the implementation of artificial intelligence tools due to their constant management challenges, despite the fact that artificial intelligence still lacks a regulatory legal framework. Given the identified problems, the authors of this article seek to identify the dimensions and elements of a preparation model framework that facilitates the implementation of AI in companies(Nortje & Grobbelaar, 2020). In this article, the strengths and weaknesses of cybersecurity in an Ecuadorian organization are identified and it is suggested that cybersecurity governance should be integrated by implementing a framework.(Giomara et al., 2023). They determined that there is a problem in cybersecurity governance, and standards such as NIST, the Cybersecurity Framework, and COBIT 2019 should be implemented, with the goal of defining a cybersecurity-oriented information technology governance framework.(Orellana-cabrera et al., 2022). Cybersecurity governance issues are critical in financial systems and in the national security of a country. For this reason, the authors recommend, first of all, carrying out a theoretical study on the different maturity models, gathering information based on existing information, and proposing a cybersecurity maturity model for critical infrastructures as a framework.(Loja et al., 2023). The Union of American States (OAS) determines that there are problems in cybersecurity governance and defines that the implementation of a CSF structure is recommended and that the Cybersecurity Framework (CSF) consists of three main components: Framework Core, Implementation Levels (Tiers) and Profiles(Oea, 2019). Ecuador, through the Ministry of Telecommunications and Information Society (MINTEL), is seeking alternatives to improve cybersecurity governance with a plan that addresses the following topics: Information Security and responsible use of ICT, Digital Economy, Emerging Technologies for Sustainable Development, Digital Citizen, Strengthening Digital Inclusion and Protection of Personal Data to define an appropriate framework for cybersecurity governance(Ecuador, 2025). The authors determine that Ecuador lacks legal support for cybersecurity governance management using artificial intelligence and new technologies such as blockchain; they suggest creating a legal structure with the definition of judges specialized in information and communications technologies similar to traffic, criminal, and civil judges, among others(Durango et al., 2025). They determine that it is necessary to define indicators related to the legal basis and information technologies, carry out a statistical analysis of the National Cybersecurity Index (INCIS), and identify the relevant actors for the globalization of information security(Armas et al., 2024). According to the National Cyber Security Index (NCSI), Ecuador has a 53.25% NCSI compliance rate through 2023. It is clear that cybersecurity governance in Ecuador is deficient(Foundation, e-Governance Academy 90007000, 2025). They believe that adopting a layered model to integrate Blockchain and Machine Learning significantly improves security, reaching effectiveness levels ranging from 80% to 98%. Blockchain and artificial intelligence technologies make significant contributions to improving cybersecurity governance(Toapanta et al., 2024).

The objective of this research is to perform the analysis to define a prototype for the integration of a "Framework for cybersecurity governance based on blockchain, artificial intelligence and a legal basis for an organization".

The deductive method and exploratory research were used to analyze articles related to the research topic, standards, laws, regulations and different official websites.

Why can a cybersecurity governance framework based on blockchain technologies, artificial intelligence, and a legal framework improve cybersecurity governance management in an organization?

Cybersecurity governance frameworks enable the integration of legally supported planning, strategies, security policies, standards, regulations, software, hardware, information technology infrastructure design, software, hardware, and other elements to mitigate risks, vulnerabilities, and threats so that information management is confidential, intact, and available (CIA).

In this research the results obtained are: Relevant actors for the definition of a framework for cybersecurity governance, Algorithm for the analysis of the framework for cybersecurity governance and a Prototype of a framework for cybersecurity governance.

It is concluded that all organizations, whose results in their simulations regarding the "Relevant actors for the definition of a framework for Cybersecurity Governance" are less than or equal to 75%, should look for alternatives to reach a range higher than 76% to 95% in order to mitigate risks, threats and vulnerabilities in the management of cybersecurity governance.

Related Works

The authors determine that cybersecurity governance is a challenge considering the constant problems that exist in most countries in the world, they carry out a systematic review of 42 articles referring to frameworks for cybersecurity governance and state that cybersecurity frameworks date back to 1970. The main cybersecurity frameworks used worldwide, including the NIST Framework, ISO/IEC 27001, COBIT, CIS Control and SANS Critical Security Controls(Juma et al., 2023). The cyber resilience of a cybersecurity framework is a highly relevant topic for companies across all sectors. They believe the NIST Cybersecurity Framework can guide organizations in strengthening their defenses and protecting information(Kumar Jain et al., 2024). The transportation system determines the need for a cybersecurity management system due to technological advances. They adopt cumulative cyber risk assessment. They propose a prototype that can help federal, state, and other government planners address future cybersecurity challenges(Hossain & Tarrant, 2023). They seek to evaluate information security governance in educational institutions by applying the COBIT 5 framework, focusing on five main processes derived from the mapping of business objectives related to information security: EDM03, APO12, APO13, BAI06 and DSS05; to improve security governance, they developed 20 recommendations: 7 recommendations for short-term strategies, 8 recommendations for medium-term strategies and 5 recommendations for long-term strategies(Siboro et al., 2024). They propose using the KAMI index, which is an instrument to analyze quality, integrity and maturity in the implementation of information security in an organization, according to the criteria of the SNI ISO/IEC 27001 standard. They determined the following items to analyze: Information security governance, information security risk management, information security framework, information and technology asset management, and information security(Wulansari & Novandi, 2022). They determine that a framework for cybersecurity governance is necessary to guarantee the integrity of data, in the exchange of information between different companies and consider that in the first instance a conceptual model should be created to identify the risks, vulnerabilities and threats that are generated in the management of cybersecurity governance(Silva, 2024). The authors determine that there are problems in auditing a cybersecurity program in higher education institutions and present the results of the validation of the Cybersecurity Audit Model (CSAM) in three research scenarios: An audit of a single cybersecurity domain (Educational Awareness), a multi-domain cybersecurity audit (Governance and Strategy, Legal and Compliance, Cyber Risk, Frameworks and Regulations, Incident Management, Cyber Insurance and Evolving Technologies) and finally a cybersecurity audit of all domains of the model. This validation serves to make future decisions that allow the

organization to correct cybersecurity weaknesses or improve cybersecurity governance domains and controls(Sabillon & Bermejo Higuera, 2023). They state that problems in cybersecurity governance persist in China because they have entered the digital age and mechanisms must be sought to guarantee the integrity of the data that is the basis for production and decision-making(Jiang et al., 2023). They present a holistic cybersecurity framework designed for e-Governments, which is distinguished by integrating recent advances in risk management, regulatory compliance and secure data exchange technologies, with a focus on strategic cybersecurity governance based on the MARISMA methodology(Figueroa et al., 2024). They state that university websites have problems managing cybersecurity governance. In their article, they determined that cybersecurity awareness and the use of automated assessment tools to identify vulnerabilities and penetration testing (VAPT) are lacking. The assessment was conducted in accordance with the ISO/IEC 27001 series of standards, ensuring a comprehensive and recognized approach to information security(Eshetu et al., 2024).

Methods

The deductive method and exploratory research were used to analyze the information from the different references of scientific articles and official websites that are related to the research topic, to carry out the analysis prior to the definition of the "Prototype for cybersecurity governance based on blockchain, artificial intelligence and a legal basis for an organization." In this phase, the conceptualization regarding blockchain technologies, artificial intelligence (AI) and Legal Basis is carried out in order to generate relevant indicators regarding the recommendations and solutions given to the authors.

Blockchain Technologies

Blockchain technology enables the implementation of secure, privacy-preserving decentralized systems where transactions are not controlled by third parties. Using blockchain technology, existing and new data is stored in a sealed compartment of blocks distributed across the network in a verifiable and immutable manner, ensuring information management(Elisa et al., 2023). In the processes for managing information related to medical processes in practice, blockchain does not guarantee, for this reason the authors of this article propose cutting-edge technologies such as Hyperledger, IPFS and data encryption(M. M. Alam et al., 2023). They determined that it is feasible to combine blockchain decentralization with on-chain governance to ensure security and transparency. The framework is implemented using Ganache, Metamask, MySQL, PHP, NodeJS, Solidity, and JavaScript. Blockchain technology also helps reduce process disruptions caused by man-in-the-middle attacks(Jain et al., 2024). They propose a blockchain-based national digital identity framework designed to meet the specific needs and challenges of Palestine. The proposed model leverages the security and decentralization of blockchain to create a secure, user-centric, and multipurpose platform for identity management. By analyzing the levels of identity verification, authentication, authorization, and security, the model offers a holistic approach to identity management(Hasan et al., 2024). The authors propose a secure platform verification to improve reliability, interoperability and data sharing in digital governance using blockchain and deep learning-based frameworks(Malik et al., 2023). They propose to use deep learning and blockchain frameworks to provide a secure platform that enables data sharing and interoperability for digital governance, for blockchain-based malware detection using AI to address multiple distributed conditions(Pawar et al., 2024).

Artificial Intelligence (AI)

Transparency and interpretability are critical for decision-making in AI-powered IoT systems. In AI governance, transparency enables scrutiny and accountability, while interpretability facilitates trust in AI-driven decisions. They conducted the evaluation and propose the use of two Explainable AI (XAI) techniques, SHAP and LIME, to explain the predictive results of AI models(Fares et al., 2023). They propose an AI-enhanced IT Project Management Framework that integrates predictive analytics and machine learning into all cybersecurity processes. The proposed framework defines governance and risk management through proactive risk assessment, real-time threat detection, and automated incident response, improving resilience to ever-evolving threats(Jabbar et al., 2024). They believe that the application of AI-based standards improves information security. Therefore, they analyzed nine cybersecurity standards, including seven international ones (e.g., ISO/IEC 27001:2022, NIST, IEC) and two national ones (UAE, KSA), using data from official sources for verification. They developed a recommendation system with content-based filtering (CBF), aligned with organizational maturity levels, and it was enhanced with a feedback loop for information from all user levels(Ali et al., 2024). Nigerian universities face vulnerabilities in cyberspace governance and believe it is necessary to mitigate risks. They propose practical frameworks that draw on existing literature while integrating cutting-edge tools such as intrusion detection systems, advanced cryptography, and AI-driven threat analysis(Farouk et al., 2024). The authors state that AI implementations should be considered as complex sociotechnical systems, rather than as simple technical tools, with the aim of mitigating the risks, vulnerabilities and threats generated by the advancement of ICT, AI, among others(Kroll et al., 2021). They define that the integration of machine learning (ML) into cybersecurity presents several challenges, such as data privacy, model bias, applicability, adversarial attacks, and the need for ethical governance. They propose a framework to manage ethical issues and protect ML models from adversarial manipulation, thus ensuring an effective and accountable cybersecurity governance framework(M. Alam et al., 2024). Artificial intelligence (AI) is advancing rapidly and has a major impact on cybersecurity governance, generating both advantages and disadvantages. Researchers developed and presented an AI Cybersecurity Dimensions (AICD) Framework, which is a comprehensive and multidimensional framework designed to guide academics, policymakers, and ICT and legal professionals(Malatji & Tolah, 2024).

Legal Basis

Security and trust in cloud information management are not reliable when compared to the critical characteristics of its providers regarding performance, security, trust, privacy, and compliance with laws and regulations, among others. They consider three domains: governance, transparency, and information security. They propose the implementation of a prototype, where the framework was applied in a real-life scenario and a long-term use simulation was run to verify its applicability, sensitivity, and robustness(Balcao-Filo et al., 2023). They determined that the NIST Cybersecurity Framework and Secure Control Framework encompass five functions: Identify, Protect, Detect, Respond, and Recover. The Secure Control Framework has more subdomains than the NIST Cybersecurity Framework that are not yet formally supported by the legal framework(Saritac et al., 2022). They propose a cybersecurity framework based on five interrelated algorithms: Threat Intelligence Integration, Risk Assessment and Management, Compliance Mapping, Incident Response Planning, Employee Training and Awareness supported by the legal foundation(Pandey et al., 2024). As AI evolves, and digital threats in the Philippines become more prevalent, researchers determine that the ethical integration of AI into

cybersecurity is crucial, given the ethical risks posed by AI-based cybersecurity solutions, including algorithmic bias and data privacy concerns. They consider comprehensive ethical frameworks and legal safeguards to ensure the responsible use of AI in cybersecurity, as well as the importance of education and policy recommendations to guide future AI governance, to be a priority and critical(Blancaflor et al., 2024). They analyzed that security policies are the basis for mitigating risks and vulnerabilities in cybersecurity governance and information security. They carried out a legislative evolution considering the history of the European cybersecurity network, which begins with the adoption of the Budapest Convention on Cybercrime in 2001, the Common Framework for Electronic Communications Networks and Services in 2002, and the creation of the European Union Agency for Cybersecurity (ENISA) in 2006(Sterlini et al., 2020). They propose that public-private partnerships can improve cybersecurity governance; due to the lack of this partnership, countries that have implemented cybersecurity governance have suffered privacy violations and conflicts within the legal system; because a legal framework for proper cybersecurity governance management is lacking(Park & Kwon, 2024). They state that the challenges of implementing an adequate framework for the integration of cybersecurity and software engineering persist. Therefore, it is necessary to study SSD security methods and ensure that security is implemented throughout the software development lifecycle (SDLC). They recommend analyzing the company's organizational structure, the behavior of internal and external users, legal, political, and governance foundations, as well as SSD approaches(Alhuqail & Jamail, 2023). The authors mention that the European Union Agency for Cybersecurity (ENISA) is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. Created in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, to improve the trustworthiness of ICT products, services and processes with the use of cybersecurity certification schemes, with the cooperation of Member States and EU bodies and helping Europe prepare for the cyber challenges of the future. The EU maintains that the governance of cybersecurity and information security should be supported by laws, regulations, policies under a legal framework of a region or country(Nineta Polemi, 2023). This article proposes an assessment framework and a systematic review of trends in cybersecurity risk assessment governance and compliance. Based on the results obtained, the authors recommend future frameworks supported by regulatory considerations that balance privacy, performance, and ethical requirements. Cybersecurity governance, they state, must, above all, preserve privacy, supported by a legal framework(Aljarrah et al., 2024). The authors state that since 2012, EU institutions have identified two areas that are under constant critical observation regarding cybersecurity: gaps in legal policies and the lack of integration that have not allowed the generation of an adequate framework for cybersecurity governance that would mitigate risks, vulnerabilities and threats in cybersecurity and information security management(Salvaggio & González, 2023).

Cybersecurity Governance Framework Perspectives

Table 1 determines the relevant indicators of the different proposals analyzed from the reviewed articles regarding blockchain technologies, artificial intelligence (AI) and legal basis to visualize the trends of each one.

Table 1. Indicators To Support the Formulation of a Framework for Cybersecurity Governance.

Indicators	Basis	Type	Ref.
Secure and privacy-	Verifiable and immutable,	Blockchain	(Elisa et al., 2023)

preserving decentralized systems.	allowing for guaranteed information management.	Technology	
Processes for information management.	Cutting-edge technologies such as Hyperledger, IPFS, and data encryption.	Blockchain Technology	(M. M. Alam et al., 2023)
Blockchain decentralization with on-chain governance to ensure security and transparency.	Ganache, Metamask, MySQL, PHP, NodeJS, Solidity y JavaScript.	Blockchain Technology	(Jain et al., 2024)
Digital identity.	Levels of identity verification, authentication, authorization and security.	Blockchain Technology	(Hasan et al., 2024)
Reliability, interoperability, and data sharing in digital governance.	Blockchain and deep learning-based frameworks.	Blockchain Technology	(Malik et al., 2023)
Data exchange and interoperability.	Detección de Malware basado en blockchain que utiliza IA.	Blockchain Technology	(Pawar et al., 2024)
Transparency and interpretability are fundamental to decision-making in governance.	Explainable AI (XAI), SHAP and LIME techniques.	Artificial Intelligence	(Fares et al., 2023)
Predictive analytics and machine learning in all cybersecurity processes.	Through proactive risk assessment, real-time threat detection, and automated incident response.	Artificial Intelligence	(Jabbar et al., 2024)
AI-based standards.	International cybersecurity standards (e.g., ISO/IEC 27001:2022, NIST, IEC) and two national ones (UAE, KSA).	Artificial Intelligence	(Ali et al., 2024)
Vulnerabilities in cyberspace governance.	Intrusion detection systems, advanced cryptography, and AI-powered threat analysis.	Artificial Intelligence	(Farouk et al., 2024)
Sociotechnical systems.	Use of new techniques based on ICT and AI.	Artificial Intelligence	(Kroll et al., 2021)
Machine learning (ML) in cybersecurity.	Data privacy, model bias, applicability, adversarial attacks, and the need for ethical governance.	Artificial Intelligence	(M. Alam et al., 2024)
Impact on cybersecurity governance.	AI Cybersecurity Dimensions Framework	Artificial Intelligence	(Malatji & Tolah, 2024)

	(AICD).		
Security and trust in cloud information management.	Performance, security, trust, privacy, and compliance with laws and regulations.	Legal basis	(Balcao-Filo et al., 2023)
NIST Cybersecurity Framework and Secure Control Framework.	They are not yet formally supported by the legal framework.	Legal basis	(Saritac et al., 2022)
Cybersecurity framework.	Integration of Threat Intelligence, Risk Assessment and Management, Compliance Mapping, Incident Response Planning, Employee Training and Awareness supported by the legal foundation.	Legal basis	(Pandey et al., 2024)
Ethical integration of AI into cybersecurity.	They consider comprehensive ethical frameworks and legal guarantees.	Legal basis	(Blancaflor et al., 2024)
Security policies.	They carried out a legislative evolution considering the history of the European cybersecurity network.	Legal basis	(Sterlini et al., 2020)
Public-private sector association.	Without this partnership, countries that have implemented cybersecurity governance have suffered privacy violations and conflicts within the legal system.	Legal basis	(Park & Kwon, 2024)
Integration of Cybersecurity and Software Engineering.	SSD security methods and security implementation throughout the software development lifecycle (SDLC).	Legal basis	(Alhuqail & Jamail, 2023)
European Union Agency for Cybersecurity (ENISA)	Reinforced by the EU Cybersecurity Act, ENISA contributes to EU cyber policy.	Legal basis	(Nineta Polemi, 2023)
Trends in cybersecurity risk assessment governance and compliance.	Supported by regulatory considerations that balance privacy, performance, and ethical requirements with legal support.	Legal basis	(Aljarrah et al., 2024)

Critical observation regarding cybersecurity	Policy-legal gaps and poor integration have prevented the development of an adequate framework for cybersecurity governance.	Legal basis	(Salvaggio & González, 2023)

Table 1 shows the indicators with their respective foundations expressed for each indicator supported by the references.

Results

The results obtained in this research:

- Relevant stakeholders for defining a cybersecurity governance framework
- Algorithm for analyzing the cybersecurity governance framework
- Prototype of a cybersecurity governance framework.

Relevant stakeholders for defining a cybersecurity governance framework

Table 2 outlines 20 key stakeholders that contribute to the development of a cybersecurity governance framework integrating blockchain, artificial intelligence, and a legal foundation for an organization. In this phase, the evaluation simulation was conducted based on the following considerations:

- The evaluation was scored on a scale from 0 to 100 using the Likert scale.
- A total of 20 relevant stakeholders were assessed.
- Five different scenarios were defined for the simulation.
- The evaluation applied the expert judgment technique.
- Only whole numbers (integers) were used in the scoring process.
- The results obtained were interpreted using Likert scale ranges.
- These results can serve as a reference for the development of a cybersecurity governance framework.

Likert Scale Design

For this evaluation–experimentation, the Likert scale was applied. The assessment consists of five option ranges: two positive, two negative, and one neutral. This evaluation is supported by the expert judgment technique.

Score	Range	Assessment
5	95-100	Very satisfied
4	75-94	Satisfied
3	50-74	Neither Satisfied, Nor Dissatisfied
2	25-49	Dissatisfied
1	0-24	Very Dissatisfied

Table 2: Likert Scale Design

Table 2 shows the design of the Likert scale used for the evaluation of Table 3 for the five different scenarios. This scale is the most appropriate to use, according to expert judgment.

	Relevant actors	**Scenario 1**	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**
1	Strategic plan of the organization.	90,00	80,00	90,00	95,00	90,00
2	Operational plan of the organization.	90,00	70,00	90,00	98,00	90,00
3	Strategic Plan for Information Technologies (PETI).	90,00	80,00	90,00	95,00	90,00
4	Operational Plan (POA) of the ICT Directorate.	90,00	70,00	90,00	95,00	90,00
5	Security plan.	0,00	0,00	50,00	80,00	50,00
6	Contingency plan.	70,00	50,00	80,00	90,00	80,00
7	Backup plan	0,00	0,00	70,00	80,00	50,00
8	Processes that the organization has at the macro level.	90,00	80,00	80,00	80,00	80,00
9	Legal and judicial processes for ICT.	50,00	30,00	50,00	60,00	70,00
10	Regulations for the use of AI.	0,00	0,00	50,00	50,00	50,00
11	Logical design of the network at the integrated macro level.	90,00	70,00	90,00	95,00	90,00
12	Physical design of the network at the integrated macro level.	80,00	80,00	90,00	95,00	90,00
13	Security models that are being applied	0,00	10,00	70,00	80,00	60,00
14	Applicable safety standards.	0,00	50,00	50,00	80,00	50,00
15	Do you have any framework for cybersecurity governance?	0,00	0,00	60,00	80,00	60,00
16	Information cybersecurity governance policies available at all levels and types.	80,00	70,00	80,00	95,00	80,00
17	Artificial Intelligence (AI) software to identify cyberattacks.	0,00	0,00	60,00	85,00	50,00
18	Definition of militarized zones (MZ) and demilitarized zones (DMZ).	90,00	70,00	90,00	95,00	90,00
19	Inventory of software and hardware available.	80,00	90,00	90,00	95,00	90,00
20	Use of new technologies such as blockchain, Hyperledger Fabric networks.	0,00	0,00	80,00	90,00	70,00
	Expert judgment evaluation	49,50 %	45,00 %	75,00%	85,65 %	73,50 %

Table 3. Relevant Actors for the Definition of A Framework for Cybersecurity Governance.

Figure 1 presents a graphical representation of the evaluation of the **"Key Stakeholders for the Definition of a Cybersecurity Governance Framework"**, based on the following details:

- Scenarios 1 and 2 correspond, on the Likert scale, to the rating of neither satisfied nor dissatisfied.
- Scenarios 3 and 5 correspond, on the Likert scale, to the rating of satisfied.
- Scenario 3 corresponds, on the Likert scale, to the rating of very satisfied.

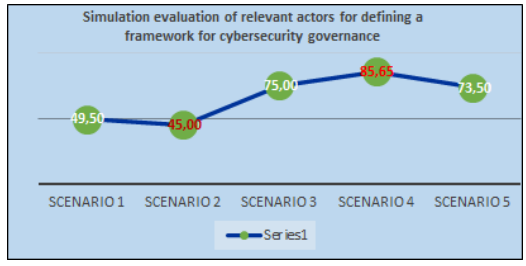

Figure 1. Simulation of Relevant Actors for the Definition of a Framework for Cybersecurity Governance.

Figure 1 presents the simulation of the evaluation conducted on the key stakeholders for the definition of a cybersecurity governance framework. The results show that in Scenarios 1 and 2, the scores are below 50%, indicating significant issues in cybersecurity management. In Scenario 5, the score is below 75%, while Scenario 3 achieves a score of 75%, which is considered the baseline for adequate cybersecurity management. In Scenario 4, the score is greater than or equal to 85%, which is deemed suitable for cybersecurity governance. It is important to note that, according to expert judgment, an ideal cybersecurity management score should exceed 95%. However, this threshold was not reached in this simulation based on the evaluation conducted by experts in this field.

Algorithm for Analyzing the Cybersecurity Governance Framework

The algorithm we propose for the definition of a cybersecurity governance framework outlines the processes that an institution should follow. This algorithm serves as a structured alternative recommended during the analysis phase for defining a cybersecurity governance framework.

Figure 2 outlines the phases for the definition of a cybersecurity governance framework, which are detailed as follows:

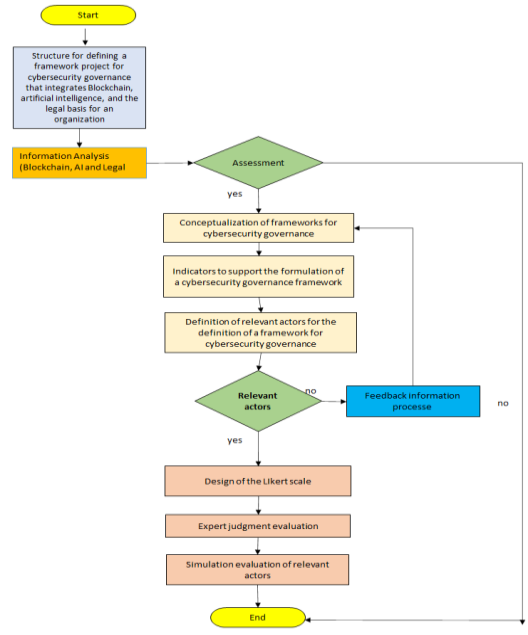

Figure 2. Algorithm for Defining a Cybersecurity Governance Framework.

Description

Phase One: We analyzed the structure for defining a framework project for cybersecurity governance that integrates blockchain, artificial intelligence, and a legal foundation for an organization. In this phase, we examined information from articles related to the topics proposed by researchers to address the issue, ensuring that the sources were from the past five years.

Phase Two: We conducted an analysis of information related to blockchain, artificial intelligence, and legal foundations with the aim of determining the current state of frameworks for cybersecurity governance that have been implemented in various organizations and countries.

Phase Three: he conceptualization of cybersecurity governance frameworks was carried out, including the identification of key indicators and stakeholders that directly influence this research. In this phase, three processes were defined: the conceptualization itself, the identification of indicators to support the formulation of a cybersecurity governance framework, and the identification of relevant stakeholders.

Phase Four: For the evaluation simulation, a Likert scale was designed, with the definition of the criteria used for the assessment. The next step involved applying expert judgment techniques. Following this, the simulation of the evaluation of the relevant stakeholders involved in a cybersecurity governance framework was conducted.

Prototype of a Cybersecurity Governance Framework

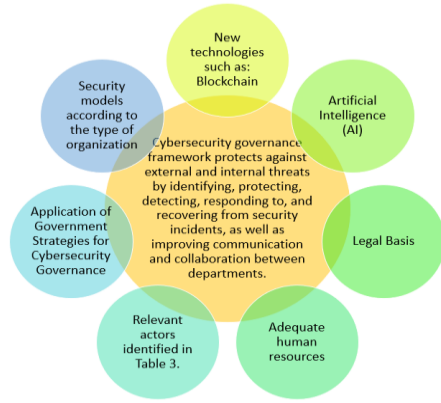

Figure 3. Prototype for the Integration of a Cybersecurity Governance Framework.

Figure 3 shows the integration of all relevant actors for the generation of a prototype for the integration of security that will allow us to adequately mitigate risks, threats and vulnerabilities in the management of cybersecurity governance.

Discussion

The following presents the results obtained in this research, including: Key stakeholders for the definition of a framework, an algorithm for analysis, and a prototype of a cybersecurity governance framework. These results are intended to be considered in future analyses prior to the definition of a cybersecurity governance framework.

This research does not include implementations; instead, simulations were carried out using information from relevant stakeholders to determine the current state of cybersecurity governance. Based on this, we proceeded to analyze and generate appropriate instruments, which will be applied at different levels, such as executive, administrative, faculty, and student levels.

The results reviewed and analyzed from the articles defined in the methodology phase show no contributions similar to those obtained in this research. We can confidently assert that the contributions in this research are novel: Key stakeholders for the definition of a cybersecurity governance framework, an algorithm for analyzing the framework, and a prototype of a cybersecurity governance framework.

The methodology and results presented in this research can be replicated and applied in any organization within countries with similar cultures and information technology infrastructure that wish to implement a cybersecurity governance framework integrating blockchain, artificial intelligence, and legal foundation

Future Work and Conclusions

Future work in the short term will include evaluation through surveys generated for the relevant stakeholders identified in the research to more accurately determine the current cybersecurity governance status of the selected organization.

It was concluded that all organizations, based on the simulations conducted regarding the "Key Stakeholders for the Definition of a Cybersecurity Governance Framework", must seek

alternatives if their results are less than or equal to 75%. They should aim to achieve a score within the range of 76% to 95% in order to adequately mitigate risks, threats, and vulnerabilities in cybersecurity governance management.

The definition of "Key Stakeholders for the Definition of a Cybersecurity Governance Framework" serves as the foundation for conducting simulations in different scenarios, which helps determine the current state of cybersecurity within an organization.

Before defining a project for cybersecurity governance, it is essential to establish an "Algorithm for the Analysis of the Cybersecurity Governance Framework". This algorithm allows us to visualize the relevant processes that must be followed, considering the integration of blockchain, artificial intelligence, and legal foundations to mitigate risks, vulnerabilities, and threats in information management.

It was concluded that the result obtained for the definition of a "Prototype of a Cybersecurity Governance Framework" is crucial for identifying the fundamental elements involved in the analysis and structuring phase of a cybersecurity governance project.

Finally, it was concluded that, for an adequate cybersecurity governance framework, it is necessary to apply artificial intelligence (AI), emerging technologies such as blockchain, and a legal foundation supported by the legal framework of the respective countries. Additionally, it is essential to create a legal project that regulates artificial intelligence in accordance with the country's legal framework.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Author Contribution

All authors collaborated in the process of elaboration of the article. Moises Toapanta, Jeanette Jordán Buenaño and Santiago Vayas worked mainly in the Introduction, Analysis of the processes, Summary, Mendeley citation research data, references from Scopus and PubMed and Review of all phases of the article and the Literature. Rubén Nogales and Rodrigo Del Pozo mainly in the methodology, search for information and results and Diego Andrade A., Antonio Orizaga T., mainly in the selection of the validation scales, discussion and conclusions.

Dr. Moises Toapanta, PhD: Supervision, validation, and project administration

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability Statement

The data supporting the findings of this study are available upon request from the corresponding author. Due to the nature of this research, participants were not asked for permission to share their data publicly, so supporting data is not available.

Acknowledgements

The authors would like to thank the Dirección de Investigación y Desarrollo (DIDE), Facultad de Jurisprudencia y Ciencias Sociales, Carrera de Derecho de la Universidad Técnica de Ambato

(UTA), Centro de Estudios de Seguridad (CESEG), Universidad de Santiago de Compostela (USC) España, the Department of Information Systems of CUCEA, University of Guadalajara (UDG), and RNI-Senescyt.

References

Alam, M., Deepak, Pandey, B., Ahmad, S., Shahid, M., & Ahmad, F. (2024). Machine Learning In Cybersecurity: Opportunities and Challenges. Proceedings - 2024 IEEE 16th International Conference on Communication Systems and Network Technologies, CICN 2024, 663–670. https://doi.org/10.1109/CICN63059.2024.10847405

Alam, M. M., Islam, M. S., Muntaha, S., Alam, M. T., & Tanha, K. J. (2023). A Secure and Optimized Healthcare Data Governance Framework Leveraging Hyperledger Fabric Blockchain. 2023 26th International Conference on Computer and Information Technology, ICCIT 2023, 13–15. https://doi.org/10.1109/ICCIT60459.2023.10441320

Alhuqail, S. K., & Jamail, N. S. M. (2023). Implementation of an Effective Framework in Merging Cybersecurity and Software Engineering. Proceedings - 2023 6th International Conference of Women in Data Science at Prince Sultan University, WiDS-PSU 2023, 31–36. https://doi.org/10.1109/WiDS-PSU57071.2023.00019

Ali, S. M., Razzaque, A., Yousaf, M., & Shan, R. U. (2024). An Automated Compliance Framework for Critical Infrastructure Security through Artificial Intelligence. IEEE Access, 13(January). https://doi.org/10.1109/ACCESS.2024.3524496

Aljarrah, S. J., Cherbal, S., Mashaleh, A., Karaki, J. Al, & Gawanmeh, A. (2024). On the Comparative Analysis of Trends in Cybersecurity Risk Assessment, Governance, and Compliance Frameworks. 2024 International Jordanian Cybersecurity Conference, IJCC 2024, 136–142. https://doi.org/10.1109/IJCC64742.2024.10847280

Armas, D. G. A., Toapanta, S. M., Díaz, E. Z. G., Trejo, J. A. O., Arellano, R. M., & Hifóng, M. M. B. (2024). An Approach to Information Security Based on the Legal Basis for an Organization in Ecuador. Journal of Computer Science, 20(10), 1330–1338. https://doi.org/10.3844/jcssp.2024.1330.1338

Balcao-Filo, A., Ruiz, N., Rosa, F. D. F., Bonacin, R., & Jino, M. (2023). Applying a Consumer-Centric Framework for Trust Assessment of Cloud Computing Service Providers. IEEE Transactions on Services Computing, 16(1), 95–107. https://doi.org/10.1109/TSC.2021.3134125

Blancaflor, E. B., Eleccion, F. G., Ferry, F. L., Oplado, J. P., Pajarillo, R. E., & Villaluz, A. (2024). Ethical Use of AI for Cybersecurity and Facing Digital Threats in the Philippines. International Conference on Computer and Communication Engineering Technology, CCET, 241–245. https://doi.org/10.1109/CCET62233.2024.10837790

Durango, R. D. P., Moisés, T. T., Zharayth, G. D., Pavón, P. T., Roció, L. a., Antonio, O. T., & Roció, M. a. (2025). Analysis for the Formulation of a Project for the Management of Cybersecurity Governance for the Optimization of Resources in an Organization. Journal of Ecohumanism, 4(1), 560–579. https://doi.org/10.62754/joe.v4i1.5837

Ecuador, E. nuevo. (2025). Programas del Plan de ciberseguridad. Ministerio de Telecomunicaciones Y de La Sociedad de La Información. https://tdtecuador.mintel.gob.ec/programas/

Elisa, N., Yang, L., Chao, F., & Cao, Y. (2023). A framework of blockchain-based secure and privacy-preserving E-government system. Wireless Networks, 29(3), 1005–1015. https://doi.org/10.1007/s11276-018-1883-0

Eshetu, A. Y., Mohammed, E. A., & Salau, A. O. (2024). Cybersecurity vulnerabilities and solutions in Ethiopian university websites. Journal of Big Data, 11(1), 1–35. https://doi.org/10.1186/s40537-024-00980-z

Fares, N. Y., Nedeljkovic, D., & Jammal, M. (2023). AI-enabled IoT Applications: Towards a Transparent Governance Framework. 2023 IEEE Global Conference on Artificial Intelligence and Internet of Things, GCAIoT 2023, 109–114. https://doi.org/10.1109/GCAIoT61060.2023.10385106

Farouk, S., Uppin, C., & George, G. (2024). Enhancing Cybersecurity in Nigeria: A Proposed Risk Management Framework for Universities. International Conference on Science, Engineering and Business for Driving Sustainable Development Goals, SEB4SDG 2024, 1–8. https://doi.org/10.1109/SEB4SDG60871.2024.10629748

Figueroa, V., Sánchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernández-Medina, E. (2024). Towards a Holistic Cybersecurity Framework for e-Governments. 2024 7th IEEE Biennial Congress of Argentina, ARGENCON 2024, 1–8. https://doi.org/10.1109/ARGENCON62399.2024.10735846

Foundation, e-Governance Academy 90007000, C. code: (2025). Porcentaje de cumplimiento de la NCSI. National Cyber Security Index (NCSI). https://ncsi.ega.ee/country/ec_2022/

Giomara, E., Neira, C., Humberto, C., Urgilés, F., Mariuxi, C., Jhovany, J., Espinoza, S., Bernabé, M., & Egas, R. (2023). Diagnóstico y línea base de los activos de información e infraestructura crítica de ciberseguridad del estado ecuatoriano. Pro Sciences: Revista de Producción, Ciencias E Investigación, 7(1), 101–119. https://doi.org/10.29018/issn.2588-

Hasan, F. A., Ashqar, H. I., Alsobeh, A., & Darwish, O. (2024). Blockchain-Based National Digital Identity Framework - Case of Palestine. 2024 International Conference on Intelligent Computing, Communication, Networking and Services, ICCNS 2024, 76–83. https://doi.org/10.1109/ICCNS62192.2024.10776538

Hossain, G., & Tarrant, J. (2023). CyberTMS : A Recommendation Framework for Cognitive Transportation Cybersecurity Management System in the Society 5.0. ISDFS 2023 - 11th International Symposium on Digital Forensics and Security, 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131723

Jabbar, H., Al-Janabi, S., & Syms, F. (2024). AI-Integrated Cyber Security Risk Management Framework for IT Projects. 2024 International Jordanian Cybersecurity Conference, IJCC 2024, 76–81. https://doi.org/10.1109/IJCC64742.2024.10847294

Jain, K., Chirag, Mittal, H. K., Vasesi, S., Paramjeet, & Kumar, J. (2024). Blockchain Stationed Managerial Framework for Logistics & Oblige Chain Direction for Reliable Data Control. Proceedings - 2024 2nd International Conference on Advanced Computing and Communication Technologies, ICACCTech 2024, 230–237. https://doi.org/10.1109/ICACCTech65084.2024.00046

Jiang, W., Ye, J., & Tan, Y. (2023). Research of Cybersecurity Measures for Data Governance. 2nd IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics, ICDCECE 2023, 1–6. https://doi.org/10.1109/ICDCECE57866.2023.10151409

Juma, A. H., Arman, A. A., & Hidayat, F. (2023). Cybersecurity Assessment Framework: A Systematic Review∗. 10th International Conference on ICT for Smart Society, ICISS 2023 - Proceeding, 1–6. https://doi.org/10.1109/ICISS59129.2023.10291832

Kroll, J. a., Michael, J. B., & Thaw, D. B. (2021). Enhancing Cybersecurity via Artificial Intelligence: Risks, Rewards, and Frameworks. Computer, 54(6), 64–71. https://doi.org/10.1109/MC.2021.3055703

Kumar Jain, Y., Dhaarna Singh Rathore, C. a., Johrawanshi, A., Gupta, M., Choudhary, D. K., & Pandey, A. (2024). Cybersecurity Frameworks: A Roadmap for Business Resilience. 2024 International Conference on Cybernation and Computation, CYBERCOM 2024, 102–108. https://doi.org/10.1109/CYBERCOM63683.2024.10803234

Loja, L., Patricio, C., Zenteno, C., Antonio, J., Urgilés, F., Humberto, C., Vintimilla, O., & Diana, A. (2023). Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador

Cybersecurity maturity model for critical infrastructures case study: Ecuador. Pro Sciences: Revista de Producción, Ciencias E Investigación, 7(48), 39–56. https://doi.org/10.29018/issn.2588-1000vol7iss48.

Malatji, M., & Tolah, A. (2024). Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics, 1(0123456789), 13–16. https://doi.org/10.1007/s43681-024-00427-4

Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B. R., Goyal, S. B., John Martin, R., Srinivasan, K., & Mittal, A. (2023). Building a Secure Platform for Digital Governance Interoperability and Data Exchange Using Blockchain and Deep Learning-Based Frameworks. IEEE Access, 11(July), 70110–70131. https://doi.org/10.1109/ACCESS.2023.3293529

Nineta Polemi, I. P. (2023). Multilayer Framework for good Cybersecurity Practices for IA (Issue June). https://doi.org/10.2824/588830

Nortje, M. a., & Grobbelaar, S. S. (2020). A Framework for the Implementation of Artificial Intelligence in Business Enterprises: A Readiness Model. Proceedings - 2020 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2020, 1–10. https://doi.org/10.1109/ICE/ITMC49519.2020.9198436

Oea. (2019). Ciberseguridad: Marco Nist. Un aboraje integral de la ciberseguridad. In White Paper Series. https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Orellana-cabrera, X. E., Sistemas, I. De, & Sistemas, I. De. (2022). Cybersecurity Oriented IT Governance Framework for the Banking Sector under COBIT 2019. 7(3), 706–723. https://doi.org/10.23857/pc.v7i3.3758

Pandey, R., Anjimoon, S., Asha, V., Singla, A., Khan, I., & Abed, Z. A. H. (2024). Developing Robust Cybersecurity Policies and Governance Frameworks in Response to Evolving Legal and Regulatory Landscapes. 2024 OPJU International Technology Conference on Smart Computing for Innovation and Advancement in Industry 4.0, OTCON 2024, 1–6. https://doi.org/10.1109/OTCON60325.2024.10687438

Park, S. H., & Kwon, H. Y. (2024). Governance of Cyber Threat Information Sharing for Public-Private Partnerships: Comparative Analysis of National Cases. 2024 IEEE/ACIS 24th International Conference on Computer and Information Science, ICIS 2024 - Proceedings, 41–48. https://doi.org/10.1109/ICIS61260.2024.10778364

Pawar, P. P., Kumar, D., Meesala, M. K., Pareek, P. K., Addula, S. R., & Shwetha, K. S. (2024). Securing Digital Governance: A Deep Learning and Blockchain Framework for Malware Detection in IoT Networks. 2nd IEEE International Conference on Integrated Intelligence and Communication Systems, ICIICS 2024, 1–8. https://doi.org/10.1109/ICIICS63763.2024.10860155

Sabillon, R., & Bermejo Higuera, J. R. (2023). New Validation of a Cybersecurity Model to Audit the Cybersecurity Program in a Canadian Higher Education Institution. 2023 Conference on Information Communications Technology and Society, ICTAS 2023 - Proceedings, 1–6. https://doi.org/10.1109/ICTAS56421.2023.10082731

Salvaggio, S. a., & González, N. (2023). The European framework for cybersecurity: strong assets, intricate history. International Cybersecurity Law Review, 4(1), 137–146. https://doi.org/10.1365/s43439-022-00072-9

Saritac, U., Liu, X., & Wang, R. (2022). Assessment of Cybersecurity Framework in Critical Infrastructures. 2022 IEEE Delhi Section Conference, DELCON 2022, 56–59. https://doi.org/10.1109/DELCON54057.2022.9753250

Siboro, I. N. A. P., Siallagan, J., Purba, A., Ambarita, L., Nggebu, S., & Lasino. (2024). Evaluation of Information Security Governance in Educational Institutions Using the COBIT 5 Framework. 2024

6th International Conference on Cybernetics and Intelligent System, ICORIS 2024, 1–6. https://doi.org/10.1109/ICORIS63540.2024.10903958

Silva, L. Da. (2024). Integrating Cybersecurity , Data Sovereignty and Trustworthiness in Agri-data Sharing Environments : A Conceptual Framework. 2024 Cyber Research Conference - Ireland (Cyber-RCI), 101073381, 1–8. https://doi.org/10.1109/Cyber-RCI60769.2024.10939388

Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & Van Eeten, M. (2020). Governance Challenges for European Cybersecurity Policies: Stakeholder Views. IEEE Security and Privacy, 18(1), 46–54. https://doi.org/10.1109/MSEC.2019.2945309

Toapanta, T. S. M., Del Pozo, D. R., Izurieta, R. R., Guamán, J. a., Orizaga, J. a., M. Arellano, R., & Baño Hifóng, M. M. (2024). Blockchain-based Security Model to Mitigate the Risks of a Database for a Public Organization. Journal of Internet Services and Information Security, 14(3), 78–98. https://doi.org/10.58346/jisis.2024.i3.005

Wulansari, T. T., & Novandi, D. (2022). Evaluation of Information Security Management Using the KAMI Index Framework. 2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022, 4, 173–177. https://doi.org/10.1109/ICSINTESA56431.2022.10041714.