Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Analysis for the Formulation of a Project for the Management of Cybersecurity Governance for the Optimization of Resources in an Organization

Rodrigo Del Pozo Durango[1], Moisés Toapanta T.[2], Zharayth Gómez D.[3], Pamela Toapanta Pavón[4], Roció Llumiquinga A.[5], Antonio Orizaga T.[6], Roció Maciel A[7].

Abstract

Persistent Challenges in Cybersecurity Governance Project Formulation: A Case Study in Ecuador and Beyond. The formulation of projects aimed at managing cybersecurity governance to optimize organizational resources presents persistent challenges both in Ecuador and globally. Among the most prevalent issues are: A lack of knowledge in identifying relevant standards and policies, Insufficient human resources with expertise and training in cybersecurity, and Deficiencies in norms, prototypes, and appropriate project management models for cybersecurity governance. The objective of this research is to perform the analysis for the formulation of a project for managing cybersecurity governance to optimize resources in an organization. A deductive approach and exploratory research methods were employed to analyze relevant documents and literature. Key Findings: Indicators to support the formulation of cybersecurity governance projects, Proposed solutions for project formulation in cybersecurity governance, Identification of relevant stakeholders essential for project development and resource optimization, Algorithm development utilizing flowchart techniques for project formulation. Conclusions: Simulation results, evaluated through the Likert scale and expert judgment, revealed varying levels of satisfaction: Scenarios 1 and 3: Satisfaction below 75% – indicating dissatisfaction, Scenarios 2 and 4: Satisfaction between 76% and 94% – indicating satisfaction, Scenario 5: Satisfaction between 95% and 100% – indicating high satisfaction. It is concluded that to ensure successful project formulation, all key stakeholders must achieve satisfaction levels exceeding 75%.

Keywords: *Information Governance; Information Technology; Information Security; Cybersecurity; ICT Projects, Resource Optimization.*

Introduction

Problems in formulating a project for managing cybersecurity governance to optimize resources in an organization are persistent in Ecuador and worldwide; among the most identified problems is the lack of knowledge in identifying standards, policies, human resources with training in the area of knowledge, norms, prototypes, and appropriate models for managing projects oriented to managing cybersecurity governance. Next, we will confirm this problem according to the analysis of publications made by different authors and official websites.

The authors of this research identify the cybersecurity problems in Ecuador by carrying out a diagnosis to establish a line of information assets and critical cybersecurity infrastructure, to carry out the information gathering and an evaluation of the current situation to determine the critical infrastructure and strategic infrastructure(Giomara et al., 2023). Public policies on cybersecurity in Ecuador and worldwide are considered strategic with the growth of the information society, networks and the phenomenon of cyberspace and the constant evolution of the Internet; the authors state that cybersecurity should be addressed at a strategic, tactical, and operational level(Eduardo Leyva-Méndez, 2021). Cybersecurity issues have a great impact on the financial sector and national security, for this reason, countries, especially Ecuador, must adopt a comprehensive approach to mitigate risks, vulnerabilities, and threats through a cybersecurity capacity maturity model considering critical infrastructures(Loja et al., 2023). They state that it is a fundamental part of corporate governance for the protection of its information assets, for this reason, an adequate model must be defined that meets the needs of the organization. The authors analyze standards

[1]Postgraduate Director, Universidad Estatal de Bolívar (UEB), Guaranda, Bolívar, Ecuador; rdurango1973@yahoo.es
[2]*Postgraduate Subsystems, Universidad Católica de Santiago de Guayaquil (UCSG), Guayaquil, Ecuador; segundo.toapanta@cu.ucsg.edu.ec
[3]Research Department, Gestión de Tecnologías Para El Mundo (GTM), Quito, 170301, Ecuador, zharaythgomez2709@gmail.com
[4]Facultad de Ciencias administrativas, Universidad Central del Ecuador, Quito, 170129, Ecuador, pamela12004@hotmail.com
[5]Departamento de Ciencias de la Computación, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador, rmllumiquinga@espe.edu.ec
[6]Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, México; jose.orizaga@academicos.udg.mx
[7]Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, México, ma.maciel@academicos.udg.mx

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

such as NIST Cybersecurity Framework and COBIT 2019 Framework, to define a framework oriented to information technology governance with cybersecurity(Ximena Elizabeth Orellana-Cabrera, 2022). The constant problems of cybersecurity have increased on a large scale worldwide; due to this situation, President Barack Obama of the USA on February 12, 2013 determined the creation of the National Institute of Standards and Technologies (NIST) and the development of the Cybersecurity Framework for the protection of critical infrastructures, which is now known as the Cybersecurity Framework (CSF)(Almagro, 2019). As of August 3, 2022, Ecuador has its National Cybersecurity Strategy (ENC) for the first time, which will allow citizens to access digital services with greater security and strengthen the protection of their data. In addition, it opens new options to generate regulation to protect all actors in society from cybercrime and strengthen the technological infrastructures of public and private entities. Ecuador is vulnerable to cyber threats, according to the Global Cybersecurity Index (GCI), issued by the ITU, published in 2020, which places the country in 119th place out of 182, with 182 being the country with the greatest vulnerabilities worldwide. The Global Cybersecurity Index defined by Mintel for 2022 is 35.3% and for 2025 it is 51.3%. They also state that Ecuador has an evaluation of 0.00 out of 20 points in the organizational measures pillar (Ministerio de telecomunicaciones y de la sociedad de la Información, 2024). The National Directorate of Civil Registry of Ecuador has problems with identification, authentication, authorization, and auditing to mitigate the confidentiality, integrity, and availability of information to work in a distributed architecture (Student et al., 2016). Information security problems regarding the impact on administrative processes due to cyber-attacks in public and private organizations in Ecuador and worldwide persist despite having a first-class technological infrastructure(S. M. T. Toapanta et al., 2019). The Ministry of Telecommunications and Information Society has problems managing information in its processes (Toapanta Toapanta et al., 2020). Higher education institutions in Ecuador are at increased risk of cyberattacks and data breaches, which can have serious consequences for both the organization and its stakeholders(Delgado et al., 2016). The lack of appropriate indicators of professional identity to improve information security governance as an alternative to solving problems (S. M. T. Toapanta et al., 2022). The problem is that security models deployed in databases in public organizations suffer cyber-attacks due to vulnerabilities in their security management systems (S. M. Toapanta et al., 2020). The status of effective information management is critical for public organizations, particularly in developing regions such as Latin America, where cybersecurity capabilities are limited, leaving them vulnerable to increasingly sophisticated cyber threats, resulting in financial losses and reputational damage(T. S. M. Toapanta et al., 2024). Information security problems persist at both the technical and legal levels, among others. One of the main causes in Ecuador is the lack of an adequate legal framework for the field of information and communication technologies(Armas et al., 2024). In the National Cyber Security Index (NCSI), which is another of the international organizations that provides real-time diagnoses regarding the cybersecurity situation of countries that have an international agreement, the "National Cyber Security Index (NCSI) Ecuador has 53.25% security(Foundation, e-Governance Academy 90007000, 2024). Information technology is the foundation for e-government infrastructure, but this makes governments more exposed to cyber risks. The authors conduct a study of cyber risks in the public sector to build linear models to explain the relationships between cyber losses, local government budgets, and IT expenditures. They find that cyber losses used to have a strong positive relationship with the size of the budget of the affected governments. They find that investment in information technology is becoming more effective in terms of reducing the loss-to-budget ratio(Kesan & Zhang, 2021).

With the above background, we can see the serious problem that public and private organizations have regarding cybersecurity governance. Additionally, we mention that another of the serious problems that public organizations in Ecuador have is that in their organic structure, the ICT management is at the same level as the administrative, financial, operational, and legal management, among others. Finally, in this analysis, we must also consider that Ecuador lacks an organic structure for ICT at a national level similar to the juvenile, transit, civil, and criminal judges, among others, which are part of the problems for the formulation of projects for the management of information security governance.

Why is it necessary to carry out an analysis to formulate a project for managing cybersecurity governance to optimize resources in an organization?

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

To determine alternatives that allow generating projects for the management of cybersecurity governance with the optimization of technological resources that allow the mitigation of risks, vulnerabilities, and threats in cybersecurity governance.

The objective of this research is to carry out the analysis for the formulation of a project for the management of cybersecurity governance for the optimization of resources in an organization.

The deductive method, exploratory research, is used to analyze the information from the documents that are related to this research.

The results of this research are: Indicators to support the formulation of a project for cybersecurity governance, Proposed solutions related to the formulation of projects for cybersecurity governance, Identification of relevant stakeholders essential for project development and resource optimization, and an Algorithm for the formulation of projects using flowchart techniques are alternatives to improve project management.

The results of the simulation, evaluated using the Likert scale and expert judgment, indicate varying levels of satisfaction across different scenarios. In scenarios one and three, satisfaction levels were below 75%, classifying them as dissatisfied. Scenarios two and four showed satisfaction levels between 76% and 94%, indicating general satisfaction. Scenario five achieved the highest satisfaction, with results ranging from 95% to 100%, reflecting a very satisfied response. These findings present an alternative for enhancing project management.

Literature Review

They compare cybersecurity governance awareness from the perspective of the young, educated and tech-savvy population of the United Arab Emirates (UAE) and the United States of America (USA) to promote global cyber governance guidelines and practice. The researchers' input is key contributions to inform cybersecurity policymakers in the UAE and the Gulf Cooperation Council (GCC) region, with the aim of improving cybersecurity, governance, awareness and trust among citizens based on the information obtained regarding awareness(Shah et al., 2023). They define the relationships with IT service management and IT security, based on the COBIT 2019 reference framework, focusing on the AP013 domain processes regarding administrative security BAI06 IT change management and DSS02 managed service requests and incidents in the defined company(Saputra et al., 2022). They define digital governance using blockchain and deep learning-based frameworks to ensure the privacy, security and reliability of electronic platforms and systems used to manage and deliver public services. Interoperability and data sharing are essential for digital governance(Malik et al., 2023). The digitalization of information increases cybersecurity incidents, which is why the area of cybersecurity has been identified as a key area for companies to use all the benefits of modern technology. The authors propose a framework through the theory regarding the dynamic capability view (DCV) and the theory that it has to study what impact (CM) has on the company's performance(Kok & Teoh, 2021). It states that one of the problems of cybersecurity governance is the misinterpretation in the implementation of cybersecurity frameworks, given that they are excessively based on new technologies and consider human factors as secondary. The authors evaluated the existing cybersecurity frameworks and proposed a new approach, an agile cybersecurity framework that integrates technology and organizational culture in a globalized way(Handri et al., 2024). The authors present a comprehensive cybersecurity framework with five interconnected algorithms: threat intelligence integration, risk assessment and management, compliance mapping, incident response planning, and employee training and awareness. This research contributes to cybersecurity methodologies, with a dynamic and adaptive approach to protecting against spreading cyberthreats(Pandey et al., 2024). They propose a comprehensive approach to explore how master data management (MDM) governance aligns with cybersecurity protocols to protect against breaches. The methodology they applied is to synthesize methodologies and best practices, proposing an integrated strategy(Pansara et al., 2024). They consider data to be an important factor in production in the industry so that people can access, apply and process data more easily, and improve the utilization of data resources with integrity. With the importance of data in the infrastructure of the digital economy, data

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

security governance has become the focus of data governance(W. Jiang et al., 2023). It determines that in Big Data, data transmission is becoming more frequent and faster and the data life cycle is extended, generating more challenges for the governance of security and privacy risks. Additionally, it states that a governance measure that combines technology and regulation has the potential to become the best practice(Wang et al., 2021). They determine that isolated risks influence cybersecurity management, they consider that alignment with enterprise risk management (ERM) is essential to ensure that risk management is managed proactively, strategically and comprehensively to mitigate risks and threats in cybersecurity governance management(Althonayan & Andronache, 2019). The authors of this research determine a mixed association between AI, e-governance, and cybersecurity; however, they believe that this relationship is specific to cybersecurity. They state that there must be a direct relationship between artificial intelligence (AI), e-governance, and cybersecurity. In this research, they determined the mediating role of e-governance with AI and cybersecurity(Bokhari & Myeong, 2023). Information technologies are transversal in any type of company, regardless of size, since they are crucial for the development of its activities according to its corporate purpose; with the evolution of the Internet, the levels of risk in information management are increasingly critical, which is why the implementation of corporate governance and information security is considered necessary. Researchers determined that there are many reference frameworks, including COBIT 2019, but one of the problems in small companies is having an inadequate budget(Skrodelis et al., 2020). The authors state that it is important to analyze the application of artificial intelligence (AI) today, given that AI is exposed to the risks of cyberattacks, one of the causes being the lack of specific laws for AI. They identified three challenges to achieving compliance of AI systems with the cybersecurity requirement: Taking into account the diversity and complexity of AI technologies, assessing AI-specific risks, and developing AI systems that are secure by design. They consider the overview of AI cybersecurity practices and identify gaps in current approaches to assessing the security compliance of AI systems(Hamon et al., 2024).

Methodology

In this research, the deductive method and exploratory research were used to analyze the information from the different references and official websites that are related to carrying out the analysis before the formulation of a project for the management of cybersecurity governance for the optimization of resources in an organization, considering an organization in Ecuador as a case study. In this phase, the following foundations, trends, standards, and reference frameworks, among others, were analyzed that must be analyzed for the case study or any organization in the world with similar characteristics for the formulation of a project for the management of cybersecurity governance.

Conceptualizing Cybersecurity Governance

Cybersecurity governance provides a strategic-level view of how an organization will develop and implement mechanisms in internal cybersecurity infrastructures to ensure the security of data and information across its projects. They define cybersecurity risk and establish a management-level committee to oversee cybersecurity risks and issues. Mature cybersecurity governance includes cybersecurity planning and its alignment with applicable laws and regulations related to cybersecurity and data protection. The cybersecurity strategy should also be aligned with an organization's overall strategy and vision. The strategy takes into account the management of information and data security issues and risks(Financie Crimen Academy, 2024).

ISO/IEC 27001 and ENS, Are the Perfect Combination for Cybersecurity

The ISO/IEC 27001 Information Security Management System and the National Security Scheme (ENS) have become a perfect combination for organizations to have better cybersecurity management, always focusing on continuous improvement of risk and threat control. Both certification schemes are analyzed in depth here. Within this framework, AENOR designed the Cybersecurity and Privacy Ecosystem for the new digital era, based on international ISO standards/norms, as well as current Spanish and European laws

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

and regulations. It is a fact that cybersecurity is transversal to any information system/technology used by an organization(Boris Delgado Riss, 2024).

Cybersecurity in Ecuador

Ecuador is vulnerable to cyber threats, according to the Global Cybersecurity Index (GCI), issued by the ITU and published in 2020, which places the country in 119th place out of 182, with 182 being the country with the greatest vulnerabilities worldwide. The key performance indicators will be monitored and evaluated by the National Cybersecurity Coordinator quarterly and will submit annual reports to the National Cybersecurity Committee. The indicators, together with the compliance goals, will be subject to modifications approved by the National Cybersecurity Committee as the implementation of the National Cybersecurity Strategy progresses(Ecuador, 2022).

Cobit 2019

ISACA leverages the expertise of its half-million engaged professionals in information and cyber security, governance, assurance, risk, and innovation, as well as its business performance subsidiary, CMMI Institute(Cobit 2019, 2019).

Frameworks and Standards for Cybersecurity

A framework refers to a work environment. These work environments comprise a set of policies determined to address a specific problem that can be used as a guide to solve conflicts with similar characteristics. Cybersecurity models or standards are defined as those practices developed and implemented by organizations with the aim of increasing their cybersecurity(VGS Tech solutions, 2024).

Table 1. Main Security and Cybersecurity Frameworks and Standards for The Formulation of a Project

Description	Function	Type
Control frameworks	The cybersecurity model is responsible for processing a simple strategy to assign it to security teams. In addition, control frameworks are tasked with assigning the control guidelines to be followed in the organization. Likewise, being able to technically analyze the starting point is another advantage that this type of framework offers us.	Frameworks
Program Frameworks	Its purpose is to analyze the condition of the relevant cybersecurity software. Program frameworks advocate for understandable computer security and facilitate communications between the department in charge of these tasks and the directors.	Frameworks
Risk frameworks	They are responsible for determining those decisive points in the process with the aim of advising and managing the level of uncertainty. Like program frameworks, these simplify internal communications, thus making the process simpler. This cybersecurity model gives greater importance to activities related to network protection.	Frameworks
ISO/IEC 27001 y 27002	This standard belongs to the information security management system (ISMS). It is a management model that ensures information security under an integral management domain.	Safety standard
NERC	The NERC cybersecurity standard is responsible for developing the regulations that are applied to reinforce electrical systems. Despite this, it has developed certain regulations for various sectors. These standards provide complete management control regarding network security and, at the same time, support industrial processes with the implementation of various practices.	Safety standard
NIST	It is a cybersecurity framework that provides an effective classification of cybersecurity outcomes and a procedure for assessing and managing	Safety standard

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

	these outcomes. Its purpose is to cooperate with private sector companies that provide critical infrastructure by assigning them certain guidelines to contribute to improvement.	
ISO 15408	It is the standard responsible for implementing those common criteria that make possible the linking and integration of products that have different software and hardware.	Safety standard

Table 1 provides a general description of the security frameworks and standards so that readers can consider the security and cybersecurity framework and standards according to the type and structure of the organization where a project is to be formulated.

The Influence of Artificial Intelligence On E-Governance and Cybersecurity in Smart Cities: A Stakeholder Perspective

Artificial intelligence (AI) has been identified as a critical technology of the Fourth Industrial Revolution (Industry 4.0) to protect computer network systems against cyberattacks, malware, phishing, damage, or illicit access. AI has the potential to strengthen the cyber capabilities and security of nation-states, local governments, and non-state entities through e-governance(Bokhari & Myeong, 2023).

Benchmarking Human Factors in Cybersecurity: Implications for Cyber Governance

Provides an extensive overview of cybersecurity awareness in the young, educated, and tech-savvy population of the United Arab Emirates (UAE), compared to the United States of America (USA) to advance the scholarship and practice of global cyber governance(Shah et al., 2023).

Secure Platform for Interoperability and Data Exchange in Digital Governance Using Blockchain And Deep Learning-Based Frameworks

A secure platform is a critical component of digital governance, helping to ensure the privacy, security, and reliability of electronic platforms and systems used to manage and deliver public services. Interoperability and data sharing are essential to digital governance, allowing different government agencies and departments to seamlessly share data, information, and resources, regardless of the platforms and technologies they use(Malik et al., 2023).

Development of an Agile Cybersecurity Framework with an Organizational Culture Approach Using the Q Methodology

Cyberattacks continue to pose significant threats and damage across a wide range of industries. The main problem causing this lies in the misinterpretation of the implementation of cybersecurity frameworks. They often rely excessively on technology as the primary solution and neglect human factors(Handri et al., 2024).

Three Challenges to Protecting AI Systems in The Context of AI Regulations

They examine the interaction between artificial intelligence (AI) and cybersecurity in light of future regulatory requirements on the security of AI systems, focusing specifically on the robustness of high-risk (Hamon et al., 2024).

Fronesis: Early Detection of Ongoing Cyberattacks Based on Digital Forensics

An approach to digital forensics-based early detection of cyberattacks. The approach combines ontological reasoning with the MITRE ATT&CK framework, the Cyber Kill Chain model, and continuously acquired digital artifacts from the monitored computer system. Fronesis examines the collected digital artifacts by applying rule-based reasoning on the Fronesis cyberattack detection ontology to identify traces of adversarial technique(Dimitriadis et al., 2023).

Analysis of Blockchain System with Token-Based Accounting Method

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

The flexible authority management mechanism of the proposed system is regulation-friendly, as the intensity of supervision and governance can be tailored to accommodate different application scenarios(Cai et al., 2019).

Prototype for Managing Cybersecurity in Small Businesses

Cybersecurity is defined as the protection of information assets by addressing threats that put information at risk. Organizations, regardless of size, must manage cybersecurity risks to improve the security and resilience of their assets. Large companies are increasingly investing in cybersecurity. However, the perception of this danger in smaller companies is low and few have protecting their systems on their list of priorities(Rea Guaman et al., 2018).

Cybersecurity

Impact and detection of security events through monitoring prototype: This article presents a proposal for a prototype of a monitoring and analysis tool for computer events to have a security component with the purpose of reinforcing our navigation and use of web systems in small businesses, home networks or medium-sized companies focusing on cybersecurity(Alanis Hernández et al., 2024).

Information Security and Cybersecurity Model

The Information Security and Cybersecurity Model aims to preserve the confidentiality, integrity, and availability of information, allowing data privacy to be maintained. The Model will operate through the following five phases: diagnosis, planning, implementation, performance evaluation, and continuous improvement. The phases will include objectives, goals, procedures, and follow-ups, allowing information security and cybersecurity to be a sustainable management system. The Model will be reviewed regularly since it is part of the Integrated Planning and Management Model; therefore, when identifying changes in the regulations in the business, in its structure, objectives, or in general, it must be updated to ensure that it remains adequate and adjusted to the identified requirements(La, 2024).

Advantages of a Cybersecurity Maturity Model

The authors determine that the "Capability Maturity Model", as a model for evaluating an organization's processes, is designed based on Cobit 2019, ITIL, ISO27001/27002. The model consists of 63 Controls, which are divided into 14 Domains(Bravo, 2024).

Analysis of Cybersecurity Cultural Maturity Models

They state that there are countless models related to the cultural maturity of cybersecurity in organizations. They present the most relevant models taking into account the role of professionals in the area of knowledge in the construction of training and awareness plans. The security models detailed in this document are: the Citigroup Information Security Evaluation Model (CITII-SEM), the COBIT Maturity Model, and the CERT/CSO Security Capability Evaluation Model(Escobar, 2022).

Understanding The Plural Landscape of Cybersecurity Governance in Spain: A Question of Capital Exchange

The authors determine the contribution and collaboration networks of public and private actors to the provision of cybersecurity in Spain; they support the data from three sources: policy and legal documents, a Delphi study with cybersecurity experts, and 34 interviews. Based on the theoretical foundations of nodal governance and anchored pluralism; they argue that the position of the actors and the dynamics of public-private collaboration involved in cybersecurity governance can be understood through the analysis of the exchange of capital. The analyses they carried out reveal that public organizations occupy a preeminent position in cybersecurity governance despite the greater economic and cultural capital of large technological corporations(Del-Real & Díaz-Fernández, 2022).

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Model-Based Cybersecurity Analysis

Critical infrastructures (CIs), such as power grids, link a large number of physical components from different vendors to the software systems that control them. These systems are constantly threatened by sophisticated cyberattacks. The need to improve the cybersecurity of such CIs, through holistic system modeling and vulnerability analysis, cannot be overstated. This is challenging, as a CI incorporates complex data from multiple interconnected physical and computational systems. Meanwhile, the exploitation of vulnerabilities in different information technology (IT) and operational technology (OT) systems leads to various cascading effects due to the interconnections between systems. The researched paper makes use of a comprehensive taxonomy to model such interconnections and the implicit dependencies within complex CIs, bridging the knowledge gap between IT security and OT security(Y. Jiang et al., 2023).

Blockchain For Artificial Intelligence (AI): Improving Compliance with the EU AI Act Through Distributed Ledger Technology. A Cybersecurity Perspective

They conducted research into the potential of blockchain technology to mitigate certain cybersecurity risks associated with artificial intelligence (AI) systems. In line with ongoing regulatory deliberations within the European Union (EU) and the growing demand for more resilient cybersecurity measures in the field of AI(Ramos & Ellul, 2024).

Cyberdefense and Cybersecurity, Beyond the Virtual World: Ecuadorian Model of Governance in Cyberdefense

Cyber defense and cyber security have become key areas of strategic studies. Their current development coincides with the advent of the information society, computer networks, and the "Internet" phenomenon, whose expansion has configured the fifth dimension of modern warfare and has significantly affected the daily lives of various actors in the global world. Their study becomes an obligatory task for the political-strategic management of the defense of nations. In Ecuador, these issues (widely discussed) have focused on a pragmatic dimension(Vargas Borbúa et al., 2017).

Government Information Security Scheme (EGSI)

It seeks to preserve the confidentiality, integrity, and availability of information by applying an information security risk management process and selecting controls to address identified risks(Guerrero et al., 2024).

In this phase we have defined the theoretical foundations, approaches, and models that support and provide the frame of reference for the study regarding the standards, models, prototypes, and guides, among others, of the information security governance situation in Ecuador, Latin America, and the world for the formulation of a cybersecurity governance management project; with this information we are clear about the problem of cybersecurity governance in organizations.

Additionally, for the formulation of a project for the management of cybersecurity governance for the optimization of resources in an organization, it is recommended to carry out an analysis of the current situation, assess the viability, profitability, and sustainability, and consider the technical, economic, social impact aspects, among others that will be analyzed in the following research so that the project is executed effectively and efficiently.

Results

The results obtained in this research are:

- Indicators to support the formulation of a cybersecurity governance project.
- Proposed solutions related to the formulation of cybersecurity governance projects.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

- Identification of relevant stakeholders essential for project development and resource optimization.
- Algorithm for the formulation of projects using flowchart techniques.

Indicators To Support the Formulation of a Cybersecurity Governance Project

In this phase of the research, the results obtained were the "indicators to support the formulation of a project for cybersecurity governance" which allowed us to identify the indicator, its basis, and the type. The result obtained is of great importance since it allows us to support the problems in information security governance and its influence on the formulation of projects in this area of knowledge.

Table 2. Indicators To Support the Formulation of a Project for Cybersecurity Governance.

Indicators	Basis	Type	Ref.
Diagnosis to establish a line of information assets and critical cybersecurity infrastructure.	Gathering information and assessing the current situation.	Diagnosis	(Giomara et al., 2023)
Public policies on cybersecurity.	Growth in the information society.	Strategic, tactical, and operational	(Eduardo Leyva-Méndez, 2021)
Impact on the financial sector.	Mitigate risks, vulnerabilities, and threats.	Comprehensive approach	(Loja et al., 2023)
Protection of information assets.	Corporate governance.	Standards, Frameworks, and Methodologies	(Ximena Elizabeth Orellana-Cabrera, 2022)
The number of standards.	National Institute of Standards and Technology (NIST).	Standard	(Almagro, 2019)
National Cybersecurity Strategy (NCS).	Global Cybersecurity Index (GCI), issued by the ITU.	National and international standards	(Ministerio de telecomunicaciones y de la sociedad de la Información, 2024)
Identification, authentication, authorization, and auditing.	Confidentiality, integrity, and availability of information.	Safety principles	(Student et al., 2016)
Impact on administrative processes.	Cyber-attacks on public and private organizations.	Technological infrastructure	(S. M. T. Toapanta et al., 2019)
Processes for information management.	Policies Ministry of Telecommunications and Information Society.	Processes	(Toapanta Toapanta et al., 2020)
Risk of cyber-attacks and data breaches.	Policies of higher education institutions in Ecuador.	Processes	(Delgado et al., 2016)
Suitable ICT professionals.	Information Security Governance.	Standards in education	(S. M. T. Toapanta et al., 2022)
Identifying unsuitable cybersecurity models.	Computer attacks.	Technical	(S. M. Toapanta et al., 2020)
Limited cybersecurity capabilities.	Vulnerability in cyber threats.	Technical and Management	(T. S. M. Toapanta et al., 2024)

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Cybersecurity problems are persistent.	Lack of an adequate legal framework for the field of information and communication technologies.	Technical and legal	(Armas et al., 2024)
Cybersecurity situation in Ecuador.	National Cyber Security Index (NCSI).	Standard	(Foundation, e-Governance Academy 90007000, 2024)
Technological infrastructure in e-government	Linear models	Technical	(Kesan & Zhang, 2021)

Table 2, generates indicators to support the formulation of a project for cybersecurity governance; these indicators should be considered in the future for the assessment in the formulation of projects oriented towards cybersecurity governance.

Proposed Solutions Related to the Formulation of Projects for Cybersecurity Governance

After having carried out the diagnosis of the information of the related work phase, the results obtained were the "proposed solutions related to the formulation of projects for information governance" which allows us to visualize more clearly what solutions have been proposed and what they are being supported on, which can be at a technological, administrative, political level, among others.

Table 3. Proposed Solutions Related to the Formulation of Projects for Cybersecurity Governance

Proposed solution	Objective or Support	Potential Impact	Ref.
A comparison is made of cybersecurity governance awareness from the point of view of the young, educated, and tech-savvy population.	Promote global cyber governance guidelines and practices.	Cybersecurity policies in the UAE and USA.	(Shah et al., 2023)
IT Service Management and IT Security.	COBIT 2019 Framework.	Managed Service Requests and Incidents.	(Saputra et al., 2022)
Digital governance using blockchain and frameworks.	Deep learning.	Interoperability and data exchange.	(Malik et al., 2023)
Framework through theory regarding the dynamic capability view (DCV).	Application of moderate technologies.	Digitization of information.	(Kok & Teoh, 2021)
Evaluating existing cybersecurity frameworks.	Misinterpretation in the implementation of cybersecurity frameworks.	Agile cybersecurity that integrates technology and culture.	(Handri et al., 2024)
Comprehensive cybersecurity framework with five interconnected algorithms.	Cybersecurity methodologies, with a dynamic and adaptive approach.	Protection against spreading cyber threats.	(Pandey et al., 2024)
Comprehensive approach to master data management (MDM).	Synthesize methodologies and best practices.	Integrated strategies.	(Pansara et al., 2024)
That data is an important factor in production in the industry.	Improving the utilization of data	Data governance.	(W. Jiang et al., 2023)

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

	resources with integrity.		
Big Data transmission is becoming more frequent and faster.	Generating more challenges for security and privacy risk governance.	Technology and regulation.	(Wang et al., 2021)
Alignment with enterprise risk management.	Risk management that is managed proactively, strategically, and comprehensively.	Cybersecurity governance management.	(Althonayan & Andronache, 2019)
The mixed partnership between AI, e-governance, and cybersecurity.	Artificial intelligence (AI), e-governance and cybersecurity.	Mediating e-governance with AI and cybersecurity.	(Bokhari & Myeong, 2023)
Information technologies are transversal in any type of company.	Implementing corporate governance and information security.	Have an adequate budget.	(Skrodelis et al., 2020)
Applying artificial intelligence (AI) to mitigate cybersecurity governance.	Diversity and complexity of AI technologies.	Specific risks of AI.	(Hamon et al., 2024)

In Table 3., you can see the different proposed solutions related to the formulation of projects for cybersecurity governance; which must be considered so that this research makes additional contributions aimed at solving the research problem.

Identification of Relevant Stakeholders Essential for Project Development and Resource Optimization

Table 4 defines 14 relevant actors who facilitate formulating cybersecurity governance projects to optimize an organization's resources. In this phase, the assessment simulation was carried out with the following considerations:

- The evaluation is from 0 to 100 points using the Likert scale.
- 14 relevant actors are evaluated.
- Five different scenarios were defined for the simulation of the evaluation.
- For the evaluation, the expert judgment technique was applied.
- For the evaluation, whole numbers without decimals must be used.
- In the simulations the Likert scale ranges are applied to the results obtained.
- The results obtained can be used as a reference for the formalization of projects in the ICT area

Likert Scale Design

The Likert scale, evaluation is composed of five ranges of options that correspond to two positive, two negative, and one neutral, this evaluation is supported by applying the expert judgment technique, below, we detail the ranges of the Likert scale with its corresponding rating defined for this case study.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Table 4. Likert Scale Design

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 4 shows the design of the Likert scale used for the evaluation in Table 5 in the five different scenarios

Table 5. Evaluating Key Stakeholders in Cybersecurity Governance Project Formalization

Relevant actors	**Scenarios**	**Scenario 2**	**Scenario 3**	**Scenario 4**	**Scenario 5**
Human resources	90,00	90,00	80,00	70,00	100,00
New technologies	70,00	80,00	60,00	80,00	95,00
Artificial Intelligence (AI)	80,00	90,00	50,00	90,00	100,00
Prototypes	80,00	80,00	70,00	100,00	95,00
Models	70,00	100,00	70,00	95,00	100,00
Project guides and methodologies	80,00	90,00	50,00	80,00	95,00
ICT methodologies	40,00	80,00	40,00	80,00	95,00
Policies	70,00	70,00	40,00	70,00	95,00
Strategies	80,00	60,00	50,00	85,00	100,00
Rules	80,00	80,00	40,00	70,00	100,00
Regulations	80,00	90,00	50,00	90,00	95,00
Frameworks and Standards	50,00	70,00	70,00	90,00	95,00
Legal basis	80,00	75,00	80,00	90,00	95,00
Resource optimization	80,00	100,00	70,00	90,00	100,00
Expert judgment evaluation	73,57	82,50	58,57	84,29	97,14

Below, we present in Figure 1, in the corresponding graph, the evaluation of the "Relevant actors for the formulation of projects for cybersecurity governance for the optimization of resources in an organization" with the following details:

- Scenario 1 and 3 correspond in the Likert table to the rating neither satisfied nor dissatisfied
- Scenario 2 and 4 correspond in the Likert table to the rating satisfied
- Scenario 5 corresponds in the Likert table to the rating very satisfied

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

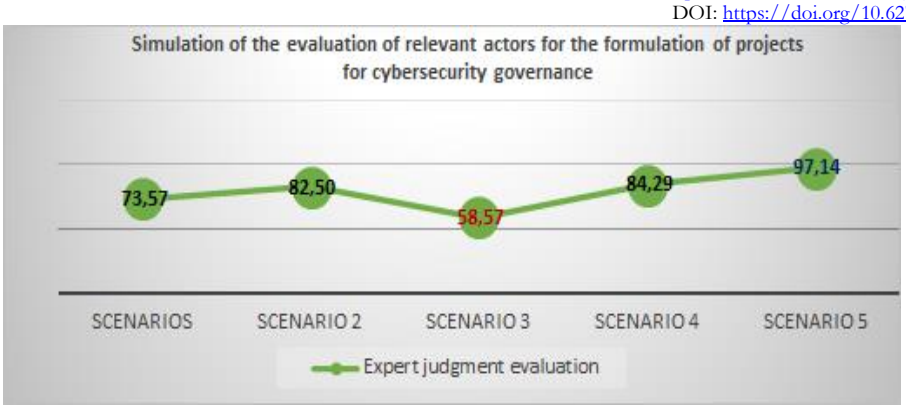

Figure 1. Simulation of the Evaluation Carried Out on the Relevant Actors

In Figure 1, we have the simulation of the assessment carried out on the relevant actors where we could observe that the results in scenarios 1 and 3 are below 75% and scenarios 2 and 4 exceed 75%. Scenario 5 has a score above 95%, being the most optimal in this simulation.

Overview of Key Actors Influencing Project Formulation

Human Resources

The human resources to carry out these activities must be from the area of ICT knowledge preferably with a minimum of ten years' experience so that they can better visualize the formulation of projects for the management of cybersecurity governance.

New Technologies

New technologies are related to updated ICT infrastructures with TIER 4 support, high availability servers in terms of hardware, and public or private Hyperledger Fabric based on blockchain, among others.

Artificial Intelligence (AI)

For the definition of projects, artificial intelligence (AI) must be considered, which is a field of computer engineering that focuses on the generation of systems that can perform tasks that normally require human intelligence, such as deep learning, reasoning, and perception. Artificial intelligence has its advantages and disadvantages, it is important to analyze when to use it.

Prototypes

Analyze the different prototypes that the organization to be evaluated has or does not have related to information security governance for a public or private organization. We must clarify that the prototype allows us to simulate or test as a final product.

Models

Models are used to present the appearance of the final product, such as a model for the formulation of a project for cybersecurity governance with resource optimization. In this research, different models were analyzed.

Project Guides and Methodologies

It is important to know if the PMI project guide, Agile methodology, and Scrum, among others, are applied in the organization to allow for adequate management of projects, applying them to all operational, tactical, and strategic processes of the organization.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

ICT Methodologies

ICT methodologies such as COBIT 2019, and ITIL, among others, are those that must be verified if organizations are applying them for the formulation of projects for cybersecurity governance management in a globalized environment.

Policies

For the assessment, security policies must be analyzed at the technical, operational, administrative, management, and governance levels; understanding the importance of security policies at the corporate level of a public or private organization

Strategies

Analyze whether public or private organizations have several business strategies such as Strategic objectives, strategic alignment, strategic sectors, strategic planning, strategic areas, and strategic investments, among others; which will influence the formulation of projects for information security governance.

Rules

These are the procedures that each of the organizations generates to improve the management of the administration processes. These standards must be supported by the legal basis of the control bodies depending on the corporate name of each organization.

Regulations

The regulations are defined as: the International Telecommunication Union (ITU) and other national and international regulations that are related to the formulation of projects for cybersecurity governance.

Frameworks and Standards

At this point, it will be evaluated whether the organization has control, program, risk frameworks, and standards such as ISO/IEC 27001 and 27002, NERC, NIST, and ISO 15408, among others, to guarantee the processes in the formulation of projects.

Legal Basis

For the formulation of a project for the management of cybersecurity governance for the optimization of resources in an organization, it must be subject to a legal basis, internal policies and guidelines such as the mission, vision and strategic objectives of the organization.

Resource Optimization

To optimize resources when formulating a project for managing information security governance in an organization, the following must be considered: assess the viability, profitability, and sustainability; consider the technical, economic, social, and even environmental aspects if the project warrants it.

Algorithm for Project Formulation Using Flowchart Techniques

The proposed algorithm for formulating a cybersecurity governance management project outlines the processes an organization must follow to develop IT-related projects. This serves as a structured alternative to guide project development before the analysis phase.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Figure 2 details the phases for the formulation of projects for the management of cybersecurity governance, which are detailed below.

Description

First phase: Formulation of a cybersecurity governance management project for resource optimization in an organization: In this process, defined as the first phase, we collect information taking into consideration the research topic and that the information is preferably no older than five years.

Second phase: Information analysis: To carry out the previously determined analyses that the information is related to the identification of the problem, related work and information related to standards, prototypes, models, frameworks and Standards for Cybersecurity, methodologies, policies among others.

Third phase: Conceptualization, Indicators and Solutions: In this phase we determined three processes that correspond to the methodology regarding the analysis of the relevant information to reach the two processes that are the results obtained in this research.

Fourth phase: Processes to simulate the evaluation: In the first instance, the Likert scale design was carried out where the parameters for the evaluation were defined, in the following process the evaluation is carried out applying the expert judgment techniques, to then obtain the simulation of the evaluation of the relevant actors.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

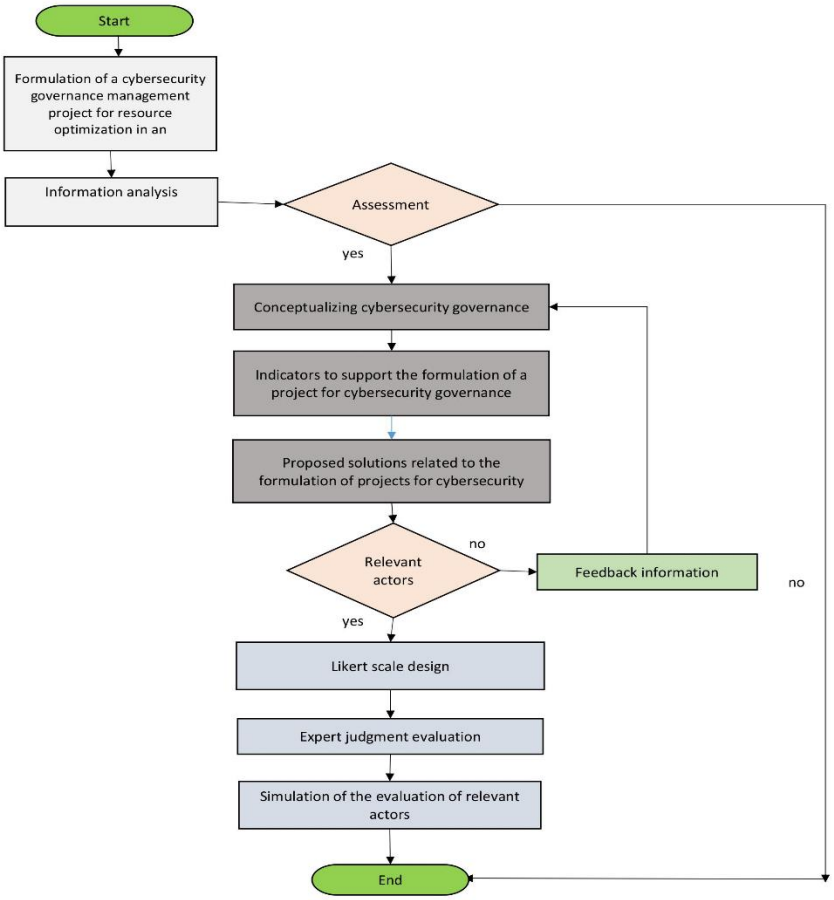

Figure 2. Algorithm for Formulating Projects for Cybersecurity Governance

Discussion

The results regarding the Relevant Actors for the formulation of projects for cybersecurity governance for the optimization of resources in an organization and the Algorithm for the formulation of projects using flowchart techniques are alternatives to improve project management that none of the authors of the references present, being our new contribution in this research and in the first result we have adopted the generation of indicators and the second result we have identified the solutions of the authors of the reference considering as the adoption of knowledge. to improve.

In this research, evaluations, and simulations are conducted using the Likert scale and expert judgment to assess the 14 key actors influencing the analysis and formulation of cybersecurity governance projects aimed at optimizing organizational resources. However, the actual implementation of the project is not carried out.

Our results provide an alternative approach to conducting the analysis required for formulating cybersecurity governance projects aimed at optimizing organizational resources. Additionally, most authors cited in the introduction and related works agree that challenges persist in managing ICT projects, highlighting the importance of new contributions in this area.

The results provide an alternative approach for formulating cybersecurity governance projects to optimize organizational resources. This approach can be applied during the analysis phase in organizations worldwide that share similar cultures and technological characteristics.

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Future Work and Conclusions

In the near future, this research will continue, and the results obtained will be applied to implement a cybersecurity governance project within an organization. The implementation will follow the phases of analysis, planning, monitoring, control, and closure, focusing on optimizing organizational resources.

The results of the simulation, evaluated using the Likert scale and expert judgment, indicate varying levels of satisfaction across different scenarios. In scenarios one and three, satisfaction levels were below 75%, classifying them as dissatisfied. Scenarios two and four showed satisfaction levels between 76% and 94%, indicating general satisfaction. Scenario five achieved the highest satisfaction, with results ranging from 95% to 100%, reflecting a very satisfied response. These findings present an alternative for enhancing project management.

The results obtained on indicators supporting the formulation of a cybersecurity governance project are highly relevant during the analysis phase. These indicators will be essential for conducting future evaluations in these areas, contributing to more effective governance and resource optimization.

The research concludes that identifying proposed solutions for cybersecurity governance project formulation enhances clarity regarding the contributions of referenced authors. This process facilitates the adoption of relevant insights during project implementation, ensuring more effective and efficient management.

In conclusion, for successful project formulation, all relevant actors must achieve a satisfaction level exceeding 75%.

Authors' Contributions

All authors collaborated in the process of elaboration of the article. Rodrigo Del Pozo Durango, Moises Toapanta, and Pamela Toapanta Pavón worked mainly on the Introduction, Analysis of the administrative processes, Summary and Review of all phases of the article, and the Literature. Zharayth Gómez and Roció Llumiquinga A. mainly in the methodology, search for information and results, and Roció Maciel A., Antonio Orizaga T., mainly in the selection of the validation scales, discussion, and conclusions.

Author Ethical Declarations

We confirm that the work has not been published elsewhere in any form or language

Funding Information: No funding was received for conducting this study.

Conflict of Interest: The authors state no conflict of interest.

Declaration of Interests

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.

References

Alanis Hernández, E., López Sandoval, E., Colín Morales, J. M., Viñas Álvarez, S., & Sosa Sales, A. (2024). Ciberseguridad: Impacto y Detección de Eventos de Seguridad Mediante Prototipo de Monitoreo. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(3), 2975–2989. https://doi.org/10.37811/cl_rcm.v8i3.11511

Almagro, L. (2019). Ciberseguridad: Marco Nist. In *White Paper Series: Vol. Edición 5* (p. 20). https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Althonayan, A., & Andronache, A. (2019). Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment. *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019*, 1–9. https://doi.org/10.1109/CyberSA.2019.8899445

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

Bokhari, S. A. A., & Myeong, S. (2023). The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective. *IEEE Access*, *11*(July), 69783–69797. https://doi.org/10.1109/ACCESS.2023.3293480

Boris Delgado Riss, C. M. F. (2024). ISO/IEC 27001 y ENS, binomio perfecto para la ciberseguridad. *AENOR La Revista de Evaluación de Conformidad*, *1*(1), 1–2. https://revista.aenor.com/348/isoiec-27001-y-ens-binomio-perfecto-para-la-ciberseguridad.html

Bravo, C. R. (2024). *Ventajas de un Modelo de Madurez en Ciberseguridad*.

Cai, T., Cai, H. J., Wang, H., Cheng, X., & Wang, L. (2019). Analysis of Blockchain System With Token-Based Bookkeeping Method. *IEEE Access*, *7*, 50823–50832. https://doi.org/10.1109/ACCESS.2019.2911124

Cobit 2019. (2019). Governance and Management Objectives. In *COBIT® 2019 Framework*. https://netmarket.oss.aliyuncs.com/df5c71cb-f91a-4bf8-85a6-991e1c2c0a3e.pdf

Delgado, J., Galárraga, F., Fuertes, W., Toulkeridis, T., Villacís, C., & Castro, F. (2016). A proposal of an entity name recognition algorithm to integrate governmental databases. *2016 3rd International Conference on eDemocracy and eGovernment, ICEDEG 2016*, 26–33. https://doi.org/10.1109/ICEDEG.2016.7461472

Del-Real, C., & Díaz-Fernández, A. M. (2022). Understanding the plural landscape of cybersecurity governance in Spain: a matter of capital exchange. *International Cybersecurity Law Review*, *3*(2), 313–343. https://doi.org/10.1365/s43439-022-00069-4

Dimitriadis, A., Lontzetidis, E., Kulvatunyou, B., Ivezic, N., Gritzalis, D., & Mavridis, I. (2023). Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks. *IEEE Access*, *11*(January), 728–743. https://doi.org/10.1109/ACCESS.2022.3233404

Ecuador, M. D. T. Del. (2022). Estrategia Nacional de Ciberseguridad. *Estrategia Nacional de Ciberseguridad*, *1*(2), 31. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2022/10/Difusion-ENC.pdf

Eduardo Leyva-Méndez, A. I. (2021). Análisis de políticas públicas de seguridad cibernética. Estudio del caso ecuatoriano Analysis of public cyber security policies. Ecuadorian case study Análise de políticas públicas de segurança cibernética. Estudo de caso equatoriano. *Polo*, *56*(3), 1229–1250. https://doi.org/10.23857/pc.v6i3.2431

Escobar, D. S. (2022). Análisis de los modelos de madurez cultural de la Ciberseguridad. *Publicaciones de La Comisión de Estudios Sobre Sistemas de Registro*, *1*(1), 1–11.

Financie Crimen Academy. (2024). *Comprender la gobernanza de la ciberseguridad*. Financialcrimeacademy. https://financialcrimeacademy.org/es/comprender-la-gobernanza-de-la-ciberseguridad/#:~:text=La gobernanza madura de la,y visi%C3%B3n general del banco.

Foundation, e-Governance Academy 90007000, C. code: (2024). *National Cyber Security Index (NCSI)*. Www.ega.ee. 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-

Guerrero, M., Martinez, M., & Gualotuña, L. (2024). *Esquema Gubernamental De Seguridad De La Informacion (Egsi)* . Registro Oficial.

Hamon, R., Junklewitz, H., Soler Garrido, J., & Sanchez, I. (2024). Three Challenges to Secure AI Systems in the Context of AI Regulations. *IEEE Access*, *12*(April), 61022–61035. https://doi.org/10.1109/ACCESS.2024.3391021

Handri, E. Y., Indra Sensuse, D., & Tarigan, A. (2024). Developing an Agile Cybersecurity Framework With Organizational Culture Approach Using Q Methodology. *IEEE Access*, *12*(August), 108835–108850. https://doi.org/10.1109/ACCESS.2024.3432160

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

Jiang, Y., Jeusfeld, M. a., Ding, J., & Sandahl, E. (2023). Model-Based Cybersecurity Analysis: Extending Enterprise Modeling to Critical Infrastructure Cybersecurity. *Business and Information Systems Engineering*, *65*(6), 643–676. https://doi.org/10.1007/s12599-023-00811-0

Journal of Ecohumanism
2025
Volume: 4, No: 1, pp. 560 – 579
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i1.5837

Kesan, J. P., & Zhang, L. (2021). An empirical investigation of the relationship between local government budgets, IT Expenditures, and cyber losses. *IEEE Transactions on Emerging Topics in Computing*, *9*(2), 582–596. https://doi.org/10.1109/TETC.2019.2915098

Kok, C. H., & Teoh, A. P. (2021). Conceptualizing Cybersecurity Management Impact on Performance: Agility and Information Technology Governance. *2021 IEEE International Conference on Computing, ICOCO 2021*, 196–201. https://doi.org/10.1109/ICOCO53166.2021.9673548

La, M. D. E. S. D. E. (2024). *Modelo de la seguridad de la información y ciberseguridad.*

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.

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

Ministerio de telecomunicaciones y de la sociedad de la Información. (2024). *Por primera vez Ecuador cuenta con su Estrategia Nacional de Ciberseguridad.* Sistema Nacional de Información (SNI). https://www.telecomunicaciones.gob.ec/por-primera-vez-ecuador-cuenta-con-su-estrategia-nacional-de-ciberseguridad/

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

Pansara, R. R., Vaddadi, S. A., Vallabhaneni, R., Alam, N., Khosla, B. Y., & Whig, P. (2024). Fortifying Data Integrity using Holistic Approach to Master Data Management and Cybersecurity Safeguarding. *Proceedings of the 18th INDIAcom; 2024 11th International Conference on Computing for Sustainable Global Development, INDIACom 2024*, 1424–1428. https://doi.org/10.23919/INDIACom61295.2024.10498671

Ramos, S., & Ellul, J. (2024). Blockchain for Artificial Intelligence (AI): enhancing compliance with the EU AI Act through distributed ledger technology. A cybersecurity perspective. *International Cybersecurity Law Review*, *5*(1), 1–20. https://doi.org/10.1365/s43439-023-00107-9

Rea Guaman, M., Calvo Manzano, J. a, & San Feliu, T. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas. *CISTI (Iberian Conference on Information Systems & Technologies*, *1*(1), 1–7. https://eds.p.ebscohost.com/eds/detail/detail?vid=2&sid=6fd3e720-dbd3-4f3c-afd9-c20133beff8a@redis&bdata=JkF1dGhUeXBlPWlwLHNzbyZsYW5nPWVzJnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ==#AN=134951367&db=aps

Saputra, K. S., Isnaini, M., Tasya Agrefine, S., Mariam, S., & Candiwan. (2022). Analysis of Information Technology Governance on Process Management Services and Management of Information Technology Security Using COBIT 2019 (Case Study: PT XYZ). *2022 IEEE 8th International Conference on Computing, Engineering and Design, ICCED 2022, 2019*, 1–6. https://doi.org/10.1109/ICCED56140.2022.10009924

Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance. *IEEE Access*, *11*(July), 87970–87984. https://doi.org/10.1109/ACCESS.2023.3296580

Skrodelis, H. K., Strebko, J., & Romanovs, A. (2020). The Information System Security Governance Tasks in Small and Medium Enterprises. *2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2020 - Proceedings*, 0–3. https://doi.org/10.1109/ITMS51158.2020.9259305

Student, P. D., Moisés, S., Toapanta, T., Luis, P. D., & Mafla, E. (2016). Security analysis of civil registry database of Ecuador. *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) - 2016*, 1024–1029.

Toapanta, S. M., Escalante Quimis, O. A., Mafla Gallegos, L. E., & Maciel Arellano, M. R. (2020). Analysis for the evaluation and security management of a database in a public organization to mitigate cyber attacks. *IEEE Access*, *8*, 169367–169384. https://doi.org/10.1109/ACCESS.2020.3022746

Toapanta, S. M. T., Durango, R. H. D. P., Gallegos, L. E. M., Arellano, M. R. M., Trejo, J. A. O., & Hifong, M. M. B. (2022). Suitable Professional Identity Analysis to Improve Information Security Governance. *Proceedings of the 2022 International Conference on Computer, Information and Telecommunication Systems, CITS 2022*, 0–3. https://doi.org/10.1109/CITS55221.2022.9832999

Toapanta, S. M. T., Ochoa, I. N. C., Sanchez, R. A. N., & Mafla, L. E. G. (2019). Impact on administrative processes by cyberattacks in a public organization of Ecuador. *Proceedings of the 3rd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2019*, 270–274. https://doi.org/10.1109/WorldS4.2019.8903967

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

Toapanta Toapanta, S. M., Mafla Gallegos, L. E., Chevez Moran, M. J., & Ortiz Rojas, J. G. (2020). Analysis of models of security to mitigate the risks, vulnerabilities and threats in a company of services of telecommunications. *Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020*, 445–450. https://doi.org/10.1109/ICICT50521.2020.00077

Vargas Borbúa, R., Reyes Chicango, R. P., & Recalde Herrera, L. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO - Revista Latinoamericana de Estudios de Seguridad*, *1*(20), 31. https://doi.org/10.17141/urvio.20.2017.2571

VGS Tech solutions. (2024). *Frameworks de Ciberseguridad: Modelos y Estándares*. Instituto de Geogr. Nacional. https://vgst.net/contact

Wang, X. R., Luo, W., Bai, X. L., & Wang, Y. (2021). Research on Big Data Security and Privacy Risk Governance. *Proceedings - 2021 International Conference on Big Data, Artificial Intelligence and Risk Management, ICBAR 2021*, 15–18. https://doi.org/10.1109/ICBAR55169.2021.00011

Ximena Elizabeth Orellana-Cabrera, M. D. Á.-G. (2022). Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. *Polo Del Conocimiento*, *7*(3), 706–723. https://doi.org/10.23857/pc.v7i3.3758