Journal of Computer Science

Original Research Paper

An Approach to Information Security Based on the Legal Basis for an Organization in Ecuador

[1]Diego Gustavo Andrade Armas, [2]Segundo Moisés Toapanta, [1]Eriannys Zharayth Gómez Díaz,
[3]José Antonio Orizaga Trejo, [3]Rociό Maciel Arellano and [2]María Mercedes Baño Hifóng

[1]*Research Department, Gestión de Tecnologías Para El Mundo (GTM), Quito, Ecuador*
[2]*Postgraduate Subsystems, Universidad Católica de Santiago de Guayaquil (UCSG), Guayaquil, Ecuador*
[3]*Information Systems Department of the CUCEA University of Guadalajara (UDG), Guadalajara, México*

Article history
Received: 16-03-2024
Revised: 31-05-2024
Accepted: 24-06-2024

Corresponding Author:
Segundo Moisés Toapanta
Postgraduate Subsystems,
Universidad Católica de
Santiago de Guayaquil
(UCSG), Guayaquil, Ecuador
Email: segundo.toapanta@cu.ucsg.edu.ec

Abstract: Information security issues persist at both 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. The objective of this research is to conduct an analysis of information security considering the legal framework for information technologies for an organization. The deductive method and exploratory research were used to review the information and official websites. The results obtained in this research are Indicators related to the legal basis and information security, statistical analysis of the National Cyber Security Index (NCSI), Relevant actors to globalize information security and cybersecurity based on the legal basis, Prototype supported by relevant actors and Simulation for the globalization of information security and cybersecurity. It was concluded that the statistical analysis of the National Cyber Security Index (NCSI) resulted in a score of 53.25% for Ecuador, according to the 2023 report on information security and cybersecurity. This score can be improved to 83.33% based on the results obtained from the simulation conducted in five different scenarios for the globalization of information security and cybersecurity.

Keywords: Security of the Information, Cybersecurity, Cybercrime, Cyber-Attack, Legal

Introduction

The governance and globalization of information security and cybersecurity is based on the “organic law on the protection of personal data”; which states that those responsible and in charge of processing personal data may rely on international standards for adequate risk management. The government information security mechanism will cover and apply to all public sector institutions, contained in article 225 of the constitution of the Republic of Ecuador, as well as third parties that provide public services through concession or other legally recognized figures (Arrese Vilche *et al*., 2018). Article 140 of the organic law of telecommunications provides: “Steering of the sector. The ministry in charge of the telecommunications and information society sector is the governing body of telecommunications and the information society, computing, information and communications technologies and information security.

So that organizations can operate reliably in the area of ICT, it begins with the definition of standards based on national and international standards considering: Human resources security, logical security, physical security and legal security (Salcedo Parra *et al*., 2014). The legal requirements allow us to identify the necessary controls and those designated by the risk analysis, with the use of security standards. Based on the legal basis, there are controls considered fundamental and depend on current legislation regarding Data protection and privacy of personal information, protection of the organization's records and intellectual property rights. The importance of the application of legislation is to identify specific legal aspects, which must be considered in all phases of information security (legislation varies from country to country) (Cárdenas-Solano *et al*., 2016). The regulatory framework is based on the legal basis of 22 documents between laws and regulations defined by the Spanish Foundation for

Science and Technology (FECYT) (FECYT, 2022). The authors state that the problems of information security management can be mitigated with Privacy policies, security policies, policies for personnel recruitment and legal policies, among others, supported by the legal basis and legislation of the country where it is located. the organization to achieve business continuity compliance; with national and international standards (Alabdullatif *et al.*, 2018). The characteristics of information security are confidentiality, integrity and authentication to mitigate risks, vulnerabilities and threats. The authors call this concept multimedia security; with the use of the basic element of machine learning, of reservoir computing supported by a chaotic scheme. The same ones consider the technological and legal aspects of the use of machine learning elements (Kushnir *et al.*, 2020). They analyze Artificial Intelligence (AI) considering the vision of the right to the protection of personal data supported by the legal basis regarding the right to privacy. AI is mainly applied for the mass processing of information (which may contain personal data). The legal framework is robust regarding personal data in Mexico and other countries; where some of the challenges for safeguarding rights have been identified when it comes to technological environments, specifically with artificial intelligence (Andrea and Enríquez, 2021).

Why is it necessary to adopt an information security approach based on the legal framework of a country for an organization in Ecuador?

To provide the necessary arguments that will enable us in the future to identify how to mitigate risks, vulnerabilities and threats in information management based on the legal framework so that information is managed with confidentiality, integrity and availability.

The objective of this research is to conduct an analysis of information security considering the legal framework for information technologies for an organization.

The results obtained are Indicators related to the legal basis and information security, statistical analysis of the National Cyber Security Index (NCSI), relevant actors to globalize information security and cybersecurity based on the legal basis, prototype supported by relevant actors and simulation for the globalization of information security and cybersecurity.

It is concluded that the statistical analysis of the National Cybersecurity Index (NCSI) yielded a score of 53.25% for Ecuador, according to the 2023 report on information security and cybersecurity. This score can be improved to 83.33% based on the results obtained from the simulation conducted in five different scenarios for the globalization of information security and cybersecurity.

Materials and Methods

Materials

The different trends expressed by the authors of the different articles detailed below regarding the legal basis in information security and cyberattacks were analyzed.

They strengthen the fundamental right to protection of personal data, through the formulation and execution of public policies in Ecuador, considering the right to data protection in the constitutional state of rights and justice, public policies and the need to redefine prevention and awareness. They define a study methodology diagram under the following structure: Secondary information (digital repository, https://vlex.ec, constitutional court and legislation, doctrine and scientfic articles), comparative law (Argentina and Uruguay) and public policy (right to the protection of personal data) (Ordóñez Pineda *et al.*, 2022). The science of law and computer science, through computer law and legal informatics, are currently linked through Information and Communications Technologies (ICT). One of the authors defines an equation right + computer science + information society = computer law. The areas of application are Improper manipulation of data, the crime of computer espionage, computer sabotage, program piracy, homicide, qualified theft, malicious and negligent electronic access and computer falsification. Legal Informatics was born in the United States in 1959. The areas of application are Documentary legal informatics, management and control legal informatics, decision-making legal informatics, or meta-documentation. The science of law and computer science have been part of this multidisciplinary transformation process, with the aim of satisfying the current needs of humanity (Aguilar, 2015). The Ministry of Information and Communications Technologies-Min ICT is the entity in charge of designing, adopting and promoting policies, plans, programs and projects in the information and communications technologies sector. Privacy is understood as the right that all information holders have in relation to information that involves personal data and classified information that they have delivered or is in the possession of the entity within the framework of the functions that it is responsible for. protect information based on the current legal framework. For implementation, the organization must design a privacy model that allows it to comply with the minimum requirements based on legal bases and generate a privacy policy that allows the correct management of the information (M.I.N.T.E.L, 2015). In Colombia, they carried out the Legal evaluation of the DPI in telecommunications Networks referring to internet providers and ISP companies regarding the privacy of user information, taking as reference the legislative implications in some countries such as the United States of America and Canada regarding the internet governance that plays a key role within legal and technological service models considering the main organizations that govern the Internet such as Iana, Latino American, Lactld, Internic, Lacnic. They concluded that package inspection, or DPI, enforcement must be sufficiently considered, respectful and limited by laws and regulations (Salcedo Parra *et al*., 2015). The authors analyze several approaches regarding the problem of cyberattacks in the exchange of information in public and private organizations regarding indicators of commitment; tactics, techniques and procedures used by threat actors; and Suggested actions to detect, contain, or prevent attacks. The sources they use most are the privacy and data protection laws. Among the laws and regulations that they considered the most are: The laws and regulations in the European Union (EU), Laws and regulations in Norway and the US and Legal Implications of CTI Sharing. They state that the NIS directive has three main parts, which are: National capabilities, cross-border collaboration and national supervision of critical sectors (Nweke and Wolthusen, 2020). They propose a new perspective for the quantitative analysis of empirical experience supported by the legal basis. They carried out an analysis of the influence of normative legal documents on enterprise financing and the impact of the new third board listing system on enterprises' financing (Yang *et al*., 2019). They developed and implemented a method to synthesize threat and risk structures for information security based on a fuzzy approach. They used the method to model threat structures based on structural abstractions. They created a database with fuzzy rules based on procedural abstractions (Volkov *et al*., 2020). In this article, the authors defined that the software must be based on a legal basis according to the country's legislation. In the case of Europe, it is based on regulation 2017/745 of the European Parliament and the (MDR-Medical Device Regulation) that is currently in force. is current. They concluded that software must support cybersecurity standards (Lhotska, 2021). In Russia, various projects are being developed in the field of digital government, so that citizen records are used appropriately by public and private entities; a digital profile should be a digital consent system designed to transfer data from state records to other persons with compliance with current legislation and practice, as well as international practice to implement in similar solutions and projects. They conclude that the important thing is to generate trust (Bundin *et al*., 2023). Legal support is required to combat cybercrime and information management crimes, acts that were adopted in EU countries and the standards defined by the UN. They analyze the issues of methodology in cybercrime to suppress, cybercrime as found in legislation, fighting cybercrime in intergovernmental organizations: The EU and the United Nations. They concluded that legal instruments are formalized in the form of treaties, agreements, memorandums, resolutions, directives, recommendations, decisions, sanctions, declarations, economic, joint investigations and information, among others (Flissak *et al*., 2021). During the 2013 floods in Germany and Austria, they used social networks for communication to carry out prevention and save lives. They carried out a case study based on German Facebook corpus and Twitter messages with the aim of verifying the potential of each of them. They analyzed the two main challenges which are; information overload and legal issues. They consider social networks as a new paradigm and analyze Social networks in disaster management, digitalization of communication and information and automatic processing of social networks. They carried out the analysis of two flood tables, one using indicators from Facebook and the other from Twitter. They indicated that if there is a legal basis for accessing personal data in the event of disasters under data protection law, it becomes weak with respect to the law (Grunder-Fahrer *et al*., 2016). The authors defined the strategies, policies and legal obstacles facing the implementation of e-government in Afghanistan. They carried out the analysis on 387 employees from 10 organizations. They determined that a legal basis is needed for electronic government. One of the limitations they determined was that the survey has a geographical limit of Kabul, which is the capital of Afghanistan. The results obtained in the research contribute to filling a fraction of the knowledge gap on the strategy, policy and management of the e-government sector and legal barriers (Ismail *et al*., 2022). The constant threats in maritime traffic in the People's Republic of China have seen the need to implement security systems for ships, supported by the security law of the people's Republic of China 2021, considering the legal basis of this system under its jurisdiction. This system is based on the MTSL2021, which consists of security levels with plans and measures supported by the legislation of articles 12,32 and 38 of the MTSL 2021, based on the security law of the people's Republic of China of 1983 (Zhang and Hu, 2021). They analyzed the legal scenario of data governance in Europe; how it has evolved and how artificial intelligence is advancing in this area. They briefly analyzed the provisions of the GDPR applicable to the regulation of algorithms, after examining recent jurisprudence where the legal aspects of the regulation of algorithms have been the basis of the decisions handed down. On the legal basis they take into consideration that the application of algorithms is discriminatory for the worker, they take into consideration the case of Italy. The Bologna court issued an injunction against the food delivery company prohibiting the use of the software for scheduling (Zallone, 2021). Companies require a legal aspect to mitigate the risks, vulnerabilities and threats that are constant in the competitiveness, reliability and dynamic stability of the company, they consider that technology should be used, but with fuzzy modeling. Companies require legal and technological protection to avoid being struck down by cybercrime, cybercrime and cyberterrorism. They concluded that management is required based on the formation of an analysis system and tools to analyze and evaluate bankruptcy, probability and state according to the parameters established (Kuzmynchuk *et al*., 2021). They determined that cyberattack models are alternatives to mitigate the risks of information loss and kidnapping, but they must be supported by a legal basis. They carried out an analysis with information from 2020 using SPSS to generate statistics on the current situation of an organization. They determined that it must be supported by five axes: Techniques and procedures, organization, capacity, compliance with international standards and legal basis (Durmus and Varol, 2021). The authors consider that the basis for mitigating information security risks is the statistical evaluation of information security incidents and cyber-attacks that organizations receive. They determine that traditional evaluations applying standards such as ISO27000 are not sufficient, it is necessary to adapt the provisions of the basic model of the standards to the specific operating conditions of the organization (Semin *et al*., 2017).

Methods

In this research, the IMRYD research methodology and the deductive method were applied to analyze information from the references used.

We then defined a four-phase methodology to describe the different activities to achieve the results, which can be repeated in similar scenarios.

First Phase

The information from the references related to the problems regarding information security management that is defined in the Introduction was analyzed referring to how the legal basis influences to mitigate the risks, vulnerabilities and threats so that information management is with confidentiality, integrity and availability (CIA). Considering that information security must be with privacy for this analysis.

Second Phase

To continue with the analysis, methodologies and national and international standards regarding information security management are considered, such as ISO 27001 and Cobit2019, among others.

Third Phase

Applying the expert judgment methodology, the articles of the (Ordóñez Pineda *et al*., 2022; Semin *et al*., 2017) the same ones that directly support that for the management of information security, it is necessary and mandatory to have a legal basis. With this information, a result will be generated regarding indicators.

Fourth Phase

Finally, it is clarified that the methodologies we use to reach the results are: The judgment of experts in the area of ICT knowledge, the Likert scale and legal basis.

Results

The results obtained are the following:

- Indicators related to the legal basis and information security
- Statistical analysis of the National Cyber Security Index (NCSI)
- Relevant actors to globalize information security and cybersecurity based on the legal basis
- Prototype supported by relevant actors
- Simulation for the globalization of information security and cybersecurity

The results obtained are based on the information analyzed from the introduction phase, materials and methodology where we define four phases to reach the results.

Indicators Related to the Legal Basis and Information Security

Most relevant indicators that should be considered in an analysis. In Table 1, the indicators were generated based on the reference articles supported by the legal basis that have a direct influence on the management of information security, cyberattacks and cybercrime.

Table 1: Indicators related to the legal basis

Indicator	Type	Ref.
Public policies, considering the right to data protection	Legal	Ordóñez Pineda *et al*. (2022)
Equation law + computing + information society = law	Legal	Aguilar (2015)
Public privacy policies	Legal	M.I.N.T.E.L. (2015)
Internet governance such as Iana, Latino Amer icann, Lactld, Internic, Lacnic	Technical/legal	Salcedo Parra *et al*. (2015)
Engagement, tactics, techniques and procedures used by threat actors	Legal	Nweke and Wolthusen (2020)
Quantitative analysis of empirical experience	Laws regulations	Yang *et al*. (2019)
Synthesize threat and risk structures	Diffuse focus	Volkov *et al*. (2020)
Cybersecurity standards	Legislation	Lhotska (2021)
Digital consent designed to transfer data	Legislation	Bundin *et al*. (2023)
Cybercrime methodology to repress	Legal	Flissak *et al*. (2021)
Information overload and legal issues in social networks	Legal	Gründer-Fahrer *et al*. (2016)
Strategies, policies and legal obstacles	Legal barrier	Ismail *et al*. (2022)

Table 1: Continue

Security levels with plans and measures	Law	Zhang and Hu (2021)
Legal aspects of algorithm regulation	Legal	Zallone (2021)
Competitiveness, reliability and dynamic stability	Technical/legal	Kuzmynchuk *et al.* (2021)
Risks of information loss	Legal	Durmus and Varol (2021)
Statistical evaluation of information security incidents, cyber-attacks	Standard/legal basis	Semin *et al*. (2017)

Statistical Analysis of the National Cyber Security Index (NCSI)

The NCSI indicators were developed according to the national cybersecurity framework. They present the fundamental cyber threats: Denial of electronic services: Services are not accessible, Violation of data integrity: Unauthorized modification and violation of data confidentiality. The processes were developed in 5 steps for each country: The identification of cyber threats at the national level, identification of cybersecurity measures and capabilities, selection of important and measurable aspects, development of cybersecurity indicators and Grouping of cybersecurity indicators (EGA Foundation, 2023).

The NCSI focuses on measurable aspects of cybersecurity implemented by the central government of each country, detailed below:

- Current legislation-legal acts, regulations, orders, among others
- Established units: Existing organizations, departments, among others
- Cooperation formats: Committees, working groups, among others
- Results: policies, exercises, technologies, websites and programs, among others (EGA Foundation, 2023)

With the background presented and supported by the analysis of expert judgments in the area of information security and cybersecurity, among others; Ecuador has 53.25% in the management of information security according to the analysis carried out with the available information.

Figure 1, the analysis carried out by the NSI is taken into account to visualize what percentage of security ecuador has.

Relevant Actors to Globalize Information Security and Cybersecurity Based on the Legal Basis

Figure 2 defines the relevant actors, with the aim of improving governance, globalization of information security, cybersecurity, cybercrime and cyberattacks, below, we make the respective descriptions of each of them.

Below we make a general description of each of the relevant actors, which must be supported by the legal basis.

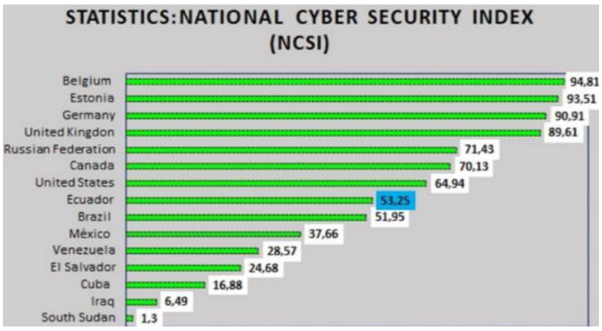

Fig. 1: Information security percentages according to (Foundation, 2023)

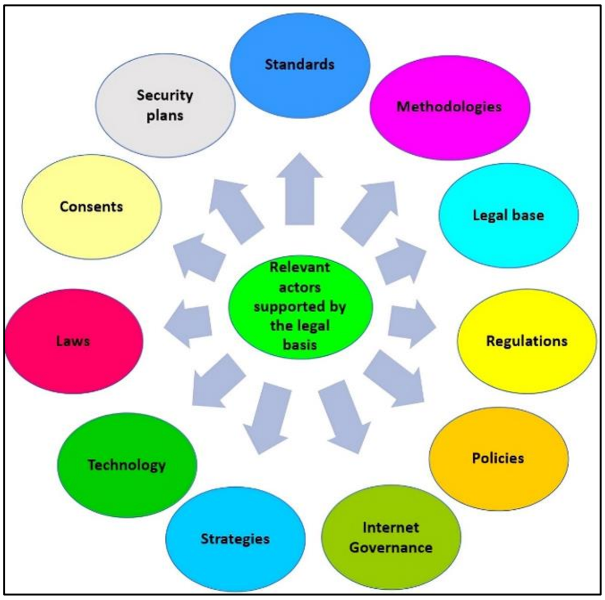

Fig. 2: Relevant actors for the globalization of information security

Standards

It is important to mention the following information security standards: ISO 27001, ISO 27701, ISO 27019. ISO/IEC 27000: Information Security Management (ISMS). ISO/IEC 27032: Guidelines for cybersecurity ISO/IEC 27033 among others; that should be considered to mitigate information management risks.

Methodologies

It refers to the way in which risks, threats and vulnerabilities will be mitigated, such as the COBIT 2019 methodology and ISO 27001, among others.

Legal Basis

The legal basis is supported by jurisprudence, laws and regulations of a country that determines the importance of the management of information security, cybersecurity and cybercrime, among others.

Regulations

The regulations are based on the legal basis that allows us to generate so that organizations have information management based on: Identification, Authentication and Audit (IAAA) so that the information is adequately managed with confidentiality, integrity and availability (INC).

Policies

Information security and privacy policies are based on the confidentiality, integrity and availability of information. The policies are administrative (governance, strategic, tactical and operational), technical, risk, technological, access and good practices, among others.

Internet Governance

It refers to the internet government of all internet service provider companies known as ISPs that are located locally or anywhere in the world.

Strategies

Strategies are those defined using the strengths, opportunities and weaknesses (SWOT) of an organization related to the management of information technologies, cybersecurity and cybercrime.

Technologies

It is the information and communications technology infrastructure that an organization has such as a data center (TIER 1, 2, 3, or 4), servers and networking equipment, among others.

Laws

It refers to the laws in force in each country based on the constitution of the republic related to information security, cybersecurity, cyber-attacks and the legal basis.

Consents

For access to data and information on social, professional networks and different organizational systems.

Security Plans

The security plans are supported by the information technology plan (PETI) to comply with the institution's strategic plan.

Prototype Supported by Relevant Actors

In the prototype that we propose according to Fig. 3, the vulnerabilities and threats that can generate a risk are identified to reduce the risk in the integrity of the data, strategies for mitigation are defined, an action plan is prepared based on the relevant actors in Fig. 2, implement and monitor strategies for mitigation.

Figure 3, in phase two, the vulnerability cycle is depicted, which will be maintained with the definition of an internal process to identify, evaluate, prioritize, correct and measure how to mitigate the vulnerability, which will be linked to a threat, in order to establish a level of control over vulnerabilities in an IT process.

Information security vulnerabilities are categorized as low, moderate, severe and critical and they differ according to the priority level. To conduct this activity, a risk matrix supported by ISO 27001 and other standards can be utilized.

Simulation for the Globalization of Information Security and Cybersecurity

The simulation was carried out with the following steps supported by expert judgment:

- Five scenarios were considered for the simulation
- Number of risks identified according to a risk matrix
- Number of high risks based on a risk matrix
- Mitigation capacity by applying relevant actors Fig. 2. To carry out this activity, the randomness or weighting function can be used according to the scenario of each organization
- Security level
- Security percentage

The formula we use for this simulation is:

$$= ((1 - (D4/C4))/E4) \tag{1}$$

where:

0, 1-1: It is the maximum probability in random form
D4 : Corresponds to the number of high and critical risks
C4 : Number of identified risks
E4 : Mitigation capacity applying relevant actors Fig. 2

To read this simulation, a scale from 1-100 was defined.

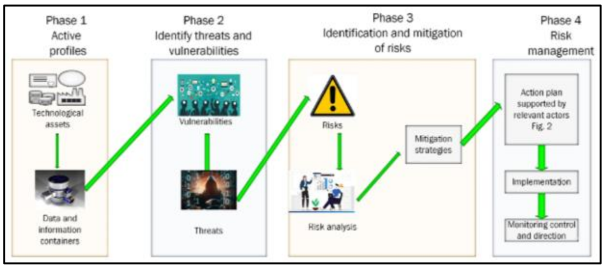
Phase 1
Active profiles
Technological assets
Data and information containers
Phase 2
Identify threats and vulnerabilities
Vulnerabilities
Threats
Phase 3
Identification and mitigation of risks
Risks
Risk analysis
Mitigation strategies
Phase 4
Risk management
Action plan supported by relevant actors Fig. 2
Implementation
Monitoring control and direction

Fig. 3: Prototype supported by relevant actors

Table 2: Scale to determine the security level

Score	Security level
76-100	Excellent
51-75	Very good
25-50	Good
0-24	Low

b. Scale for reading security level

Table 2 allows us to define each of the simulated scenarios in which range it is located; with the objective of formulating strategies to mitigate risks, vulnerabilities and threats in the globalization of information security and cybersecurity. It is important to mention that all the relevant actors defined in Fig. 2 must be supported by the legal basis, laws and jurisprudence according to the legislation of each country.

Discussion

In this research, the sequence of general steps is carried out in the methodology phase prior to obtaining the results, but the implementation is not carried out.

The authors of the references of Ordóñez Pineda *et al.* (2022); Semin *et al*. (2017) mention the importance of the legal basis in the globalization of information security and cybersecurity; our additional contribution to this research is the definition of indicators for the analysis of information security, statistical analysis of the National Cyber Security Index (NCSI), definition of relevant actors to globalize information security and cybersecurity supported by the legal basis. Security prototype to mitigate vulnerabilities, threats and information risks and Simulation for the globalization of information security and cybersecurity.

Our contributions in this research are an alternative to mitigate the risks, threats and vulnerabilities in information management, which can be applied in any public or private organization with similar characteristics based on the legal basis of each country.

Conclusion

Future research efforts in the short term will focus on customizing the results obtained in this research phase to the specific scenarios of each organization, based on the legal framework of the country. The objective is to conduct simulations, implementations and their respective validations with the aim of enhancing governance management, globalizing information security, cybersecurity, cybercrime and cyberbullying, among others.

It was concluded that the legal and technical indicators obtained as results in this research for information security analysis can be used in future customized simulations and implementations to determine the diagnosis of the information security situation in an organization.

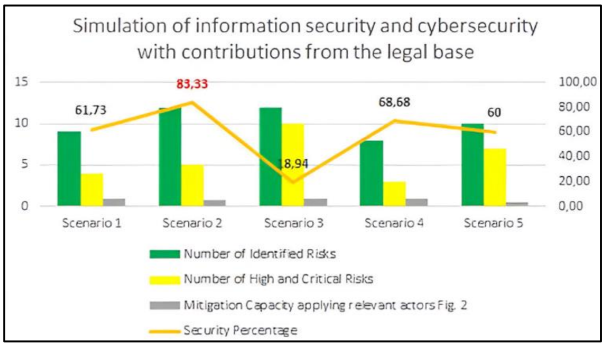

Fig. 4: Simulation for the globalization of information security and cybersecurity

The statistical analysis of the National Cyber Security Index (NCSI) yielded a score of 53.25% for Ecuador according to the 2023 report on information security and cybersecurity. This score can be improved to 83.33% according to the results obtained from the simulation conducted in five different scenarios for the globalization of information security and cybersecurity, as detailed in Fig. 4.

It was concluded that to have an information security approach based on the legal framework for an organization in Ecuador, it is necessary and essential to consider the relevant actors defined in Fig. 2, along with their respective definitions, to have a better understanding of future decision-making.

It was concluded that the security prototype presented as a result to mitigate information vulnerabilities, threats and risks allows visualization of the risk mitigation process, ensuring that security management is carried out with confidentiality, integrity and availability.

Acknowledgment

The authors thank the Research Department, Gestión de Tecnologías Para El Mundo (GTM), Information Systems Department of the CUCEA University of Guadalajara (UDG), Postgraduate Subsystems, Universidad Católica de Santiago de Guayaquil (UCSG). and RNI-Senescyt.

Funding Information

The authors have not received any financial support or funding to report.

Author’s Contributions

Diego Gustavo Andrade Armas: Research Identification objective, synthesis and bibliographic study. Stake in the written of the manuscript and the interpretation of the results.

Segundo Moisés Toapanta and Eriannys Zharayth Gómez Díaz: Participation in written the manuscript. The development of the questionnaire and its distribution, as well as data collection.

José Antonio Orizaga Trejo: Participation in data analysis and reference management.

Roció Maciel Arellano: Participation in the interpretation of results. Investigate previous research similar to the study.

María Mercedes Baño Hifóng: The contribution to the correction of the English language. Workflow monitoring and general monitoring.

Ethics

Our article is original and contains unpublished material. The authors confirm that they have read and approved the manuscript and that there are no ethical issues.

References

Aguilar, P. A. (2015). Derecho informático o informática jurídica? *Revista de Investigación En Tecnologías de La Información, 3*(6), 19–24. https://doi.org/10.36825/riti.03.06.003

AlAbdullatif, A., AlHarbi, A., AlAjaji, K., AlAmoudi, F., AlBrahim, R., & Nagy, N. (2018). Policy, Legal, Legislation & Compliance Risks that are caused by the absence of policies. *2018 21st Saudi Computer Society National Computer Conference (NCC)*, 1–5. https://doi.org/10.1109/ncg.2018.8593014

Andrea, O., & Enríquez, M. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *IUS Revista Del Instituto de Ciencias Jurídicas de Puebla*, *15*(48), 179–207. https://doi.org/10.35487/rius.v15i48.2021.743

Arrese Vilche, A. E., Cercado Barragán, D. B., & Benavides Burgos, O. R. (2018). *Implementación de Arquitectura de Seguridad de Red Interna y Perimetral Aplicado en un Municipio de la Provincia del Guayas* (1st Ed.). Cidepro Editorial. https://doi.org/10.29018/978-9942-792-17-4

Bundin, M., Martynov, A., & Shireeva, E. (2023). Citizen’s Digital Profile. Legal Aspects and Current Practice in Russia. *2023 9th International Conference on EDemocracy & EGovernment (ICEDEG)*, 1–4. https://doi.org/10.1109/icedeg58167.2023.10121979

Cárdenas-Solano, L. J., Martínez-Ardila, H., & Becerra-Ardila, L. E. (2016). Gestión de seguridad de la información: Revisión bibliográfica. *El Profesional de La Información*, *25*(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Durmus, O., & Varol, A. (2021). Analysis and Modeling of Cyber Security Precautions. *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*, 1–8. https://doi.org/10.1109/isdfs52919.2021.9486345

EGA Foundation. (2023). National Cyber Security Index (NCSI) [dataset]. In *EGA*. https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

FECYT. (2022). *Política de Seguridad de la Información v.1.3*. Fundación Española para la Ciencia y la Tecnología. https://www.fecyt.es

Flissak, C., Burdin, V., Kasianchuk, M., Kolomiiets, V., Tychna, B., & Mazuryk, S. (2021). International Legal Instruments and Counteraction Mechanisms Against Information Violations and Cybercrime. *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, 489–493. https://doi.org/10.1109/acit52158.2021.9548431

Grunder-Fahrer, S., Berger, C., Schlaf, A., & Heyer, G. (2016). Computational, Communicative and Legal Conditions for Using Social Media in Disaster Management in Germany. *2016 11th International Conference on Availability, Reliability and Security (ARES)*, 811–820. https://doi.org/10.1109/ares.2016.68

Ismail, E., Alariqi, A. A., Jawid, A., Wall, J., & Abdulrab, M. (2022). Strategy, Policy and Legal Barriers to E-Gov Implementation in Afghanistan. *IEEE Access*, *10*, 13800–13812. https://doi.org/10.1109/access.2022.3144198

Kushnir, M., Komarnytskyi, A., Tokarieva, K., Savchyn, N., Kroialo, P., & Toronchuk, V. (2020). Technological and Legal Aspects of the Use of Machine Learning Elements in Chaotic Information Processing Systems. *2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 713–716. https://doi.org/10.1109/picst51311.2020.9467935

Kuzmynchuk, N., Zyma, O., Shayturo, O., Kutsenko, T., & Terovanesova, O. (2021). Security-Oriented Bankruptcy Management as a Basis for Ensuring the Enterprises Competitiveness: Information and Analytical Tool and Counteracting Crime (Legal Aspect). *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, 453–457. https://doi.org/10.1109/picst54195.2021.9772179

Lhotska, L. (2021). Role of Legal Issues in Education of Biomedical Informatics. *2021 30th Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)*, 1–5. https://doi.org/10.1109/eaeeie50507.2021.9530745

M.I.N.T.E.L. (2015). *Modelo de Seguridad y Privacidad de la Información*. Diario Oficial. https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pd

Nweke, L. O., & Wolthusen, S. (2020). Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection. *2020 12th International Conference on Cyber Conflict (CyCon)*, 63–78. https://doi.org/10.23919/cycon49761.2020.9131721

Ordóñez Pineda, L., Correa Quezada, L., & Correa Conde, A. (2022). Políticas públicas y protección de datos personales en Ecuador: reflexiones desde la emergencia sanitaria. *Estado & Comunes, Revista de Políticas y Problemas Públicos*, *2*(15), 75–95. https://doi.org/10.37228/estado_comunes.v2.n15.2022.270

Salcedo Parra, O. J., Basto Maldonado, E. J., & Reyes Daza, B. S. (2014). Legal assessment of DPI in telecommunication networks in Colombia. *International Conference on Information Society (i-Society 2014)*, 228–233. https://doi.org/10.1109/i-society.2014.7009048

Semin, V. G., Kabanov, A. S., & Los, A. B. (2017). A statistical approach to the assessment of security threats information system. *2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS)*, 100–105. https://doi.org/10.1109/itmqis.2017.8085773

Volkov, A. I., Semin, V. G., & Khakimullin, E. R. (2020). Modeling the Structures of Threats to Information Security Risks based on a Fuzzy Approach. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 132–135. https://doi.rg/10.1109/itqmis51053.2020.9322869

Yang, J., Wen, X., Qu, Z., & Chang, H. (2019). Legal Empirical Research on Financing Complex Network. *IEEE Access*, *7*, 40843–40855. https://doi.org/10.1109/access.2019.2907162

Zallone, R. (2021). The Regulation of Algorithms and Artificial Intelligence under the GDPR, Case Law and Proposed Legislation. *2021 AEIT International Conference on Electrical and Electronic Technologies for Automotive (AEIT Automotive)*, 1–6. https://doi.org/10.23919/aeitautomotive52815.2021.9662940

Zhang, H., & Hu, C. (2021). China's Vessel Security System under the Background of the Revision of Maritime Traffic Safety Law of the People's Republic of China: Connotation and Development. *2021 6th International Conference on Transportation Information and Safety (ICTIS)*, 555–558. https://doi.org/10.1109/ictis54573.2021.9798581