ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 1, 108-115 (2023)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Prototype to Identify the Capacity in Cybersecurity Management for a Public Organization

Richard Romero Izurieta[1], Segundo Moisés Toapanta Toapanta[2,*], Luis Jhony Caucha Morales[3], María Mercedes Baño Hifóng[2], Eriannys Zharayth Gómez Díaz[4], Oscar Marcelo Zambrano Vizuete[4], Luis Enrique Mafla Gallegos[5], José Antonio Orizaga Trejo[6]

[1] *Faculty of Education Sciences; Universidad Estatal de Milagro (UNEMI), Milagro 091051, Ecuador*

[2] *Postgraduate Subsystems, Universidad Católica de Santiago de Guayaquil (UCSG), Guayaquil 090615, Ecuador*

[3] *Postgraduate School; Universidad Nacional de Tumbes, Tumbes 24001, Perú*

[4] *Research Department, Instituto Tecnológico Superior Rumiñahui, Sangolquí 171103, Ecuador*

[5] *Faculty of Engineering System, Escuela Politécnica Nacional (EPN), Quito 170525, Ecuador*

[6] *Information Systems Department (CUCEA), Universidad de Guadalajara, Guadalajara 44100, México*

ARTICLE INFO

Article history:
Received: 30 November, 2022
Accepted: 27 January, 2023
Online: 07 February, 2023

Keywords:
Cybersecurity
Management capacity
Public organizations
Security models
Security prototypes

ABSTRACT

Public organizations are subjected to a complex security situation, which can be addressed by permanently strengthening and evaluating their cybersecurity capabilities. The objective of this research is to develop a model to identify the cybersecurity management capacity of public organizations. The deductive method was applied for the review and analysis of criteria, factors and variables related to cybersecurity capacity in public organizations. It resulted in a model to identify the Cybersecurity Management Capacity of public organizations, with its process to assess and categorize organizations according to their level of cybersecurity capacity. It was concluded that public organizations from developed countries in cybersecurity such as Spain have better capacities (greater than 60% CMC) than less developed countries such as Ecuador (less than 60% CMC), due to the cybersecurity context where these organizations operate. To obtain a high level of cybersecurity, public organizations must have the support of the governments of the different political divisions of a country, as well as permanent international collaboration in the field of cybersecurity.

1. Introduction

Security problems in public organizations in Ecuador are persistent; the authors propose a model based on strategic planning for the evaluation of information security [1].

Cyberattacks and the consequences suffered by organizations increased by 50% in 2021 [2]. Security and risk assessment tools are required to develop digital economies capable of coping with and recovering from challenging situations [3]. Cyber threats are now sophisticated and advanced, with greater impact and on a global scale, cyber risk has evolved and this implies that organizations and their capabilities to deal with these threats must also evolve; More than 4,000 ransomware attacks occur daily, with financial losses of USD 265 billion, with an average system outage time of 19 days [4].

Given the complex security situation to which organizations are subjected, their capacities must be strengthened, with a holistic, proactive approach to prevention, permanently evaluating investments in security [5]. Organizations must work based on a well-articulated, shared strategic vision of IT, with a structure capable of ensuring improvements by making efficient use of available resources[6]. In addition to a strategic vision, controls must be implemented to ensure the information of the information and critical assets of the organization [7]. It is important that organizations have models, methodologies and tools to evaluate information security, to avoid suffering damages due to the intensification of sophisticated cyber-attacks [8].

Ecuador has a low level of capacity to combat cybercrime, related to a high rate of registered incidents according to statistics

* Corresponding Author: Segundo Moisés Toapanta Toapanta, segundo.toapanta@cu.ucsg.edu.ec

https://dx.doi.org/10.25046/aj080113

from national and international organizations [9]. Ecuador Digital is the strategy to transform the country into an information and knowledge society, implementing digital government, the efficiency of public administration and digital adoption in the social and economic sectors, through three pillars: connectivity, efficiency and cybersecurity. and innovation and competitiveness [10].

The countries of Latin America are highly exposed to cyber attacks, due to their multiple deficiencies in the regulatory and institutional framework, infrastructure and other aspects, which is why they have a low level of cybersecurity capacity, although they have made efforts to improve these capabilities [11]. One of the significant advances for cybersecurity in Latin American countries is the Network of Cyber Incident Response Teams (CSIRTs) for the member states of the Organization of American States (OAS), in Ecuador it is called EcuCERT [12].

The European Union (EU) is one of the blocks with the greatest development of cybersecurity capabilities, it has defined strategies and objectives that member countries must meet, they are aware of the importance of the external context, both national and supranational, to strengthen their ability to cybersecurity [13].

The objective of this research is to develop a model to identify the cybersecurity management capacity of public organizations.

Why is it necessary to measure the cybersecurity capacity of public organizations?

It is necessary to identify the cybersecurity management capacity to know the current information security situation of public organizations, so that through a strategic IT perspective, the organization can constantly improve cybersecurity and maintain itself at an optimal level that allows preventing and mitigating risks. and cyber threats.

Considering the main factors of cybersecurity, used by organizations and states around the world, implies improving and adding capabilities that guarantee the Confidentiality, Integrity, and Availability of information and protect your critical IT assets.

The assessment of compliance with each of the criteria for each cybersecurity factor allows us to identify the capabilities that the organization has, which must be improved with a strategic vision.

In this process, the deductive method and exploratory research are used for the analysis of information related to cybersecurity capacity.

The main results obtained are: A management model for cybersecurity based on strategic planning; process and matrices for the evaluation of the Cybersecurity Management Capacity.

Public organizations from developed countries in cybersecurity such as Spain have better capacities (greater than 60% CMC) than less developed countries such as Ecuador (less than 60% CMC), due to the cybersecurity context where these organizations operate. Hence, to obtain a high level of cybersecurity, public organizations must have the support of the governments of the different political divisions of a country, as well as permanent international collaboration in the field of cybersecurity.

Managing cybersecurity optimally involves starting with strategic planning that allows directing the resources and capabilities available to achieve the objectives established for the organization.

2. Materials and methods

2.1. Materials

The works that served as the basis for determining the main cybersecurity factors and variables in organizations are the following:

They define the cybersecurity culture, the main contributing factors and the metrics to evaluate organizations [14]. They evaluate the management of information security in public organizations [15]. To improve cybersecurity in public organizations, they recommend implementing a culture of Information Security [16]. They propose a conceptual model with a set of metrics to improve the efficiency of information security tasks [17]. Presents two models for the development of an information security assessment system for organizations [18]. Established a model of management success factors for information security in organizations [19]. They developed a security maturity model for organizations considering factors such as technology, people and infrastructure [20]. They recognize the key success factors of information security in organizations [21]. They analyzed how cybersecurity in organizations improves through the use of international standards and specific laws of a country [22]. They presented a conceptual model to manage the identity of the database of a public organization [23]. They present a prototype of a tool for security analysis and protection of organizations by joining component fault tree models and attack trees [24].

The levels of corruption in the local, national and international context are negatively related to the efficiency of investments in organizations. Some indicators that make it possible to measure corruption at the country level are the Corruption Perception Index (CPI) of Transparency International, the Corruption Control Index (CCI) of the World Bank and the Corruption Index of the International Country Risk Guide [25].

2.1.1 Internal factors

In Table 1, we differentiate 4 internal factors, the first is the "Strategic" factor, which must start with the Strategic Planning of Information Security, in order to protect the public organization from cybersecurity risks and threats; In this way, the entire organization is aligned to the mission, vision and defined strategic objectives, which end in the execution of projects in each of the areas, considering all strategic, tactical and operational organizational levels. Within any strategic management it is important to know the current state of cybersecurity of the organization, to know what we must improve, always with the support of senior management, creating an organizational culture of security that includes all staff [26].

Table 1: Internal factors

Factor	Detail	Reference
Strategic	Safety culture and awareness, align senior management, management	[14,16,19,21]

	support, security policy, training and awareness	
Technology, infrastructure and resources	Resources, hardware y software	[15,19]
Organization / Management	Procedure and organization, norms, international standards, best practices, controls	[15–17, 19, 20, 22, 23]
Continuous improvement	Continuous improvement, risk assessment, security measurement, auditing, security analysis and protection	[17,18,20,23,24]

We call the other group of variables "Technology, infrastructure and resources", which are essential to operate and implement any management or project in the organization, such as human, technological, material resources, among others, as well as the physical infrastructure, networks, etc.

We call the third group of variables in the "Organization / Management" factor, which are the different organizational structures that obey the strategic need, which allows managing and controlling, considering the "Technology, infrastructure and resources" factor; includes processes and procedures, considering international standards and best practices, such as ISO/27001, ITIL, COSO, etc.

We call the fourth group of variables the "Continuous Improvement" factor; which is the implementation of a permanent management system, which ensures the control and monitoring of the operation of the controls and procedures carried out, as well as the constant improvement of what is working incorrectly to achieve the protection desired by the organization.

2.1.2. External factors

Public organizations are not isolated entities, they carry out their operations within a context that will affect their security[27]. The laws, state policies and other actions to curb cybercrime in each community, city or country, together with international cooperation, can positively or negatively affect the cybersecurity of an organization[15]. There is evidence that links the development of a good cybersecurity strategy in a country and the effective use of public resources can improve the cybersecurity of organizations[28]. We have called these external factors that affect the cybersecurity of public organizations: local, national and international context.

An effective cyber security approach must involve all levels of government, according to the political division of each country; Cyberspace is constantly evolving, as are attacks, threats and risks, which is why governments need to build resilient cybersecurity at all levels, so as not to be an easy target[29].

Cybersecurity Capacity Maturity Model for Nations (CMM), developed by the Global Cybersecurity Capacity Center (GCSCC), at the University of Oxford, uses 5 dimensions: "Cybersecurity Policy and Strategy", "Cyber Culture and Society", "Education, Training and Skills in Cybersecurity", "Legal and Regulatory Frameworks" and "Standards, Organizations and Technologies". According to the 2020 Cybersecurity report of the Organization of American States, for the countries of Latin America and the Caribbean, the average maturity level is low, between 1 and 2, out of 5 levels of the CMM[30].

The Global Cybersecurity Index (GCI), is an initiative of the International Telecommunication Union (ITU) of the United Nations (UN), is based on 5 pillars: "legal measures", "technical measures", "organizational measures ", "capacity development measures" and "cooperation measure"[31]. If we review the GCI ranking, the first 10 positions are: first place United States 100; second place United Kingdom and Saudi Arabia 99.54; third place Estonia 99.48; fourth place Korea, Singapore and Spain 98.52; fifth league Russia, Arab Emirates and Malaysia 98.06; sixth place Lithuania 97.93; seventh place Japan 97.82; eighth place Canada 97.67; ninth place France 97.6; 10th place India 97.5. Europe is the continent with the best positioned countries, we have 6 in the top 10.

The National Cyber Security Index (NCSI) measures the Cybersecurity of countries considering 12 indicators: "Development of cybersecurity policies", "Analysis and information on cyber threats, Education and professional development", "Contribution to global cybersecurity", Protection of digital services", "Protection of essential services", "Electronic identification and trust services", "Protection of personal data", "Response to cyber incidents", "Cyber crisis management", "Fight against cybercrime" and "Military cyber operations"[32]. In the NCSI ranking, the first 10 countries belong to Europe, led by Greece 96.10, Lithuania 93.51, Belgium 93.51, Estonia 93.51, Czech Republic 92.21, Germany 90.91, Romania 89.61, Portugal 89.61, Spain 88.31 and Poland 87.01, which shows the progress of the European Union on cybersecurity issues.

2.2. Methods

2.2.1. First phase

A search was made for the information available on official websites and scientific databases on factors and variables that public organizations have used to analyze cybersecurity. The most common security problems suffered by organizations and their limitations to face cyber attacks were reviewed. Then the factors were analyzed and categorized into two groups, external and internal, related to the cybersecurity of public organizations.

2.2.2 Second phase

A conceptual model was designed to allow the evaluation of cybersecurity management capacity (CMC), based on the main internal and external factors found in the first phase, with a strategic approach, considering that it is one of the main deficiencies in organizations.

In order to quantify the cybersecurity management capacity of an organization, a calculation process was defined and measurement scales were created for the 5 fundamental factors of the conceptual model designed, based on variables that we can value found in the scientific literature and the practice of public

organizations. The calculation of CMC of an organization will be determined by the average of the evaluation of internal and external factors, both have the same weight.

For the factor criteria assessment scale, a standard scale between 0-10 is considered to obtain more precise results[33].

2.2.3. Third phase

To validate the Cybersecurity Management Capacity model, organizations in two different cybersecurity contexts or levels were assessed, the first context in a country developed in cybersecurity, belonging to the European Union and Spain, because it is within the top 10 both in the GCI index and in the NCSI. For the second context to compare, we have a country that still does not achieve good levels of cybersecurity, belonging to Latin America, such as Ecuador. For each context, three typical public organizations are simulated, with high, medium and low levels of cybersecurity management capacity.

To assess the external factor of the local, national and international context, the GCI 2020 ranking is taken into account, with 194 participating countries, where Spain is in position 4 with 98.52% and Ecuador is in position 119 with 26.30%[31]. To assess the level of corruption criterion, we use the Corruption Perception Index (CPI) 2021, with 180 participating countries, where Spain is ranked 34 with 61 points and Ecuador is ranked 105 with 35 points[34].

3. Results

The following results were obtained:

3.1. Cybersecurity management capacity model

Figure 1 shows the cybersecurity management capacity model (CMC), which groups 5 important factors found in the literature, 4 internal factors related to the capacities of the public organization and 1 external factor, related to the environment or context in which that the organization develops, which depending on the country can be more or less levels, depending on the respective political organization. This model proposes through the first "Strategic" factor, a perspective of IT strategic planning, which contemplates cybersecurity, to direct the organization to the achievement of its proposed objectives; For this, it must be based on the factors "Technology, infrastructure and resources", "Organization and Management", "Continuous Improvement" and "Local, National and International Context".

The mathematical model to calculate the % CMC will be given as follows:

$$F_i = \frac{\sum_{j=1}^{n} c_j}{n} \quad (1)$$

$$\%CMC = 1.25F_1 + 1.25F_2 + 1.25F_3 + 1.25F_4 + 5F_5 \quad (2)$$

where:

% CMC, is the measurement of the Cybersecurity Management Capacity of the public organization. With this % an organization can be categorized using Table 4.

F, is the assessment of each factor from i=1 to 5, according to Table 2. Each factor F is calculated by means of the average of the assessment of its criteria.

c, is the evaluation of the criteria with a score from 0 to 10, according to Table 3. For each factor F there can be criteria from j=1 to n.

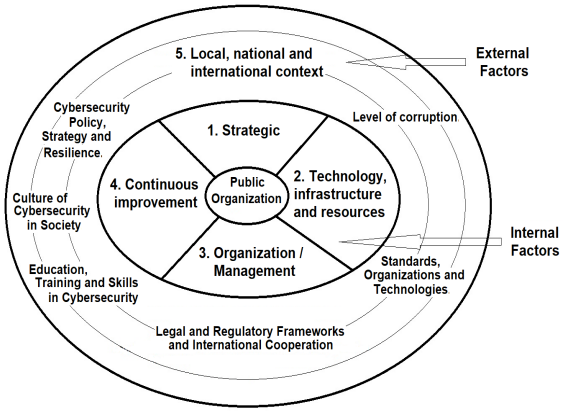

Figure 1: Cybersecurity Management Capacity Model

3.2. Process to quantify the CMC

In order to apply the CMC conceptual model and quantify the measurement, for each factor we established criteria to be evaluated for a public organization. Table 2 shows these factors with their respective criteria, which have been improved accordingly [1], For the internal factors, practical criteria used in public organizations were considered, for the external factor we considered the 5 dimensions of the CMM model and a criterion of corruption levels was added[25]. We also defined the assessment scale for each factor criterion, which can be seen in Table 3; This scale starts from 0 to 3, which meets little or nothing, until reaching 9 to 10, where it meets all of that criterion, which is the maximum score that a one-factor criterion can have.

Table 2: Evaluation factors and considerations

Factor	Evaluation criteria
1. Strategic	1. Strategic IT planning. 2. 2. Support from senior management. 3. 3. Organizational culture of Safety. 4. 4. Projects and action plans at the strategic, tactical and operational levels.
2. Technology, infrastructure and resources	1. Appropriate systems and technology. 2. Adequate IT infrastructure. 3. Sufficient human, financial, material and technological resources.
3. Organization / Management	1. Efficient and flexible organizational structure. 2. Control and management of all critical IT processes and assets. 3. International norms and standards, best IT Practices. 4. Control and management of IT strategic planning projects.
4. Continuous improvement	1. Incident and nonconformity management system.

	2. Control and monitoring of incidents and nonconformities. 3. Strategic planning considers reported incidents and nonconformities.
5. Local, national and international context	1. Cybersecurity Policy, Strategy and Resilience. 2. Culture of Cybersecurity in Society. 3. Education, Training and Skills in Cybersecurity. 4. Legal and Regulatory Frameworks and International Cooperation. 5. Standards, Organizations and Technologies. 6. Level of corruption.

Once all the criteria have been assessed, the average of each factor is calculated, to then determine the final weighted average of the 5 factors. In Table 4 we can see the 5 levels of the CMC model that a public organization can be categorized; starting from the "Initial", "Formative", "Administered", "Strategic" level, and ends with the highest level "Optimized", which should be the cybersecurity objective that a public organization must achieve.

Table 3: Factor Criteria Rating Scale

Scale	Value	Valuation Criterion
Very high	(9 – 10]	Meets all
High	(7 – 9]	Meets most
Medium	(5 – 7]	Partially complies
Low	(3 – 5]	Fulfills something
Very low	[0 – 3]	Little or no compliance

Table 4: CMC rating scale (In Organizations)

Scale	Value range	Assessment
optimized	(80 - 100]	Prepared
strategic	(60 - 80]	Consenting
managed	(40 - 60]	Vulnerable
formative	(20 - 40]	Danger
Initial	[0 - 20]	Helpless

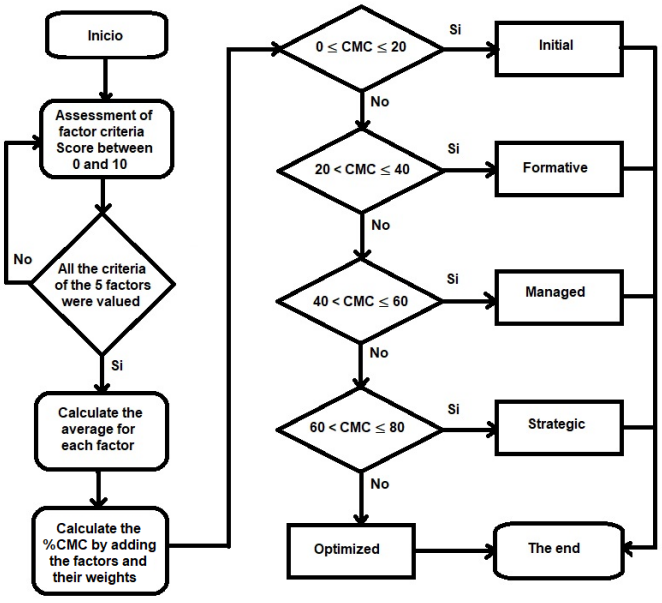

Figure 2: Process to calculate the Cybersecurity Management Capacity

Table 4 shows the CMC assessment scale, which categorizes an organization into 5 levels of capacity, similar to the CMM model; each level corresponds to 20% and goes from the Initial level that has a low assessment of the 5 factors, therefore, it is a defenseless organization, prone to attacks. The last level, on the other hand, speaks of an organization with a high rating in the 5 factors, which is prepared to prevent and combat any cyber-attack. Figure 2 shows the process for calculating the CMC; It consists of 4 stages: the assessment of the criteria for each factor considering Table 2 and 3, calculation of the average of the criteria assessments for each factor, calculation of the final average based on each factor and categorization of the organization according to the CMC of according to Table 4.

3.3. Validation of the CMC model

The validation of the CMC model of 2 different contexts Spain and Ecuador was carried out:

3.3.1 Simulation of public organizations in Spain

Table 5 shows the final averages of each of the 5 factors for the simulation of 3 public organizations with High, Medium and Low levels of internal factors of the CMC model for the context of Spain. In Fig. 3 the results of the 3 organizations in Spain, where the red color represents the lack of CMC.

3.3.2. Simulation of public organizations in Ecuador

Table 6 shows the final averages of each of the 5 factors for the simulation of 3 public organizations with High, Medium and Low levels of internal factors of the CMC model for the Ecuadorian context. In Fig. 4 the results of the 3 organizations from Ecuador, where the red color represents the lack of CMC.

Table 5: Spain context simulation

Factor	High	Medium	Low
1. Strategic	8.90	6.55	2.25
2. Technology, infrastructure and resources	9.50	5.68	3.14
3. Organization / Management	9.20	6.79	2.88
4. Continuous improvement	8.80	6.23	2.67
5. Local, national and international context	9.23	9.23	9.23
Final percentage	91.63%	77.69%	59.80%
Category	Optimized	Strategic	Managed

Table 6: Ecuador context simulation

Factor	High	Medium	Low
1. Strategic	8.90	6.55	2.25
2. Technology, infrastructure and resources	9.50	5.68	3.14
3. Organization / Management	9.20	6.79	2.88
4. Continuous improvement	8.80	6.23	2.67
5. Local, national and international context	2.78	2.78	2.78
Final percentage	59.38%	45.44%	27.55%
Category	Managed	Managed	Formative

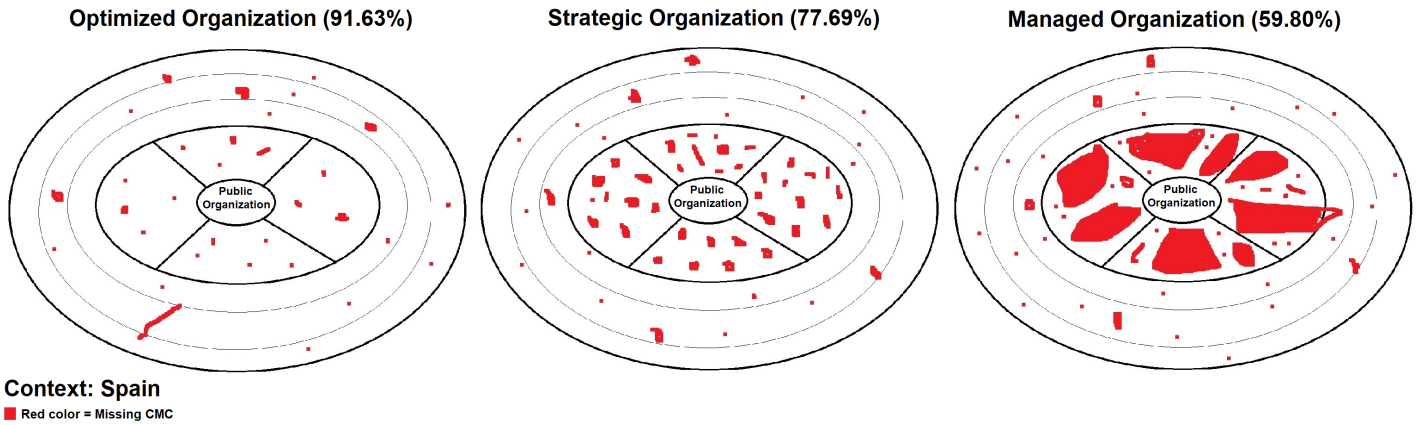

Figure 3: Simulation of public organizations in the context of Spain

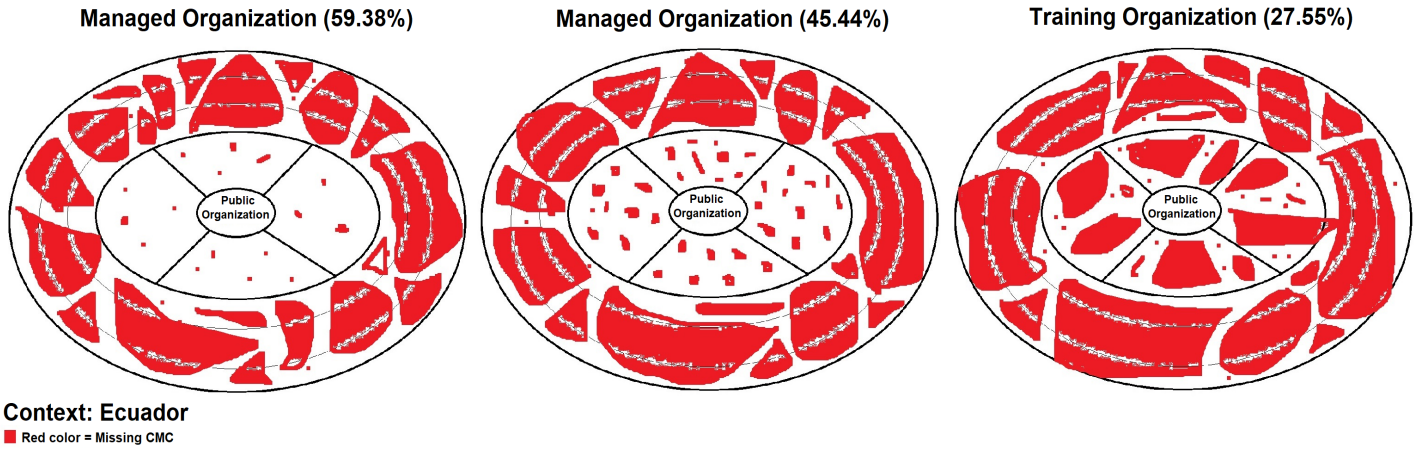

Figure 4: Simulation of public organizations in the Ecuadorian context

Fig. 3 shows the result of the simulation of the 3 organizations in the context of Spain, according to Table 5, the first with a valuation of high internal factors (Optimized), the second with medium factors (Strategic) and the third with factors low (Managed). For each organization, the graph resembles an onion because it has several layers, in the heart or center is the public organization, which is protected by the layer of internal factors of the CMC model, then there are several layers that belong to external factors, defined as a local, national and international context, the number of layers will depend on the political division of each country where the organization is located. We can see that the external factor of Spain greatly supports organizations in their cybersecurity management capacity, the parts marked in red represent the lack of capacity for each factor, which for the context of Spain are few.

Fig. 4 shows the result of the simulation of the 3 organizations in the context of Ecuador, according to Table 6, the first with a valuation of high internal factors (Administered), the second with medium factors (Administered) and the third with factors low (Formative). We can see that the external factor of Ecuador does little to support organizations in their cybersecurity management capacity, the parts marked in red represent the lack of capacity for each factor and for this context in Ecuador there are many.

6. Discussion

A conceptual model is presented to determine the Cybersecurity Management Capacities in public organizations based on the most important factors found in the literature, both internal and external, where both groups of factors have the same weight. The 4 internal factors, "Strategic", "Technology, infrastructure and resources", "Organization / Management" and "Continuous improvement", form the first cybersecurity protective shield for the organization. The external factor "Local, national and international context" forms the following cybersecurity protective shield, which must work closely related to the internal factors of the organization, to achieve an "Optimized" category, which defines that the organization is prepared to face the possible computer attacks.

We can see in Figures 3 and 4 the simulation of organizations in 2 different contexts, such as Spain with excellent cybersecurity capabilities and Ecuador with limited cybersecurity capabilities. The results of the model show that, despite having similar internal factors in both contexts, the external factor makes the CMC superior for organizations in Spain, categorized as "Optimized" and "Strategic", while for Ecuador the CMC shows organizations

with problems in cybersecurity capacity, which can only be categorized as "Managed" and "Formative". This implies that in order to achieve optimal cybersecurity management capabilities, organizations have to strengthen not only internal factors, but also the external factor, which is the context in which the organization operates. The CMC model can be an important tool to know the current state of cybersecurity management capacity of organizations and to carry out periodic analyzes of the progress made to improve cybersecurity.

The proposed CMC model was developed from the perspective of assessing capabilities, based on the information that we know with certainty and have available, both internally and externally, from the context where the organization operates, which are actions of the different levels of government of a country and the international community. A large number of works reviewed in the literature maintain the perspective of evaluating cyber risk, based on unknown information, using probabilities of possible incidents and their effects; historical data is generally not available and subjective methods end up being used, such as expert judgment[35].

The results of the simulation of the CMC model for the public organizations showed notable differences for the compared contexts; In an advanced cybersecurity context like that of Spain, the vast majority of organizations will have a %CMC greater than 60%, which means that they may have a better chance of anticipating and resisting cyber-attacks. On the other hand, in the context of Ecuador, the vast majority of organizations will have a %CMC lower than 60%, which means that they are vulnerable, have many limitations of all their factors and are less likely to foresee and resist cyber-attacks. It is important to clarify that having a 100% CMC does not mean that the organization is safe from receiving cyber-attacks, it means that it has its cyber management capabilities developed to the maximum, in such a way that it can prevent or receive a minor impact, in such a way that business continuity is not threatened.

The ObservaCiber 2021 report shows results of important advances in cybersecurity of organizations in Spain, which supports the results of this work, with high %CMC found in organizations for the context of Spain[36]. Research carried out in Ecuador showed low levels of cybersecurity in public organizations[22]. International research also shows similar results, showing organizations with many cybersecurity problems, suggesting actions with government support and international collaboration to improve the low levels of cybersecurity shown[15].

7. Future work and conclusions

7.1. Future work

As future work, a validation of the model should be carried out in organizations of different contexts worldwide, in this way the CMC model can be perfected, validating the factors and criteria exhaustively, to ratify or modify them.

7.2. Conclusions

The Cybersecurity Management Capacities model allows to evaluate the current situation of the organization, to go gradually according to its resources and needs, to improve the CMC until reaching an "Optimized" level, so that the organization has capacities that allow to foresee and protect your critical assets and sensitive information.

This CMC model highlights the need for public organizations to have the support of the governments of the different political divisions of a country, as well as permanent international collaboration in the field of cybersecurity. This is evidenced by the simulation carried out, where organizations from developed countries such as Spain have better capacities (greater than 60% CMC) than less developed countries such as Ecuador (less than 60% CMC), due to the cybersecurity context where these organizations operate.

Having a high % of CMC means that the organization has developed the necessary capabilities to be proactive and reactive in the face of possible attacks and cybersecurity problems, ensuring the continuity of the organization's operations and the reliability, integrity and availability of information. The CMC is a double protective shield, one internal and one external, but that does not imply that having a 100% CMC does not receive attacks and cyber threats, because that does not depend on the CMC.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors thank the Doctorado en Estadística y Matemática Aplicada de la Universidad Nacional de Tumbes, Universidad Católica de Santiago de Guayaquil (UCSG), Instituto Tecnológico Superior Rumiñahui (ISTER), Escuela Politécnica Nacional (EPN), CUCEA Universidad de Guadalajra de México (UDG) and Secretaría de Educación. Superior, Ciencia, Tecnología e Innovación" (Senescyt).

References

[1] R. Romero I., L.J. Caucha M., S.M. Toapanta T., L.E. Mafla G., J.A. Orizaga T., "Analysis of the Information Security of Public Organizations in Ecuador," in The 2021 International Conference on Computational Science and Computational Intelligence, IEEE: 823–829, 2021, doi:10.1109/CSCI54926.2021.00195.

[2] Check-Point-Research, Check Point Software's 2022 Security Report: Global Cyber Pandemic's Magnitude Revealed, 2022.

[3] World Economic Forum, Global Cybersecurity Outlook 2022, Cologny/Geneva.

[4] U.L.C.S. Andrew Morrison, Principal, Cyber Security Landscape 2022.

[5] Check-Point-Research, CYBER SECURITY REPORT, 2021.

[6] G.M. Jonathan, K.S. Hailemariam, B.K. Gebremeskel, S.D. Yalew, "Public Sector Digital Transformation: Challenges for Information Technology Leaders," in 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 1027–1033, 2021, doi:10.1109/IEMCON53756.2021.9623161.

[7] W.A. Conklin, D. Shoemaker, "Cyber-resilience: Seven steps for institutional survival," EDPACS, **55**(2), 14 – 22, 2017, doi:10.1080/07366981.2017.1289026.

[8] M. Nassar, J. Khoury, A. Erradi, E. Bou-Harb, "Game Theoretical Model for Cybersecurity Risk Assessment of Industrial Control Systems," in 2021 11th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2021, 2021, doi:10.1109/NTMS49979.2021.9432668.

[9] M. Ron, W. Fuertes, M. Bonilla, T. Toulkeridis, J. Diaz, "Cybercrime in Ecuador, an exploration, which allows to define national cybersecurity policies," in 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), 1–7, 2018, doi:10.23919/CISTI.2018.8399357.

[10] MINTEL, Libro Blanco de Territotios Digitales en Ecuador, Ministerio de

Telecomunicaciones y de la Sociedad de la Información, Quito, 2019.
[11] A. Urbanovics, "Cybersecurity Policy-Related Developments in Latin America," Academic and Applied Research in Military and Public Management Science, **21**(1), 79–94, 2022.
[12] S. Creese, W.H. Dutton, P. Esteve-González, "The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions," Personal and Ubiquitous Computing, **25**(5), 941–955, 2021, doi:10.1007/s00779-021-01569-6.
[13] S. Creese, W.H. Dutton, P. Esteve-Gonzalez, M. Goldsmith, E. Nagyfejeo, J. Saunders, B. von Solms, C. Weisser Harris, "The Solution is in the Details: Building Cybersecurity Capacity in Europe," Available at SSRN 4178109, 2022.
[14] B. Uchendu, J.R.C. Nurse, M. Bada, S. Furnell, "Developing a cyber security culture: Current practices and future needs," Computers and Security, **109**, 2021, doi:10.1016/j.cose.2021.102387.
[15] E.K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, B. Klepacki, "Information security assessment in public administration," Computers & Security, **90**, 101709, 2020, doi:10.1016/j.cose.2019.101709.
[16] A. Nasir, R.A. Arshah, M.R. Ab Hamid, S. Fahmy, M.A. Bakar, "Information security culture model for malaysian organizations: A review," International Journal, **9**(1.3), 117–121, 2020, doi:10.30534/ijatcse/2020/1691.32020.
[17] F.Ö. Sönmez, "A conceptual model for a metric based framework for the monitoring of information security tasks' efficiency," in Procedia Computer Science, 181–188, 2019, doi:10.1016/j.procs.2019.09.459.
[18] R. Hoffmann, J. Napiórkowski, T. Protasowicki, J. Stanik, "Measurement models of information security based on the principles and practices for risk-based approach," Procedia Manufacturing, **44**, 647–654, 2020, doi:10.1016/j.promfg.2020.02.244.
[19] R. Diesch, M. Pfaff, H. Krcmar, "A comprehensive model of information security factors for decision-makers," Computers & Security, **92**, 101747, 2020, doi:10.1016/j.cose.2020.101747.
[20] O.M.M. Al-Matari, I.M.A. Helal, S.A. Mazen, S. Elhennawy, "Adopting security maturity model to the organizations' capability model," Egyptian Informatics Journal, **22**(2), 193–199, 2021, doi:10.1016/j.eij.2020.08.001.
[21] K. Arbanas, N. Žajdela Hrustek, "Key success factors of information systems security," Journal of Information and Organizational Sciences, **43**(2), 131–144, 2019, doi:10.31341/jios.43.2.1.
[22] S.M. Toapanta, A. Jimenez, L.E. Mafla, "An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of Ecuador," in Proceedings of the 2019 2nd International Conference on Education Technology Management, 61–66, 2019, doi:10.1145/3375900.3375909.
[23] M. Toapanta, E. Mafla, J. Orizaga, "Conceptual model for identity management to mitigate the database security of the registry civil of Ecuador," Materials Today: Proceedings, **5**(1, Part 1), 636–641, 2018, doi:https://doi.org/10.1016/j.matpr.2017.11.127.
[24] B. Kruck, P. Munk, D. Angermeier, "Safe and Secure: Mutually Supporting Safety and Security Analyses with Model-Based Suggestions," in Proceedings - 2021 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2021, 172 – 181, 2021, doi:10.1109/ISSREW53611.2021.00061.
[25] X.M. Nguyen, Q.T. Tran, "Corruption and corporate investment efficiency around the world," European Journal of Management and Business Economics, **31**(4), 425 – 438, 2022, doi:10.1108/EJMBE-11-2020-0321.
[26] H. Serna Gómez, others, Gerencia estratégica. Planeación y gestión, teoría y metodología, 3R Editores, 2008.
[27] L. Masilela, D. Nel, "The role of data and information security governance in protecting public sector data and information assets in national government in South Africa," Africa's Public Service Delivery and Performance Review, **9**, 10, 2021, doi:https://doi.org/10.4102/apsdpr.v9i1.385.
[28] Z. Li, X. Guo, Q. He, "A Study of Chinese Policy Attention on Cybersecurity," IEEE Transactions on Engineering Management, 2020, doi:10.1109/TEM.2020.3029019.
[29] M. Masombuka, M. Grobler, P. Duvenage, "Cybersecurity and local Government: Imperative, Challenges and Priorities," in ECCWS 2021 20th European Conference on Cyber Warfare and Security, 285, 2021.
[30] BID - OEA, Ciberseguridad riesgos, avances y el camino a seguir en América Latina y El Caribe, 2020.
[31] G.C. Index, "URL: https://www. itu. int/myitu/-/media/Publications/2021-Publications," Global-Cybersecurity-Index-2020. Pdf [in English], 2020.
[32] e-Governance Academy Foundation, National Cyber Security Index NCSI, CSIRT, 2020.
[33] K.S. Crandall, "Risk Assessments: A Weighted Score Approach to Improving Risk Management Decisions," in 2020 Intermountain Engineering, Technology and Computing, IETC 2020, 2020, doi:10.1109/IETC47856.2020.9249164.
[34] Transparency international, Corruption Perceptions Index CPI, 2021.
[35] M. Battaglioni, G. Rafaiani, F. Chiaraluce, M. Baldi, "MAGIC: A Method for Assessing Cyber Incidents Occurrence," IEEE Access, **10**, 73458 – 73473, 2022, doi:10.1109/ACCESS.2022.3189777.
[36] ObservaCiber, Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea, 2021.