Evaluating the impact of risk management and cybersecurity on decision-making in the Peruvian National Informatics System

Frank Agustín Olivos Estrada[1], Willian Sebastian Flores-Sotelo[2], Carmen Rosa Barrera-Avalos[3], Williams Arturo Martínez-Aberga[4], Richard Sulca-Guillen[5], Jorge Miguel Chávez- Díaz[2]
[1]Graduate School, Universidad César Vallejo, Lima, Perú
[2]Graduate School, Universidad Nacional Federico Villarreal, Lima, Perú
[3]School of Accounting, Universidad Nacional Federico Villarreal, Lima, Perú
[4]School of Accounting, Universidad Privada del Norte-UPN, Lima, Perú
[5]School of Accounting, Universidad Nacional de San Cristóbal de Huamanga, Ayacucho, Perú

Article Info

Article history:

Received Dec 24, 2024
Revised Aug 20, 2025
Accepted Sep 1, 2025

Keywords:

Information systems
Information technology
Information technology security
Policy keyword
Public administration

ABSTRACT

This research addresses the influence of risk management (RM) and cybersecurity (CIB) on decision making (DM) of the Peruvian State's National Informatics System (SNIEP) in the year 2024, in line with sustainable development goal 9. Using a quantitative, non-experimental, cross-sectional design approach, a sample of 487 CIB analysts was analyzed to explore the relationship between these critical variables. The findings show uneven implementation of RM and CIB practices, which significantly impact the DM and quality of information (Sig 0.000), processes (Sig 0.001), and the effectiveness of system decisions (Sig 0.060). In addition, key areas were identified to strengthen the integration of RM and CIB strategies in the state's digital environment, highlighting their importance to ensure informed and resilient decisions in the face of growing cyber threats. The study provides empirical evidence on their impact on the quality, effectiveness and security of DM in government digital environments. The research contributes both to the development of a theoretical framework that articulates concepts of RM, CIB, and DM in the public sector, and to the formulation of strategies and policies that promote a secure and efficient digital infrastructure, aimed at improving public services and citizen trust in the contemporary digital environment.

Corresponding Author:

Jorge Miguel Chávez-Díaz
Graduate School, Universidad Nacional Federico Villarreal
Jr. Prolongación Camaná N°1014 Lima, Perú
Email: jchavezdi@unfv.edu.pe

1. INTRODUCTION

Problem situation: globally, cybersecurity (CIB) represents a significant threat to both the public and commercial sectors. According to the World Economic Forum's Global Risks 2021 report, 39% of experts surveyed consider cyberattacks to be a significant threat to the global [1]. The global issue of risk management (RM) affects all types of companies, including private and publicly traded companies. The World Economic Forum's Global Risks Report 2021 indicates that 35.7% of respondents consider extreme events to be the most likely risk to the world [1]. In addition, decisions have a significant impact on the global performance of companies. According to a study by McKinsey and Compañy [2], only 20% of the decisions made by companies create significant value.

In the regional context, Latin American and Caribbean countries obtained an average score of 25.32 out of 100 in the IDB CIB index in 2020, an increase of 25% over 2016 [3]. In addition, 54% of organizations in Latin America experienced a CIB incident in 2020, an increase of 12% over the previous year [3]. On the other hand, many Latin American companies are not prepared for emergencies because they lack a RM strategy [4]. When asked about the challenges they face in making good decisions, a large percentage of Latin American managers cited a lack of data and analysis [5].

Among the 194 nations evaluated for their CIB, Peru ranks 81st (54.25 out of 100) in the Global CIB Index 2020 [6]. This position shows that the main target of cyber-attacks is the essential services of the Public Administration by targeting networks, data and infrastructures, creating denial of service conditions that threaten the continuity and reliability of its activities [7]. In addition, Ruidias *et al.* [8] reports that 22% of all public companies have a RM strategy.

The lack of sufficient CIB safeguards in public institutions in Metropolitan Lima (Perú) is a cause for concern, as it threatens the privacy, authenticity and accessibility of the State's most important data. The situation of public organizations in Metropolitan Lima is of much greater concern, as their credibility and access to essential public services and healthcare are threatened by insufficient RM strategies. Many Peruvian government institutions report a lack of adequate data systems to back up their decisions [8]. Public service delivery in Metropolitan Lima is plagued by ineffective decision-making procedures, faulty communication and unprofessional data analysis.

Strengthening Peruvian State's National Informatics System’s (SNIEP's) capacity against cyber threats improves information security and decision making (DM), making digital public services more efficient. This research is key in the face of increasing cyber-attacks and allows designing policies and plans that protect sensitive data, promote jobs in digital security and boost innovation. It also contributes to modernize the technological infrastructure of the Peruvian State, promoting a more secure, efficient and aligned governance with sustainable development.

El estudio es muy importante para el contexto peruano y por supuesto latinoamericano, ya que diferentes sectores económicos enfrentan limitaciones para obtener financiamiento como consecuencia de la incertidumbre macroeconómica y el nivel de riesgo país [9]. Esta situación que repercute en la composición y solidez de la estructura financiera de las empresas de todo tamaño [10], [11].

The following problems are considered: how do RM and CIB influence DM in the SNIEP in the year 2024? This is broken down into three specific problems: how do RM and CIB influence the quality of information, the decision-making process and the effectiveness of decisions of the Peruvian National Informatics System in 2024?

The study contributes to knowledge about the intersection between information security and public governance. Theoretically, it integrates concepts of RM, CIB, and decision theory, expanding the understanding of these fields in the context of the public sector. Research on RM and CIB in DM SNIEP is very important considering the increasing number of cyber-attacks and the pressing need to safeguard sensitive government assets. National security and the efficiency of governance in the digital age are two important issues that this research aims to address.

The practical implications of this research are significant, as the findings can directly improve data protection strategies and DM in the state computer system. The study can help strengthen the ability of the state computer system to withstand and recover from cyber-attacks by investigating how these variables influence DM. In addition, the findings may contribute to the development of more effective policies and strategies for the protection of sensitive data and the continuity of digital public services.

From a social point of view, the research seeks to reinforce public trust in the Administration's digital services and to protect citizens' sensitive information. The research strategy is based on a rigorous quantitative analysis, which could serve as a model for future studies of this type. From a legal standpoint, the study complies with Peruvian data protection and information security regulations, which may influence future laws on government CIB.

The general objective of this research is to evaluate the influence of RM and CIB on SNIEP DM in the year 2024; this objective is broken down into three specific objectives: first, to determine the influence of RM and CIB on the quality of information, DM process and effectiveness of SNIEP decisions in the year 2024.

Literature review: CIB in the public sector is an essential and complex area that encompasses the protection of sensitive government data, the preservation of digital infrastructure and the strengthening of citizen confidence in digital services [12]. Its relevance lies in the fact that it constitutes a pillar for national and public security by preventing cyber threats with potential financial, political and military repercussions [13]. In addition, a robust CIB strategy is indispensable for the development of e-government, as the perception of risk can hinder the adoption of these services [14].

CIB is a fundamental field focused on protecting computers, networks and data from unauthorized access, cyberattacks and other malicious activities. It encompasses a range of measures and strategies to safeguard digital assets and sensitive information [15], [16]. CIB is essential due to the increasing dependence on digital systems and the internet, which exposes organizations to various cyber threats such as ran-somware, phishing, and insider threats [17]. The field is continually evolving to address new vulnerabilities and attack vectors, making it a dynamic and complex area of study [18], [19].

RM in the public sector is a multifaceted process that involves identification, assessment and mitigation of risks to ensure effective delivery service and safeguard public resources [20]. This involves budget planning and resource allocation [21], regulatory frameworks [22], and policies that even integrate RM into corporate governance [23]. Strategic and structural support based on a solid organizational culture is also key [24].

The importance of efficient RM encompasses ensuring the protection of business processes, assets and revenues, thus supporting the overall mission of the company [25]. It also improves safety by preventing incidents that could cause harm to employees, customers and the environment [26], [27]. It provides a structured approach to DM under uncertainty, improving the quality and reliability of business decisions [28].

The theory provided by ISO 31000 provides three dimensions: the strategic dimension, which involves ensuring that risks are an integral part of strategy formulation and review processes, as well as long-term programming. The operational dimension, which implies that risks are incorporated into daily processes, projects and activities to manage and mitigate them effectively at the tactical and execution level. The compliance dimension, which requires managing risks to meet regulatory and contractual obligations, as well as to preserve the interests of shareholders and stakeholders [29].

H1. RM and CIB influence SNIEP DM by 2024.

DM: combining RM and CIB efforts ensures that both known and emerging risks are addressed, which is essential for maintaining high information quality [30], [31]. User participation in the identification of information security risks can lead to better RM practices and improved information quality [32]. High-quality information is critical to making informed business decisions. Effective RM and CIB practices ensure that the information used in DM is reliable and accurate [33]. Poor information quality due to inadequate RM or CIB measures can lead to major business disruptions and strategic failures [34].

H2: RM and CIB have an impact on the quality of SNIEP information, 2024.

The integration of RM and CIB significantly influences the decision-making process within organizations. It ensures that risk issues are integrated into the strategic decision-making process and aligned with the organization's performance objectives [35]. In addition, effective RM involves the use of both qualitative and quantitative methods. Qualitative methods provide a sense of risk, while quantitative methods, such as cyber risk quantification (CRQ), provide precision by numerically estimating potential threats and their impacts, which facilitates more informed DM [36], [37].

H3: RM and CIB have an impact on the SNIEP DM process, 2024.

RM and CIB play a key role in improving the effectiveness of DM in organizations. By identifying, assessing and mitigating risks, organizations can make more informed and strategic decisions, thereby improving overall performance and resilience. RM and CIB are critical to effective DM in organizations. By adopting comprehensive RM frameworks, aligning CIB with strategic objectives, and leveraging the right tools and methods, organizations can improve their decision-making capabilities, reduce risk, and improve overall performance [38]-[41].

H4: RM and CIB influence the effectiveness of SNIEP decisions, 2024.

This study acknowledges the possible omission of variables that could influence the results, such as leadership style, organizational culture, political interference, and budgetary constraints. These factors, although not addressed in the current model, could provide a more comprehensive understanding of the phenomenon analyzed. Their inclusion in future research is suggested to strengthen the validity and scope of the proposed models.

2. METHOD

The quantitative approach was used, coupled with a hypothetical deductive (theoretical) approach that yielded results that validated the RM and its effects on public awareness, based on the theory [42]. Because of its usefulness in addressing local, regional or national social issues through the development of hypotheses and the formulation of problems, the applied type was chosen. The design focused on the process of developing a plan to address the research topic. Since no tests were performed and all data were collected at the same time, the design can be described as non-experimental and cross-sectional [42]. A multivariate causal explanatory correlational study was carried out, since it not only examines the association between variables, but also seeks to establish causal relationships between multiple variables [42].

In summary, the study used basic research to generate new knowledge. This approach allows the exploration of underlying concepts and phenomena without a defined practical application by carefully examining them [43]. By using this method, the research was able to deepen the analysis by exploring fundamental and permanent principles, which made it possible to create a solid analytical framework and identify gaps in knowledge. In addition, it guided research questions and innovative approaches in the doctoral thesis on DM in the SNIEP, by focusing on the disinterested detailed study of these concepts and phenomena without a pre-established practical objective. In this way, the study was able to contribute new knowledge through a careful disinterested analysis of the underlying fundamentals.

Variables are defined as variable 1: RM, according to [29], is an iterative and coordinated process that guides and governs an organization, seeking to increase the probability of positive events and decrease the frequency of negative events, integrating with operations, strategies, objectives, and organizational governance to facilitate prioritization of tasks, informed DM, strengthening of controls and achievement of objectives, ensuring timely involvement of stakeholders and continuous improvement through education and work; this process is composed of three main dimensions: risk identification, risk analysis and assessment, and risk treatment.

As variable 2: CIB, according to Solms and Niekerk [44] involves safeguarding cyberspace, electronic information and the information and communication technologies that make it possible, as well as users in their individual, social and national capacities, and their tangible and intangible assets susceptible to cyber-attacks. The culture of the CIB, technical security controls and security policies and procedures were dimensions considered.

As variable 3: DM is a rational process of identifying and selecting alternatives to achieve a specific objective, incorporating multi-criteria decision theory to handle multiple objectives and options with both quantifiable and non-quantifiable attributes. As part of this procedure, possible complete, mutually exclusive substitutes are sought, the definition of criteria reflecting objectives and effects, the evaluation of preferences, weightings and trade-offs, and the optimization of positive objectives while minimizing negative ones. In this sense, we worked with the following dimensions: quality of information, DM process and effectiveness of decisions [45]. Figure 1 shows graphically the objective of the study, based on two variables: RM and CIB applied to the National Information System of the Peruvian State and its dimensions.

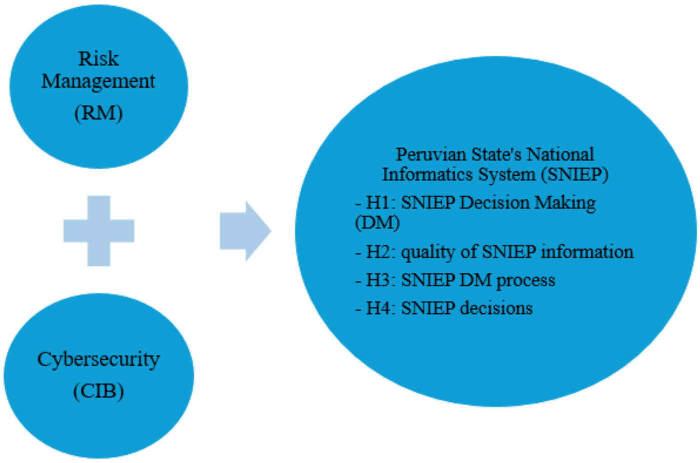
Risk Management (RM)
Cybersecurity (CIB)
Peruvian State's National Informatics System (SNIEP)
- H1: SNIEP Decision Making (DM)
- H2: quality of SNIEP information
- H3: SNIEP DM process
- H4: SNIEP decisions

Figure 1. Study variables

The population is made up of all instances with unique characteristics; a sample is selected from this population, and among them, 156,062 professionals, both men and women, who worked in the ICT domain in Peru. This group included 20,320 CIB analysts who were part of the SNIEP. The inclusion criterion included these professionals, while the exclusion criterion considered children under 5 years of age and technical personnel and users. The probabilistic sample was 487 individuals randomly selected from the total population. These were selected using a stratified procedure, ensuring proportional representation of subgroups such as ministries and regions. This subgroup made it possible to acquire knowledge and establish relationships through scientific analysis, the objective of which was to develop theoretical models on the subject under study.

The population units were chosen randomly and in proportion to their size, so these samples are known as probability samples. The results can be confidently extrapolated to the population if the samples are probability samples, which is suggested because of the correlational scope [42]. Given the quantitative nature of the research, the survey method will be useful for collecting and analyzing the responses [42]. Questionnaires were used as instruments for the collection of information, which served as summative indexes, typologies and scales to calibrate the attitudes of the population under investigation.

The reliability of the instrument was determined by Cronbach's alpha, and to validate the adequacy of the factor analysis in this study, two key statistical tests were used. The Kaiser-Meyer-Olkin measure (KMO) yielded results that indicate a sufficiently high correlation between variables to justify the factor analysis, although it suggests that there could be room for improvement in sample adequacy. On the other hand, Bartlett's test of sphericity rejected the null hypothesis of no correlation between variables (p<.001), providing significant statistical evidence that the variables are correlated. This last result fulfills an essential requirement to proceed with factor analysis, supporting the relevance of this technique in the research context.

The 27-item reliability test questionnaire was developed using Google Forms and each question corresponds to one of the two variables. The surveys and the data they collected were handled with the utmost care to ensure privacy, confidentiality and while honoring the participants.

The SPSS program was used to analyze the data collected, applying descriptive and inferential statistical techniques. Tables were prepared to present proportions and frequency; however, a multiple correlation model and nonparametric ordinal logistic regression were used to analyze the inferential data [46], [47]. This methodology allowed not only to describe the data collected, but also to examine the relationships between variables and to test the hypotheses put forward, thus providing a solid basis for research findings in the field of CIB and RM in DM [48].

3. RESULTS AND DISCUSSION

3.1. Description of variables

Table 1 shows, with respect to RM, that 24.8% of CIB analysts consider the level of RM to be very poor, 19.7% say that it is a standard level and 55.4% quite high. On the other hand, in dimension 1, risk identification, 12.5% of analysts consider the level to be deficient. On the other hand, risk analysis, and assessment, 12.7% of CIB analysts scored a very poor level, 33.5% between a standard level, and 32.0% high. In the third dimension, the treatment of risks, 10.1% of analysts indicated a very poor level, 32.0% an average level and 57.9% an adequate level. In the fourth dimension, the treatment of risks, 10.1% of analysts rank very poorly, 33.5% at a standard level, and 32.0% high.

Table 1. Detail of the multiple layers and characteristics of the RM variable

Ranks/levels	Poor		Fair		Good		Total	
Variable and dimensions	f	%	f	%	f	%	f	%
RM	121	24.8	96	19.7	270	55.4	487	100.0
D1: risk identification	61	12.5	164	33.7	262	53.8	487	100.0
D2: risk analysis and assessment	62	12.7	163	33.5	156	32.0	487	100.0
D3: risk treatment	49	10.1	156	32.0	282	57.9	487	100.0

Table 2 shows how often and in what proportion certain levels of the CIB variable and its dimensions occur; on the CIB variable, it was observed that 23.2% of CIB analysts suggested an very poor level of CIB; within the first dimension, security policies and procedures, 12.7% of CIB analysts stated an very poor level, 34.7% a standard level, and 52.6% quite high; in the second dimension, technical security controls, 9.9% of CIB analysts reported a very poor level, 31.0% a standard level, and 59.1% fairly high. As for the third dimension, CIB culture, 12.3% of analysts reported a very poor level, 33.3% a standard level, and 54.4% high.

Table 2. Detail of the multiple layers and characteristics of the CIB variable

Ranks/levels	Poor		Fair		Good		Total	
Variable and dimensions	f	%	f	%	f	%	f	%
CIB	113	23.2	200	41.1	174	35.7	487	100.0
D1: security policies and procedures	62	12.7	169	34.7	256	52.6	487	100.0
D2: technical safety controls	48	9.9	151	31.0	288	59.1	487	100.0
D3: CIB culture	60	12.3	162	33.3	265	54.4	487	100.0

Table 3 shows the levels of the DM variable and their frequencies in percentages. Regarding the DM variable, 19.9% of CIB analysts reported a very good level of DM, while 42.5% reported a standard level and 37.6% a high level. In dimension 1, information quality, 10.5% of the analysts reported a very poor level. In the second dimension, DM process, 12.5% of the CIB analysts had a very poor level, 28.3% a standard level, and 59.1% quite high. In the third dimension, decision effectiveness, 6.6% had a very poor level, 34.3% a standard level, and 59.1% high. In the fourth dimension, the quality of information, 6.6% have a very poor level, 34.3% a standard level, and 59.1% high. Finally, in the fourth dimension, information quality, 6.5% of CIB analysts have a very poor level, 28.3% a standard level, and 59.1% high.

Table 3. Detail of the multiple layers and characteristics of the variable DM

Ranks/levels	Poor		Fair		Good		Total	
Variable and dimensions	f	%	f	%	f	%	f	%
DM	97	19.9	207	42.5	183	37.6	487	100.0
D1: quality of information	51	10.5	157	32.2	279	57.3	487	100.0
D2: DM process	61	12.5	138	28.3	288	59.1	487	100.0
D3: effectiveness of decisions	32	6.6	167	34.3	288	59.1	487	100.0

3.2. Hypothesis testing

H1: RM and CIB influence SNIEP DM in 2024.

Table 4 shows the significance value (p<0.05), which indicates that the regression model is sufficient to continue the study. Also, according to Nagelkerke's Pseudo R-squared 0.075 statistics, RM and the CIB have a mutual dependency ratio in DM of 7.5%.

Table 4. Information on model fit and R-squared explaining the influence of RM and CIB on DM

Model	Logarithm of the likelihood - 2	Chi-square	gl	Sig.	Pseudo R square	
Intersection only	137.330				Cox y Snell	.066
Final	104.268	33.062	4	.000	Nagelkerke	.075
Liaison function: logit.					McFadden	.032

According to the significant results shown in Table 5, it can be deduced that both RM and CIB influence DM. When the RM is low and fair, DM is bad and not fair. Similarly, when CIB is poor and fair, DM is poor and fair. Also, considering significance, the null hypothesis is rejected, which means that CIB and RM impact DM in SNIEP in 2024.

Table 5. Parameter estimates for RM and CIB at DM

		Estimate	Desv. error	Wald	gl	Sig.	95% confidence interval	
							Lower limit	Upper limit
Umbral	[DM=Poor]	-2.214	.192	133.154	1	.000	-2.590	-1.838
	[DM=Fair]	-.215	.160	1.807	1	.179	-.529	.099
Location	[RM=Poor]	-.643	.208	9.499	1	.002	-1.051	-.234
	[RM=Fair]	-.708	.226	9.806	1	.002	-1.151	-.265
	[RM=Good]	0^a	.	.	0	.	.	.
	[CIB=Poor]	-.686	.231	8.838	1	.003	-1.138	-.234
	[CIB=Fair]	-.689	.200	11.852	1	.001	-1.081	-.297
	[CIB=Good]	0^a	.	.	0	.	.	.

H2: RM and CIB have an impact on the quality of SNIEP information, 2024.

The regression model is sufficient to proceed with the analysis, as shown in Table 6, as it is significant (p<0.05) when entering the model fit data. Similarly, regarding the Pseudo R2 test, the Pseudo R-squared statistic - according to Nagelkerke - reveals a value of 0.043, suggesting a 4.3% dependence of RM and CIB on the quality of DM information.

Table 6. Model fit and Pseudo R2 explaining the influence of RM and CIB on the quality of DM information

Model	Logarithm of the likelihood - 2	Chi-square	gl	Sig.	Pseudo R square	
Intersection only	101.140				Cox y Snell	.036
Final	83.070	18.070	4	.000	Nagelkerke	.043
					McFadden	.020
Link function: logit.						

The results of the significance tests indicate that the variables RM (p=0.205>0.05) and CIB (p=0.025<0.05) influence the information quality dimension of DM (p=0.004<0.05) at both the bad and re-gular levels, with significances of 0.000<0.05 and 0.000<0.05, respectively. This means that, when RM is at a bad level, DM in the information quality dimension will also be bad and re-gular, and vice versa when CIB is low and fair. Likewise, the null hypothesis will be rejected, so: RM and CIB impact the quality of the information used in the DM of the SNIEP to 2024, see Table 7.

Table 7. Parameter estimates with respect to RM and CIB on the quality of DM information

		Estimate	Desv. error	Wald	gl	Sig.	95% confidence interval	
							Lower limit	Upper limit
Umbral	[Quality of information=Poor]	-2.765	.220	158.301	1	.000	-3.196	-2.335
	[Quality of information=Fair]	-.868	.175	24.620	1	.000	-1.211	-.525
Location	[RM=Poor]	-.276	.218	1.604	1	.205	-.703	.151
	[RM=Fair]	-.562	.232	5.860	1	.015	-1.017	-.107
	[RM=Good]	0a	.	.	0	.	.	.
	[CIB=Poor]	-.547	.244	5.030	1	.025	-1.025	-.069
	[CIB=Fair]	-.617	.212	8.460	1	.004	-1.033	-.201
	[CIB=Good]	0a	.	.	0	.	.	.

Liaison function: logit.
a. This parameter is set to zero because it is redundant.

H3: The RM and CIB have an impact on the SNIEP DM process, 2024.

Table 8 shows that there is a significant result (p<0.05) when entering the model fit data, indicating that the regression model is sufficient to proceed with the study. Similarly, with respect to the pseudo R2 test, the pseudo R-squared statistic-according to Nagelkerke-reveals a value of 0.043, suggesting a 4.3% dependence of RM and CIB on the SNIEP DM process.

Table 8. Information on the fit of the R-squared model explaining the influence of RM and CIB on the DM process

Model	Logarithm of the likelihood - 2	Chi-square	gl	Sig.	Pseudo R square	
Intersection only	112.655				Cox y Snell	.036
Final	94.690	17.965	4	.001	Nagelkerke	.043
					McFadden	.020

Liaison function: logit.

According to the significance results, it is noted that RM has a negative impact on the DM process dimension when the p-value is less than 0.05 and CIB has a negative impact when the p-value is less than 0. 004 and CIB are negatively correlated with DM when the p-value is less than 0.05 and CIB is positively correlated with DM when the p-value is less than 0.05 and DM when the p-value is less than 0.000 is also negative and fairly impacted by CIB. Likewise, considering the importance of the decisions, we reject the null hypothesis and conclude that the CIB and RM have an impact on the DM of the SNIEP in 2024, see Table 9.

Table 9. Parametric test of the significant influence of RM and CIB on the process of DM

		Estimate	Desv. error	Wald	gl	Sig.	95% confidence interval	
							Lower limit	Upper limit
Umbral	[DM Process=Poor]	-2.567	.213	145.365	1	.000	-2.984	-2.149
	[DM Process=Fair]	-.954	.177	28.937	1	.000	-1.302	-.607
Location	[RM=Poor]	-.492	.216	5.178	1	.023	-.917	-.068
	[RM=Fair]	-.431	.235	3.354	1	.067	-.891	.030
	[RM=Good]	0a	.	.	0	.	.	.
	[CIB=Poor]	-.697	.243	8.218	1	.004	-1.173	-.220
	[CIB=Fair]	-.493	.214	5.288	1	.021	-.913	-.073
	[CIB=Good]	0a	.	.	0	.	.	.

Liaison function: logit.
a. This parameter is set to zero because it is redundant.

H4: RM and CIB influence the effectiveness of SNIEP decisions, 2024.

Table 10 shows that, when entering the model fit data, it is significant (p<0.05), establishing that the regression model is adequate to continue the analysis. Likewise, the Pseudo R-squared statistic, specifically Nagelkerke reports a result of 0.043, which indicates a 4.3% dependence of RM and CIB on the effectiveness of SNIEP decisions.

Table 10. Model fit and Pseudo R2 explaining the influence of RM and CIB on the effectiveness of DM decisions

Model	Logarithm of the likelihood - 2	Chi-square	gl	Sig.	Pseudo R square	
Intersection only	88.469				Cox y Snell	.036
Final	79.418	9.050	4	.060	Nagelkerke	.043
					McFadden	.020
Liaison function: logit.						

From the significance results, it can be inferred that the variables RM (p=0.131>0.05) and CIB (p=0.119>0.05) have an impact on DM effectiveness at both the bad and fair levels, with significances of 0.000<0.05 and 0.000<0.05, respectively. This means that when the RM is at a bad level, the DM in the decision effectiveness dimension will also be bad and fair, and vice versa when the CIB is low and fair. RM and CIB impact DM effectiveness in SNIEP, 2024, see Table 11.

Table 11. Parameter estimates regarding RM and CIB on the effectiveness of DM decisions

		Estimate	Desv. error	Wald	gl	Sig.	95% confidence interval	
							Lower limit	Upper limit
Umbral	[Effectiveness of decisions=Poor]	-3.102	.242	164.671	1	.000	-3.576	-2.628
	[Effectiveness of decisions=Fair]	-.793	.174	20.826	1	.000	-1.134	-.452
Location	[RM=Poor]	-.331	.219	2.275	1	.131	-.760	.099
	[RM=Fair]	-.319	.237	1.808	1	.179	-.785	.146
	[RM=Good]	0^a	.	.	0	.	.	.
	[CIB=Poor]	-.383	.246	2.430	1	.119	-.864	.099
	[CIB=Fair]	-.440	.213	4.270	1	.039	-.858	-.023
	[CIB=Good]	0^a	.	.	0	.	.	.
Liaison function: logit.								

a. This parameter is set to zero because it is redundant.

The results obtained indicate that the RM and CIB variables are statistically associated with the dimensions of the SNIEP, including decision-making, information quality, the decision-making process and the decisions themselves, all with a significance level of p=0.000, which shows a high statistical reliability in the results. However, the Nagelkerke R² values 0.075 for decision-making and 0.043 for the other dimensions reveal that, although there is a statistically significant relationship, the explanatory power of the model is low. In quantitative terms, this implies that RM and CIB explain only 7.5% of the variability in decision-making and only 4.3% in the other dimensions evaluated, which limits their ability to predict or fully describe the behavior of the SNIEP.

These figures suggest that, although RM and CIB are relevant elements for understanding SNIEP performance, there are other factors not included in the model that have a more decisive influence on the dimensions analyzed. From a practical perspective, this implies that public policies aimed at improving information management and decision-making processes should contemplate more comprehensive strategies, including additional organizational, technological and human variables. Among the main limitations of the research are the low explanatory capacity of the model, the cross-sectional approach that prevents establishing causality, and the possible omission of key variables that affect the SNIEP, which limits the generalizability and applicability of the results for the formulation of public policies.

RM and CIB, although relevant, are only components within a broader, multifactorial ecosystem of national CIB decision-making. Factors such as the geopolitical environment, institutional maturity, international alliances, technological investment, and organizational culture also have a significant impact, which justifies why the model does not capture the full complexity of the phenomenon.

3.3. Discussion

3.3.1. Risk management and cybersecurity about SNIEP decision making

The investigation of RM and CIB on SNIEP DM in 2024 yielded significant findings. The overall objective was to assess the influence of these factors on DM, and the results revealed a 7.5% dependence according to Nagelkerke's pseudo R-squared statistic. This indicates that the effective implementation of RM practices and CIB measures has a considerable impact on the system's decision-making processes. RM, as a systematic and proactive process to identify, assess and address risks, enables organizations to make informed and informed decisions, considering the uncertainties and potential consequences of each alternative. This proactive and structured approach helps institutions anticipate potential adverse events and develop strategies to mitigate them or take advantage of associated opportunities, resulting in a more robust and resilient DM.

In addition, RM facilitates the prioritization of resources and efforts by making it possible to identify the most critical risks with the greatest potential impact, and to make better use of the resources available to deal with them. This is especially relevant in the context of the public sector, where resources are often limited and demands are multiple and varied. Adequate RM makes it possible to optimize the allocation of resources and focus efforts on those aspects that are most important for the achievement of institutional objectives and the production of a public benefit.

However, CIB-defined as the combination of technological, organizational and human safeguards designed to prevent unauthorized access to computer systems, networks and related data-is an essential component in ensuring the reliability, authenticity and accessibility of DM data. CIB is becoming an essential part of the operation of any business, public or private, in today's highly digitized and connected world, where cyber-attacks are common and increasingly intelligent. The ability of companies to maintain their activity, their credibility, the protection of their customers' information and the trust of their citizens are vulnerable to cyber-attacks, so it is essential to have a solid CIB strategy that protects the organization's systems, networks and data.

These findings are consistent with the study by Chenou [49] who concluded that CIB is an indispensable element in every aspect of digital justice in Colombia, and that it is necessary to strengthen the legal framework, develop awareness and training programs, increase the infrastructure to handle cyber-attacks, and learn how other countries have improved their CIB. This research underscores the importance of addressing CIB problems in the public sector with a comprehensive and interdisciplinary approach, including not only technical aspects, but also legal, educational and international cooperation. It also emphasizes the need to build both human and institutional capacity to counter cyber risks and ensure the security and reliability of digital processes in the administration of justice.

3.3.2. Risk management and cybersecurity about quality of SNIEP information

Regarding the first specific objective, a 4.3% influence of RM and CIB on the quality of information used in DM was determined. This highlights the importance of having complete, accurate and timely data to support decisions, which is favored by solid RM and CIB. Information quality is a critical aspect of DM, as erroneous, incomplete or outdated data can lead to suboptimal or even detrimental decisions for the organization. Therefore, ensuring data completeness, consistency and up-to-dateness is fundamental for making sound and strategic decisions.

In this sense, RM makes it possible to identify and evaluate possible risks that may affect the quality of information, such as human errors in data entry, failures in information systems, malicious manipulation of data, among others. Based on this identification, controls and mitigation measures can be established to prevent or reduce the impact of these risks on information quality. For example, the implementation of data validation and verification processes, periodic audits, segregation of duties and the establishment of access levels and permissions according to roles and responsibilities.

The CIB plays a fundamental role in protecting the integrity, confidentiality and availability of information. Digital security controls, such as data encryption, user authentication, intrusion detection, among others, safeguard data against unauthorized access, tampering, leakage or loss. Likewise, the implementation of security policies and procedures, such as password management, classification of information according to its criticality, and incident response protocols, contribute to maintaining a secure and reliable information environment for DM. This approach is complemented by continuous audit testing and financial fraud detection [50].

RM helps identify and mitigate threats that may compromise the integrity and reliability of information, while CIB establishes controls and measures to protect systems and databases against unauthorized access, tampering, or loss of information. For example, conducting periodic risk assessments can help identify vulnerabilities in information systems, such as security flaws, outdated software or inadequate configurations, which may expose data to potential threats. Based on this identification, security measures can be implemented, such as software patches, secure configurations, monitoring of suspicious activities, among others, to protect the integrity and confidentiality of the information.

These results are in line with those presented by Rafi *et al.* [51], who identified the critical challenges that negatively affect data quality assessment in DevOps environments, highlighting real-time data analysis, data visualization, and missing and invalid information as priority issues to be addressed. This study underscores the importance of having adequate processes and tools in place to ensure data quality in dynamic and complex environments, such as those that characterize software development and cloud infrastructure management. The automation of data validation and cleansing processes, as well as the use of real-time analysis and visualization techniques, can contribute to improving the quality of information and facilitate informed and timely DM.

3.3.3. Risk management and cybersecurity about SNIEP decision making process

Regarding the second specific objective, a 4.3% influence of RM and CIB on the DM process itself was identified. This suggests that incorporating risk and digital security considerations into decision-making methodologies and criteria can improve the effectiveness and robustness of decisions. RM provides a framework for evaluating different alternatives and their potential consequences, considering the risks associated with each option and enabling more informed and strategic DM. By integrating risk assessment into the DM process, organizations can anticipate potential negative impacts and develop contingency, and mitigation plans for each alternative, enabling more resilient and adaptive decisions in the face of uncertainty and environmental changes.

RM improves quality and efficiency in DM by providing a structured, evidence-based methodology for evaluating and comparing options through clear criteria, reliable analysis and scenario modeling. This facilitates objective and transparent decisions that balance stakeholder preferences and trade-offs. On the other hand, the CIB protects the availability, integrity and confidentiality of critical information systems for DM, protecting them from cyber threats such as malware, phishing and denial of service attacks. Given the growing role of digital technologies in processing large volumes of data, ensuring their security is essential to preserve the quality and timeliness of organizational decisions.

These findings are related to those proposed by Stergiopoulos *et al.* [52], who analyzed patterns of cyber-attacks in the oil and gas sector, concluding that improved basic security controls and staff awareness are required to strengthen informed DM against these threats. This study highlights the importance of implementing technical security measures, such as network segmentation, patch and update management, and suspicious activity monitoring, to protect industrial control systems and critical information assets. It also stresses the need to develop training and awareness programs for employees to identify and report potential security incidents, and to comply with established policies and procedures to maintain a secure environment.

3.3.4. Risk management and cybersecurity about SNIEP decisions

The analysis of the third specific objective showed a 4.3% influence of RM and CIB on the effectiveness of SNIEP decisions, although the regression model did not find statistical significance. The effectiveness of DM, defined as the ability to achieve expected results and generate value, depends on sound processes and reliable data. RM allows the evaluation of impacts, risks and benefits of alternatives, considering costs, deadlines and obstacles, facilitating choices aligned with organizational priorities. CIB ensures the continuity, integrity and protection of critical systems, preventing interruptions due to incidents such as ransomware or phishing and mitigating reputational, legal and strategic risks associated with leaks of sensitive information.

This aligns with the findings of [52] who concluded that CIB significantly influences RM in an educational institution in Callao in 2023, with a 37.7% variability in RM attributable to the influence of CIB. This study highlights the importance of implementing digital security controls and measures to protect the information assets and critical processes of educational organizations, such as academic management, research and innovation. It also highlights the need to develop a culture of CIB at all levels of the institution, from students and teachers to managers and administrative staff, to create a secure and reliable environment that favors learning and knowledge generation.

The behavioral patterns component focuses on identifying and analyzing employee behaviors and attitudes that may generate CIB risks, whether due to error, negligence or lack of knowledge. This involves studying the habits and practices of users in the handling of information and systems, as well as their level of awareness and training in digital security issues. Based on this analysis, awareness-raising, training and communication strategies can be developed to promote secure and responsible behavior, and to actively involve employees in the protection of information assets.

The RM matrix component makes it possible to evaluate and prioritize the identified CIB risks, considering their probability of occurrence, their potential impact and the existing controls to mitigate them. This matrix facilitates the DM on the most appropriate treatment measures for each risk, whether to avoid, reduce, transfer or accept it, and the allocation of responsibilities and resources for its implementation. Likewise, the risk matrix is a dynamic tool that must be updated periodically, as the internal and external conditions of the organization change, and as new risks are identified or existing ones are modified.

Also, [53] concluded that the regulations on CIB in Peru are still not very specific, there is a clear relationship between CIB and cybercrime, and there is a need to strengthen the capacities of citizens in general on CIB, from the top to the lowest level in organizations. These findings underscore the importance of developing more robust and specific CIB policies and regulations, as well as promoting a culture of awareness and training at all levels of Peruvian public institutions. The regulations on CIB in Peru have developed progressively in recent years, but there are still important gaps and challenges. For example, Peru's Personal Data Protection Law establishes principles and obligations for the processing of personal data but does not specifically address CIB risks and controls to protect such data in digital environments.

Likewise, Peru's digital security legislation defines general objectives and guidelines to strengthen digital security in the country but does not establish a detailed regulatory framework or specific obligations for public and private entities. In this context, it is necessary to develop a more complete and updated legislation on CIB that addresses aspects such as RM, critical infrastructure protection, incident response, public-private cooperation, among others, and that is consistent with international standards and best practices.

In addition, the relationship between CIB and cybercrime poses significant challenges for the prevention, investigation and punishment of cybercrime in Peru. Cybercrime encompasses a wide range of illegal activities committed using information and communication technologies, such as electronic fraud, ransomware, phishing, identity theft, among others. These crimes can have a significant impact on the security and privacy of citizens, as well as on the stability and confidence of the country's financial and commercial system. In terms of related theories, the results are aligned with the CIB framework proposed by [13], which considers the technical, organizational and human dimensions as key aspects for an effective CIB. This multidimensional approach recognizes that CIB goes beyond technological solutions, and requires policies, procedures, organizational culture and people awareness to adequately protect digital assets and critical information.

CIB encompasses three key dimensions: technical, organizational and human. The technical dimension comprises technological controls such as encryption, authentication and intrusion detection, designed to prevent, detect and respond to cyber threats, ensuring confidentiality, integrity and availability of information. The organizational dimension includes policies, procedures and structures, such as clear roles, incident management and business continuity, integrating CIB into the organization's processes and culture. Finally, the human dimension focuses on training and raising employee awareness of cyber risks, promoting secure behaviors, and addresses ethical and legal aspects such as privacy and personal data protection.

The research is based on the ISO 31000 standard, which provides a framework for integrating RM into organizational governance, facilitating informed decisions and institutional resilience. It also highlights the role of CIB in protecting digital assets and preventing threats that affect the quality of decisions. A comprehensive approach-technical, organizational and human-adapted to the Peruvian context is proposed, highlighting the need for capacity building, preventive culture and effective communication in the public sector.

4. CONCLUSION

It is concluded that RM and CIB significantly influence SNIEP DM in 2024. Their implementation improves the quality, process, and effectiveness of decisions by ensuring accurate and secure data, fostering a structured and agile environment, and aligning decisions with strategic objectives. Measures such as technical controls, security culture and staff training strengthen the State's IT infrastructure and confidence in its decisions.

It is recommended that longitudinal studies be conducted to evaluate the evolution of RM and CIB in the National Informatics System over time, to identify trends, progress and persistent challenges. Likewise, broaden the scope of the research to other public entities and levels of government, such as regional and local governments, to obtain a more representative and comparative view. Finally, it is recommended that Peruvian state entities develop and implement a comprehensive CIB management system (CIBMS), aligned with international standards such as ISO 31000 and NIST SP 800-37, adapted to the specific context and needs of the Peruvian public sector. This system should include risk identification, analysis, evaluation, and treatment processes, as well as monitoring, communication and continuous improvement mechanisms.

It is suggested to promote research, development and innovation in the field of CIB and RM in the country, through strategic alliances with universities, research centers and specialized companies. Similarly, raise awareness and educate citizens in general about the risks and responsibilities associated with the use of digital technologies, and the importance of CIB and the protection of personal data for the exercise of their rights and freedoms. This involves developing communication and public education campaigns, providing clear and accessible information on the most common cyber threats and basic prevention and protection measures, and promoting the participation and empowerment of civil society in the governance of the CIB.

The practical relevance of the study lies in its ability to guide the improvement of the digital infrastructure of the Peruvian State, showing how RM and CIB strengthen decision-making in the SNIEP. By identifying practices and policies that optimize the quality and security of information, the study provides valuable inputs to design strategies that make digital public services more efficient and reliable, increase institutional resilience to cyber threats and promote more transparent and effective governance.

It is suggested that capacity building programs be implemented for technical staff and strategic decision makers, integrated threat intelligence platforms be established to unify national and international sources, and regular simulation exercises be conducted to improve preparedness and coordination in the face of cyber incidents. These measures would complement the current approach and enable a more holistic response to complex and evolving risks.

Finally, the results of the study make a concrete contribution to SDG 9 (industry, innovation, and infrastructure) by highlighting the need to strengthen national critical infrastructure from a cyber perspective. Improving responsiveness and tactical intelligence not only strengthens digital defense, but also incentivizes a trusted environment for technological innovation, investment in resilient digital infrastructure, and the sustainable development of key industrial capabilities.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Frank Agustín Olivos Estrada	✓		✓		✓	✓		✓	✓	✓				
Willian Sebastian Flores-Sotelo	✓		✓		✓	✓		✓		✓				
Carmen Rosa Barrera-Avalos		✓		✓		✓				✓		✓		
Williams Arturo Martínez-Aberga	✓			✓	✓	✓			✓					
Richard Sulca-Guillen		✓		✓		✓		✓	✓					
Jorge Miguel Chávez-Díaz		✓	✓			✓	✓			✓	✓	✓		

C :	**C**onceptualization	I :	**I**nvestigation	Vi :	**Vi**sualization
M :	**M**ethodology	R :	**R**esources	Su :	**Su**pervision
So :	**So**ftware	D :	**D**ata Curation	P :	**P**roject administration
Va :	**Va**lidation	O :	Writing - **O**riginal Draft	Fu :	**Fu**nding acquisition
Fo :	**Fo**rmal analysis	E :	Writing - Review & **E**diting		

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Derived data supporting the conclusions of this study are available upon request from the corresponding author, JMCD.

REFERENCES

[1] E. G. Franco, "Global Risks 2020: An Unsettled World," *World Economic Forum*, pp. 8–17, 2020.

[2] McKinsey and Compañy, "How to master the seven step problem solving process," *M. Night Shyamalan*, pp. 98–102, 2023, doi: 10.2307/jj.7193915.20.

[3] Inter American Development Bank and Organization of American States, "2020 Cybersecurity Report: Risks, Progress, and the Way Forward in Latin America and the Caribbean," Jul. 2020, doi: 10.18235/0002513.

[4] M. Santiago-Castro and C. J. Brown, “Ownership structure and minority rights: A Latin American view,” *Journal of Economics and Business*, vol. 59, no. 5, pp. 430–442, Sep. 2007, doi: 10.1016/j.jeconbus.2007.04.005.

[5] N. Justo *et al.*, “Real-World Evidence in Healthcare Decision Making: Global Trends and Case Studies from Latin America,” *Value in Health*, vol. 22, no. 6, pp. 739–749, Jun. 2019, doi: 10.1016/j.jval.2019.01.014.

[6] Unión Internacional de Telecomunicaciones [UIT], *Global Cybersecurity Index (GCI)*, 2020.

[7] M. T. Toapanta, J. D. L. Cobeña, and L. E. M. Gallegos, “Analysis of cyberattacks in public organizations in Latin America,” *Advances in Science, Technology and Engineering Systems*, vol. 5, no. 2, pp. 116–125, 2020, doi: 10.25046/aj050215.

[8] R. R. S. Ruidias, B. P. Nunes, R. Manrique, and S. Siqueira, “Assessing Data Landscapes for Quality Education in Latin America: A FAIRness Perspective on Brazil, Colombia, and Peru,” *Journal of Learning Analytics*, vol. 12, no. 2, pp. 175–195, Aug. 2025, doi: 10.18608/jla.2025.8441.

[9] A. Paredes-Soria, A. S. Paredes-Egúsquiza, J. A. Villagómez-Chinchay, J. L. De V. Borda, and J. M. Chávez-Díaz, “Adapting the Extended Solow Model: The Impact of Output Determinants on Economic Growth in Peru from 2000 to 2022,” *Journal of Risk and Financial Management*, vol. 18, no. 3, pp. 112–134, Feb. 2025, doi: 10.3390/jrfm18030112.

[10] W. S. Flores-Sotelo, O. Pongo-Águila, C. A. Rivas-Peña, and J. M. Chávez-Diaz, “An analysis of fiscal management and macroeconomic stability: An econometric study of public policies in Latin American countries,” *Journal of Infrastructure, Policy and Development*, vol. 8, no. 8, pp. 1-15, Aug. 2024, doi: 10.24294/jipd.v8i8.6547.

[11] A. Paredes-Soria, H. R. Jaime-Belleza, V. I. Tafur-Anzualdo, and J. M. Chávez-Díaz, “Determinants of economic growth and the externalities of infrastructure investment, Peruvian case 2000–2022,” *Journal of Infrastructure, Policy and Development*, vol. 8, no. 13, pp. 1-20, Nov. 2024, doi: 10.24294/jipd9068.

[12] M. Veale and I. Brown, “Cybersecurity,” *Internet Policy Review*, vol. 9, no. 4, Dec. 2020, doi: 10.14763/2020.4.1533.

[13] A. Garg, A. Pandey, N. Sharma, A. Kumar, P. K. Jha, and R. K. Singhal, “An In-Depth Analysis of the Constantly Changing World of Cyber Threats and Defences: Locating the Most Recent Developments,” in *2023 International Conference on Power Energy, Environment & Intelligent Control (PEEIC)*, IEEE, Dec. 2023, pp. 181–186, doi: 10.1109/PEEIC59336.2023.10451963.

[14] B. W. Wirtz and J. C. Weyerer, “Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats,” *International Journal of Public Administration*, vol. 40, no. 13, pp. 1085–1100, Nov. 2017, doi: 10.1080/01900692.2016.1242614.

[15] F. F. Adedoyin and B. Christiansen, *Effective Cybersecurity Operations for Enterprise-Wide Systems*. GI Global, 2023, doi: 10.4018/978-1-6684-9018-1.

[16] B. Firmansyah, *Cybersecurity fundamentals*, IGI Global Scientific Publishing, 2024, doi: 10.4018/979-8-3693-3860-5.ch009.

[17] S. Kamil, H. S. A. S. Norul, A. Firdaus, and O. L. Usman, “The Rise of Ransomware: A Review of Attacks, Detection Techniques, and Future Challenges,” in *2022 International Conference on Business Analytics for Technology and Security, ICBATS 2022*, 2022, doi: 10.1109/ICBATS54253.2022.9759000.

[18] H. Elkhannoubi and M. Belaissaoui, “A framework for an effective cybersecurity strategy implementation: Fundamental pillars identification,” in *International Conference on Intelligent Systems Design and Applications, ISDA*, 2016, pp. 1–6, doi: 10.1109/ISDA.2015.7489156.

[19] A. A. Hammad, S. R. Ahmed, M. K. Abdul-Hussein, M. R. Ahmed, D. A. Majeed, and S. Algburi, “Deep Reinforcement Learning for Adaptive Cyber Defense in Network Security,” in *ACM International Conference Proceeding Series*, 2024, pp. 292–297, doi: 10.1145/3660853.3660930.

[20] E. K. Ghani, “A Qualitative Investigation on Risk Management Implementation in the Malaysian Public Sector,” *Economic Affairs*, vol. 68, no. 2, Jun. 2023, doi: 10.46852/0424-2513.2.2023.30.

[21] D. Nel, “Risk management in the South African local government and its impact on service delivery,” *International Journal of Management Practice*, vol. 12, no. 1, pp. 60-80, 2019, doi: 10.1504/IJMP.2019.096683.

[22] Y. Lu, “The Relationship Between Public Budgeting and Risk Management: Competition or Driving?,” *Enterprise Security: Second International Workshop*, 2017, pp. 40–72, doi: 10.1007/978-3-319-54380-2_3.

[23] H. Mahama, M. Elbashir, S. Sutton, and V. Arnold, “Enabling enterprise risk management maturity in public sector organizations,” *Public Money & Management*, vol. 42, no. 6, pp. 403–407, Aug. 2022, doi: 10.1080/09540962.2020.1769314.

[24] M. Woods, “A contingency theory perspective on the risk management control system within Birmingham City Council,” *Management Accounting Research*, vol. 20, no. 1, pp. 69–81, Mar. 2009, doi: 10.1016/j.mar.2008.10.003.

[25] H. Vochitoiu, F. Vedinas, O. Miclea, and C. L. Unguras, “Risk Management as a Part of the Business Process in Corporate Firms,” *New Technologies, Development and Application III*, 2020, pp 964–972, doi: 10.1007/978-3-030-46817-0_109.

[26] M. Ben-Daya, *Failure Mode and Effect Analysis*, Handbook of Maintenance Management and Engineering, 2009, pp 75–90, doi: 10.1007/978-1-84882-472-0_4.

[27] T. Khinvasara, S. Ness, and N. Tzenios, “Risk management in pharma and Medical Device industry,” *Journal of Engineering Research and Reports*, vol. 25, no. 8, pp. 130–140, 2023, doi: 10.9734/JERR/2023/v25i896.

[28] H. H. Einstein and R. L. Sousa, “Decision Analysis Applied to Natural Hazards,” *International Probabilistic Workshop* vol. 153, pp. 3-13, 2021, doi: 10.1007/978-3-030-73616-3_1.

[29] International Organization for Standardization [ISO], “ISO 31000:2018 - Gestión de riesgos - Directrices.” [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en. (Date accessed: Dec. 26, 2023).

[30] C. Sauerwein, “Integrating shared cyber security information into information security risk management,” in *CEUR Workshop Proceedings*, 2016.

[31] J. J. C. M, “Security Risk Management and Cybersecurity: From the Victim or from the Adversary?,” *Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability*, 2023, pp. 1-8, doi: 10.1007/978-3-031-20160-8_1.

[32] J. L. Spears, “The effects of user participation in identifying information security risk in business processes,” in *SIGMIS CPR’06 - Proceedings of the 2006 ACM SIGMIS CPR Conference*, 2006, pp. 351–352, doi: 10.1145/1125170.1125252.

[33] S. Flowerday and R. V. Solms, “Real-time information integrity = system integrity + data integrity + continuous assurances,” *Computers & Security*, vol. 24, no. 8, pp. 604–613, 2005, doi: 10.1016/j.cose.2005.08.004.

[34] A. A. Odejide and T. Iyamu, “Structuration analysis of factors influencing risk management system deployment,” in *2012 IEEE 6th International Conference on Management of Innovation and Technology, ICMIT 2012*, 2012, pp. 405–411, doi: 10.1109/ICMIT.2012.6225840.

[35] L. Wilbanks, “Whats Your IT Risk Approach?,” *IT Professional*, vol. 20, no. 4, pp. 13–17, 2018, doi: 10.1109/MITP.2018.043141663.

[36] C. Deaver-Vazquez, E. Taylor, D. Rowley, and B. Langis, “A Quantitative Approach to Assessing and Managing Cybersecurity Risks,” *EDPACS*, vol. 69, no. 4, pp. 7–11, Apr. 2024, doi: 10.1080/07366981.2024.2340849.

[37] O. Keskin, U. Tatar, O. Poyraz, A. Pinto, and A. Gheorghe, “Economics-based risk management of distributed denial of service attacks: A distance learning case study,” in *Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018*, 2018, pp. 343–352.

[38] K. Kramarz and J. Korpysa, “The evolution of the concept of risk management in IT+ organizations,” in *Procedia Computer Science*, 2023, pp. 4843–4849, doi: 10.1016/j.procs.2023.10.484.

[39] A. Althonayan and A. Andronache, “Resiliency under strategic foresight: The effects of cybersecurity management and enterprise risk management alignment,” in *2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019*, 2019, doi: 10.1109/CyberSA.2019.8899445.

[40] J. (Annabella) Huang and U. Murthy, “The impact of cybersecurity risk management strategy disclosure on investors’ judgments and decisions,” *International Journal of Accounting Information Systems*, vol. 54, pp. 1-17, Sep. 2024, doi: 10.1016/j.accinf.2024.100696.

[41] A. Couce-Vieira, D. R. Insua, and A. Kosgodagan, “Assessing and forecasting cybersecurity impacts,” *Decision Analysis*, vol. 17, no. 4, pp. 356–374, 2020, doi: 10.1287/DECA.2020.0418.

[42] M. Sciberras and A. Dingli, “Quantitative Research,” *Investigating AI readiness in the maltese public administration*, 2023, pp. 43–115, doi: 10.1007/978-3-031-19900-4_11.

[43] F. Hachtmann, “Basic research,” in *Encyclopedia of Sport Management*, Edward Elgar Publishing, 2024, pp. 82–83, doi: 10.4337/9781035317189.ch48.

[44] R. V. Solms and J. van Niekerk, “From information security to cyber security,” *Computing Secure*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[45] R. L. Keeney and H. Raiffa, “Decisions with Multiple Objectives: Preferences and Value Trade-Offs,” *IEEE Trans Syst Man Cybern*, vol. 9, no. 7, p. 403, 1979, doi: 10.1109/TSMC.1979.4310245.

[46] D. McFadden, “Conditional logit analysis of qualitative choice behaivor,” in *Drying Technology*, 1974, pp. 105–142.

[47] N. J. D. Nagelkerke, “A note on a general definition of the coefficient of determination,” *Biometrika*, vol. 78, no. 3, pp. 691–692, 1991, doi: 10.1093/biomet/78.3.691.

[48] D. W. Hosmer Jr., S. Lemeshow, and R. X. Sturdivant, “The Multiple Logistic Regression Model,” in Applied Logistic Regression, 3th ed., John Wiley & Sons, Inc., pp. 35-47, 2013, doi: 10.1002/9781118548387.

[49] J.-M. Chenou, “The contested meanings of cybersecurity: evidence from post-conflict Colombia,” *Conflict, Security & Development*, vol. 21, no. 1, pp. 1–19, Feb. 2021, doi: 10.1080/14678802.2021.1888512.

[50] E. G. Robel *et al.*, “Utilization of CAAT in Continuous Auditing: A Case Applied to the Ministry of Health, Peru 2022-2023,” in *Proceedings of the 22nd LACCEI International Multi-Conference for Engineering, Education and Technology (LACCEI 2024): “Sustainable Engineering for a Diverse, Equitable, and Inclusive Future at the Service of Education, Research*, Latin American and Caribbean Consortium of Engineering Institutions, 2024, doi: 10.18687/LACCEI2024.1.1.1329.

[51] S. Rafi, W. Yu, M. A. Akbar, A. Alsanad, and A. Gumaei, “Multicriteria based decision making of DevOps data quality assessment challenges using fuzzy TOPSIS,” *IEEE Access*, vol. 8, pp. 46958–46980, 2020, doi: 10.1109/ACCESS.2020.2976803.

[52] G. Stergiopoulos, D. A. Gritzalis, and E. Limnaios, “Cyber-Attacks on the Oil Gas Sector: A Survey on Incident Assessment and Attack Patterns,” *Institute of Electrical and Electronics Engineers Inc*, 2020, doi: 10.1109/ACCESS.2020.3007960.

[53] M. Tupia, M. Bruzza, and F. Rodriguez, “An information security framework for ubiquitous services in e-government structures: a peruvian local government experience,” in *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Gdansk, Poland, 2016, pp. 1309-1316, doi: 10.15439/2016F72.

BIOGRAPHIES OF AUTHORS

Frank Agustín Olivos Estrada cybersecurity and risk analyst. He works in the Digital Security Department (DEPSEDIG), belonging to the Technological Intelligence Division (DIVINTEC) of the Intelligence Directorate (DIRIN) of the National Police of Peru (PNP). Systems Engineer by profession. Master’s degree in public management from Universidad César Vallejo. He can be contacted at email: folivos@ucvvirtual.edu.pe.

Prof. Dr. Willian Sebastian Flores-Sotelo head of the Academic Doctoral Office of the EUPG-UNFV. Head of the Research, Innovation and Entrepreneurship Unit of the Faculty of Economic Sciences-UNFV. Coordinator of the INNOVA Module of the CADEP-ACACIA Research Center. Doctor in Economics, master’s in business Economic Management and graduate in Economics from the National University Federico Villarreal. Lecturer on topics related to research. Assigned to the Scientific Network of Latin America and the Caribbean, Spain and Portugal (Redalyc) and the Research Network on Research Teaching (RISEI). Specialists in economic policies, quantitative methods, technological tools for education, scientific dissemination and pedagogy. Principal Professor with more than 34 years of experience in undergraduate and graduate studies at the Universidad Nacional Federico Villarreal. He can be contacted at email: wfloress@unfv.edu.pe.

Prof. Carmen Rosa Barrera-Avalos accountant since 1992 from Universidad San Martin de Porres. She has worked in private and public companies. Masters in finance from Universidad Nacional Federico Villareal. Ph.D. in Accounting from Universidad Nacional Federico Villarreal. Professor since 2018 with appointment since 2021 at Universidad Nacional Federico Villareal. Certified Public Accountant of the College of Accountants. She can be contacted at email: cbarrera@unfv.edu.pe.

Prof. Williams Arturo Martínez-Aberga professional in Accounting, Independent Financial Auditor, with a master's degree in Tax Policy and Management. Doctorate in Accounting. Experienced in Business Management, Consultant of Companies and Non-Profit Entities. Specialist in Implementation of Management Systems. Teacher of Higher Education in different Universities in Peru. He can be contacted at email: williams.martinez@upn.pe.

Prof. Richard Sulca-Guillen master's degree in accounting. D. in Accounting from Universidad Nacional Federico Villarreal. Senior Lecturer at the Universidad Nacional de San Cristobal de Huamanga. Research Professor. He can be contacted at email: richard.sulca@unsch.edu.pe.

Prof. Jorge Miguel Chávez-Díaz is Associate Professor at the undergraduate and postgraduate at the Universidad Nacional Mayor de San Marcos. Ph.D.(c) in Accounting from Universidad Nacional Federico Villarreal. Masters in accounting (mention in Financial Auditing) by ULADECH. Consultant in accounting and financial issues, with the use of CAATTs. Lecturer in Accounting-Systems and Information Technology. Winner of the National Accounting Award 2023 JDCCPP in Perú. Expert in design and conceptual review for research. Member of the Editorial Committee of the scientific journal DEBE-HABER. He can be contacted at email: jchavezdi@unfv.edu.pe.