CYBERSECURITY MATURITY IN A BASIC EDUCATION SCHOOL NETWORK

MATURIDADE EM CIBERSEGURANÇA EM UMA REDE DE ESCOLAS DE EDUCAÇÃO BÁSICA

MADUREZ EN CIBERSEGURIDAD EN UNA RED DE ESCUELAS DE EDUCACIÓN BÁSICA

https://doi.org/10.56238/sevened2026.011-036

Flávio Medeiros Mariz[1], Rosalvo Ermes Streit[2], Hércules Antonio do Prado[3], Ana Paula Bernardi da Silva[4]

ABSTRACT

Educational institutions, due to their handling of sensitive data from employees, students, and their guardians, are susceptible to cyberattacks. In this context, the need for structured cybersecurity practices aligned with governance principles becomes evident. This research aims to analyze the cybersecurity maturity level of a Basic Education School Network. To this end, a quantitative exploratory-descriptive case study was conducted using the National Institute of Standards and Technology's Cybersecurity Framework 2.0, composed of 22 categories and six dimensions operationalized through 106 statements arranged on a five-point Likert scale. For the statistical legitimacy of the dimensions, the Kaiser-Meyer-Olkin criterion for dimensionality, Cronbach's Alpha for reliability, and Pearson's (r) coefficient along with the p-value for validity were employed. Maturity was determined through the Mean, Standard Deviation, and 95% Confidence Interval. As a result, all six dimensions of the framework were positioned at maturity level two out of five, termed Risk-Informed, in which risk management practices are approved by management but may not be established as organizational policy. It is concluded that, although technical measures are in place, cybersecurity governance requires strengthening, particularly in supply chain risk management, to enhance organizational maturity.

Keywords: Cybersecurity. Governance. Basic Education. Maturity.

RESUMO

As instituições de ensino, ao lidarem com dados sensíveis de alunos, responsáveis e funcionários, tornaram-se alvos frequentes de ataques cibernéticos, o que evidencia a necessidade de práticas estruturadas de segurança digital alinhadas à governança. Objetiva-se analisar o nível de maturidade em cibersegurança de uma Rede de Escolas de Educação

[1] Master's degree in Governance, Technology and Innovation. Universidade Católica de Brasília (UCB), Brazil. E-mail: flaviomariz@gmail.com
[2] Dr. in Administration. Universidade Federal do Rio Grande do Sul (UFRGS), Brazil. E-mail: rosalvo.streit@gmail.com
[3] Dr. in Computing. Universidade Federal do Rio Grande do Sul (UFRGS), Brazil. E-mail: prado.hercules@gmail.com
[4] Dr. in Electrical Engineering. Universidade de Brasília (UnB), Brazil. E-mail: anap.bernardi@gmail.com

Básica. Para tanto, procede-se a um estudo de caso, de natureza exploratória-descritiva e abordagem quantitativa, utilizando o Cybersecurity Framework 2.0 do National Institute of Standards and Technology, composto por 22 categorias e seis dimensões, operacionalizado por 106 afirmativas em escala Likert. Para validação estatística empregaram-se os testes Kaiser-Meyer-Olkin, Alfa de Cronbach e coeficiente de Pearson. Observa-se que todas as dimensões posicionam-se no nível dois de maturidade, denominado Informado por Risco, no qual as práticas são reconhecidas pela administração, mas não plenamente institucionalizadas. Conclui-se que, embora haja estrutura técnica estabelecida, a governança da cibersegurança necessita de fortalecimento, especialmente na gestão da cadeia de suprimentos, para evolução do nível de maturidade organizacional.

Palavras-chave: Cibersegurança. Governança. Educação Básica. Maturidade.

RESUMEN

Las instituciones educativas, al manejar datos sensibles de empleados, estudiantes y sus responsables, son susceptibles a ataques cibernéticos, lo que evidencia la necesidad de prácticas estructuradas de ciberseguridad alineadas con principios de gobernanza. En este sentido, esta investigación tiene como objetivo analizar el nivel de madurez en ciberseguridad de una Red de Escuelas de Educación Básica. Para ello, se desarrolló un estudio de caso de naturaleza exploratoria-descriptiva con enfoque cuantitativo, utilizando el Cybersecurity Framework 2.0 del National Institute of Standards and Technology, compuesto por 22 categorías y seis dimensiones, operacionalizadas mediante 106 afirmaciones en escala Likert. Para la legitimidad estadística se emplearon los criterios Kaiser-Meyer-Olkin, Alfa de Cronbach y coeficiente de Pearson. Como resultado, las seis dimensiones del framework se posicionan en el nivel de madurez dos de cinco, denominado Informado por Riesgo, en el que las prácticas son reconocidas por la administración, pero no plenamente institucionalizadas. Se concluye que, aunque existen controles técnicos establecidos, es necesario fortalecer la gobernanza de la ciberseguridad, especialmente en la gestión de riesgos de la cadena de suministro, para elevar el nivel de madurez organizacional.

Palabras clave: Ciberseguridad. Gobernanza. Educación Básica. Madurez.

1 INTRODUCTION

The growing digitalization in the educational environment has brought numerous benefits, but it has also imposed significant challenges, especially in the face of the increase in cyberattacks and the mishandling of sensitive data in educational institutions (Santos et al., 2023). In this context, sensitive data is understood to include the personal information of employees, students and their guardians, as well as their financial histories (Santos; Farias; Nunes, 2024).

The Microsoft report (2024) points out that educational institutions often operate with a combination of old and new systems, while making intensive use of decentralized networks and personal devices, elements that amplify vulnerabilities and make structured cyber risk management difficult.

Thus, the hybrid technological conjuncture composed of legacy systems and recent technologies, combined with the constant exposure of these environments to the internet (Microsoft, 2024), makes sensitive data handled by educational institutions susceptible to cyberattacks (Santos et al., 2023; Microsoft, 2024). This scenario announces the need for digital security-oriented approaches for educational institutions, which is called cybersecurity.

Within the scope of this research, it is understood that "[...] cybersecurity is the set of standards, practices, and processes that make it possible to protect critical systems, particularly important information, and, above all, people from potential cyber risks and threats" (Belli et al., 2023, p. 9).

However, cybersecurity must be contemplated from a broader perspective, the authors Andrade et al. (2024) state that schools have adopted specific security measures, but demand a structured governance model capable of integrating strategy, responsibilities, and institutional supervision mechanisms. Governance establishes principles oriented to the internal and external environment of the institution (Frogeri; Portugal; Guedes, 2022); because it covers the organization in its entirety, as well as the society in which it is inserted. Thus, while cybersecurity refers to the protection of sensitive data, governance establishes the need to contemplate the internal and external environment. Therefore, the alignment between both considers the digital security of the institution and its surroundings, being materialized through structured approaches, called frameworks.

Cybersecurity frameworks have the primary objective of preventing or mitigating attacks, reducing the risk of threats (Purser, 2014), combined with governance principles. In addition, a framework assumes maturity levels, which determine the degree of compliance through pre-established standards, and the measurement of these levels is an action that

guides improvements in the processes and standards adopted (Araujo; Albuquerque Jr.; Passos, 2025).

In view of the above, maturity, expressed by a cybersecurity framework, supports the institution to identify its position in relation to certain levels, aiming at improving digital security, and this measurement includes governance. However, there is a lack of systematic diagnoses about the level of cybersecurity maturity in Basic Education School Networks, especially from the integrated perspective of governance.

In this context, the following research question is formulated: what is the level of cybersecurity maturity of a Network of Basic Education Schools in the light of the Cybersecurity Framework 2.0?

This investigation is justified by the social and institutional relevance of the protection of sensitive data in the educational environment, as well as by the need for diagnoses that support strategic decisions and organizational policies aimed at strengthening cybersecurity governance. Thus, the objective of this study is to analyze the level of cybersecurity maturity of a Network of Basic Education Schools, based on the Cybersecurity Framework 2.0 of the National Institute of Standards and Technology (NIST), through the statistical validation of the indicators and the measurement of the dimensions of the framework, in a specific, measurable and achievable way.

With this intent, this investigation is divided into sections. In addition to this introduction, the following section addresses the context of digital security in the school environment, presents the place of application of this research, as well as the cybersecurity framework adopted for the maturity examination, which includes governance. In sequence, the methodological paths permeated by this investigation are presented, which are followed by the explanation of the results. Finally, the final considerations are announced.

2 THEORETICAL FRAMEWORK

2.1 CYBERSECURITY IN THE EDUCATIONAL CONTEXT

According to Santos, Farias, and Nunes (2024), many institutions deal with sensitive data on a daily basis, such as customers' personal information, financial histories, and employee records. In the educational context, this reality takes on greater complexity, as it involves data from children and adolescents, an especially vulnerable audience in the digital environment. Thus, personal information of students and their guardians becomes even more relevant from the perspective of data protection. When there are no adequate security mechanisms, these records become potential targets for cyberattacks, leaks, and misuse, compromising not only institutional integrity, but also individual rights.

In this sense, Hurel and Lobato (2018) observed that the insertion of technologies in schools occurred, in many cases, without infrastructure planning or adequate training, increasing exposure to digital risks. This finding dialogues with the diagnosis presented by the National Laboratory for Scientific Computing (LNCC, 2024), according to which the Brazilian educational sector is among the most vulnerable to cyberattacks. Such vulnerability, as evidenced, stems from the absence of consistent institutional policies aimed at digital security, indicating that the problem is not restricted to the technical dimension, but involves management and strategic planning failures.

Additionally, the UNESCO report (2023) points out that many Brazilian schools still operate with precarious infrastructure, unstable connections, and the absence of structured data protection policies. This precariousness manifests itself even more intensely in rural and peripheral regions, where technological resources are scarce and the maintenance of digital systems faces structural limitations.

Souza and Brito (2021) corroborate this scenario by warning of institutional risks arising from the absence of clear guidelines and technical fragility, factors that compromise the ability to respond to incidents, such as breaches and data leaks. Therefore, there is convergence between studies regarding the structural fragility of the educational environment in the face of digital threats.

From an economic perspective, Sapiński (2023) demonstrates that the impacts of cyber incidents go beyond the operational sphere. Based on surveys carried out in 2020, the author indicates that the average costs of a data breach reached approximately US$ 3.86 million. In addition, the estimated global cost of losses associated with cyberattacks exceeded $1.5 trillion annually, evidencing the economic and social magnitude of these incidents. These data reinforce that cybersecurity cannot be treated only as a technical issue, but as an essential strategic component for institutional sustainability.

There is convergence between Hurel and Lobato (2018), Souza and Brito (2021), UNESCO (2023) and LNCC (2024) regarding the structural vulnerability of the educational sector, whether due to insufficient technological planning, institutional fragility, precarious infrastructure or absence of consolidated policies. Such a consensus shows that the challenge goes beyond connectivity and requires a systemic approach.

In this sense, the Organization for Economic Cooperation and Development (OECD, 2019) maintains that it is necessary to ensure safe access and adequate digital education, respecting regional and sociocultural specificities.

Therefore, the responsibility for protecting information falls on the institution and its managers, who must adopt structured measures to ensure the integrity and security of data,

preventing unauthorized access and leaks. Considering the risks imputed to students and employees, arising from the handling of sensitive data (Farias; Nunes, 2024), the institutional vulnerability pointed out by the LNCC (2024), the structural precariousness evidenced by UNESCO (2023), the absence of planning highlighted by Hurel and Lobato (2018) and the financial impact indicated by Sapiński (2023), it becomes necessary to treat cybersecurity from a broader and more integrated perspective. In this context, governance emerges as a structuring dimension capable of articulating strategy, institutional responsibility, and risk management.

2.2 ORGANIZATIONAL GOVERNANCE AND CYBERSECURITY

According to Kjaer (2004), the term governance refers to the act of piloting, conducting or drafting rules, indicating a notion of direction and strategic orientation.

Historically, its consolidation in the organizational field is related to the need for regulation resulting from financial scandals that occurred in companies in the United States in the 1980s, when investors began to react against shareholders and managers who conducted organizations in a manner dissonant with institutional and corporate interests (Oliveira; Santos; Pinto, 2023). Thus, governance emerges as a response to the demand for greater control, transparency, and strategic alignment in organizations.

In the contemporary organizational sphere, Frogeri, Portugal, and Guedes (2022) associate governance with structuring principles such as transparency, equity, corporate responsibility, and accountability, operationalized through formal control and supervision mechanisms. Such principles contemplate both the internal and external environment of the institution, showing that governance is not limited to administrative processes, but involves the relationship of the organization with its stakeholders and with society. From this perspective, governance assumes a systemic character, going beyond operational management and incorporating strategic and normative dimensions.

According to Silva et al. (2023), governance has a multidimensional connotation, as it encompasses the organization in its entirety and the social context in which it is inserted, it is observed, however, that although there is consensus in the literature regarding the structuring principles of governance, its incorporation into cybersecurity still occurs gradually in educational institutions. In many cases, practices remain restricted to operational controls, such as access definition and isolated technical measures, without full integration into institutional strategy and high-level decision-making processes. It is in this context that cybersecurity frameworks assume relevance. Purser (2014) states that such frameworks have as their primary objective to prevent or mitigate attacks, reducing the risk of threats.

In addition, Maleh et al. (2021) point out that these instruments aim to increase the protection of organizational assets against cyber threats. However, when articulated with governance, frameworks are no longer merely technical instruments and become strategic tools, capable of integrating policies, responsibilities, risk management and institutional supervision. Thus, the approximation between governance and cybersecurity proves to be fundamental for the consolidation of structured and sustainable practices in the educational environment.

2.3 NIST FRAMEWORK AND MATURITY LEVELS

In this research, the Cybersecurity Framework 2.0 (CSF) stands out, called in Portuguese Cybersecurity Framework, prepared by the National Institute of Standards and Technology (NIST, 2024). The instrument is designed to be used by organizations of different sizes and sectors, including industry, government, academia and non-profit entities. Its proposal consists of offering structured guidelines for identifying, managing and mitigating cyber risks, integrating technical and strategic dimensions.

CSF 2.0 is structured in six functions, also called dimensions: identify, protect, detect, respond, recover, and governance. The first five functions make up the operational cycle of risk management, while governance assumes a transversal character, guiding the other dimensions. According to NIST (2024), the governance dimension involves understanding the organizational context, establishing the cybersecurity strategy, managing supply chain risks, defining roles, responsibilities, and authorities, as well as supervising institutional policies. The identify dimension establishes that the organization's cybersecurity risks must be understood in a systemic way, including the analysis of assets, vulnerabilities, and threats. In addition, it provides for the identification of improvement opportunities for policies, plans, and processes that underpin risk management (NIST, 2024).

The protect dimension prioritizes the implementation of security measures aimed at mitigating previously identified risks, including access control and restricting users to appropriate levels of authorization, as discussed by Abouelmehdi et al. (2017) and Santana (2021). The detect dimension, on the other hand, presupposes that possible attacks and compromises must be found and analyzed in a timely manner (NIST, 2024). In the logical sequence of the framework, the respond dimension establishes the taking of measures in the face of previously detected incidents, including containment, analysis, mitigation, reporting, and institutional communication actions (NIST, 2024).

Finally, the recover dimension determines that affected assets and operations are restored in a structured manner, allowing the reestablishment of activities and the reduction

of impacts resulting from the incident. Thus, it is observed that CSF 2.0 is not limited to technical controls, but organizes a continuous cycle of risk management guided by governance. With regard to maturity levels, CSF 2.0 (NIST, 2024) establishes four evolutionary stages: Level 1 – Partial (Partial); Level 2 – Risk-Informed; Level 3 – Repeatable; and Level 4 – Adaptive. Maturity, in this context, is associated with the degree of institutionalization of risk management practices and their integration into organizational processes.

According to Araujo, Albuquerque Jr. and Passos (2025, p. 4), "maturity is the degree of compliance of a process in relation to standards of excellence, which makes it important to measure it to guide the improvement of organizational practices." This definition shows that the measurement of maturity is not a merely classificatory exercise, but a guiding instrument for institutional improvement, although the CSF 2.0 is widely recognized as an international reference, it is observed that its empirical application in Networks of Basic Education Schools is still little explored in the national literature, especially from the perspective of the structured measurement of maturity associated with governance.

2.4 THEORETICAL GAP AND RESEARCH DIRECTION

In light of the above, considering the importance of governance and maturity in cybersecurity, combined with the need to confront attacks directed at sensitive data (Farias; Nunes, 2024), this research situates the analysis of maturity within the scope of Educational Institutions. As previously discussed, these institutions have structural and organizational weaknesses (LNCC, 2024; UNESCO, 2023), as well as potentially significant financial impacts from cyber incidents (Sapiński, 2023).

This scenario shows that cybersecurity, when dissociated from a strategic and governance perspective, tends to remain restricted to isolated operational measures. Although the national and international literature broadly addresses topics such as data protection, cybersecurity frameworks, and organizational governance principles, it is observed that the intersection between these elements is still little explored from the perspective of systematic measurement of maturity in educational contexts. In particular, there is a lack of empirical studies applied to Brazilian Basic Education Networks that use the Cybersecurity Framework 2.0 as a structuring instrument of evaluation, integrating governance and risk management in a consolidated analysis.

Thus, a gap in the literature is identified regarding the structured measurement of the level of cybersecurity maturity in educational organizations with multiple administrative units, whose operational complexity requires strategic coordination and institutional alignment. The

absence of systematic diagnoses makes it difficult to plan corrective actions and strengthen institutional digital security policies, especially in networks with wide territorial dispersion.

Therefore, the locus of this research is a Network of Basic Education Schools composed of 98 units distributed in the national territory. The choice of this context is justified by the need to understand how governance and risk management practices manifest themselves in broad and decentralized educational structures. By directing the analysis to this specific environment, it seeks to contribute to filling the identified gap, offering theoretical and empirical subsidies that guide the institutional improvement of cybersecurity maturity.

3 METHODOLOGY

3.1 RESEARCH DESIGN

Regarding the typification of this investigation, it is a Case Study (Yin, 2014), with an exploratory-descriptive nature and a quantitative approach. In the search to increase the experience about cybersecurity maturity (exploratory), which must be carried out rigorously in the presentation of findings (descriptive), it is clear that "[...] exploratory research makes precise descriptions of the situation and wants to discover the relationships between its elements and components" (Bervian; Deer; Silva, 2002, p. 63).

Nevertheless, it is quantitative due to the use of mathematical methods to allow the observation of the phenomenon in a neutral way (Minayo, 1998), enabling the objective measurement of the indicators and the systematic analysis of the identified maturity levels.

This approach favors the analytical consistency of the results, by allowing the statistical treatment of the variables and the reasoned interpretation of the data collected, in line with the purpose of evaluating, in a structured way, the maturity in cybersecurity in the context investigated.

3.2 LOCUS, POPULATION AND SAMPLE

The locus of the research is a Network of Basic Education Schools. The population consisted of 139 employees working in the area of Information Technology, considering that these professionals play a central role in the management, maintenance and protection of institutional systems. The estimated sample consisted of 103 respondents, according to the sample size calculation based on the parameters N = 139, Zα = 1.96 (95% confidence), and = 0.05, p = 0.5 and q = 0.5 (Miot, 2011).

The adoption of these parameters aimed to ensure an adequate level of statistical precision and representativeness of the data collected. Along with the questionnaire, created through Google Forms, the Informed Consent Form (ICF) was made available, and its reading

is mandatory for the continuity of the answers. This procedure ensured that the participants were duly informed about the objectives of the research, the voluntary nature of the participation and the confidentiality of the information provided.

3.3 DATA COLLECTION INSTRUMENT

The methodological procedures of this investigation were operationalized in three stages: i) data collection; ii) legitimization of indicators; and iii) maturity analysis. The first stage consisted of applying the questionnaire based on the Cybersecurity Framework 2.0 (CSF 2.0) of the National Institute of Standards and Technology (NIST, 2024), a structured instrument for evaluating practices related to cybersecurity risk management.

The questionnaire is composed of 106 statements, organized into 22 categories, which are distributed in six functions (dimensions): governance, identify, protect, detect, respond and recover. This organization allows for a systematic examination of the different components of the framework, covering both strategic and operational aspects of cybersecurity. The statements were presented on a five-point Likert scale, with the anchors strongly disagree, neutral and totally agree. This structure makes it possible to measure the degree of adherence of institutional practices to the parameters established by the CSF 2.0, allowing subsequent statistical treatment of the responses.

3.4 STATISTICAL VALIDATION OF INDICATORS

After data collection, the indicators (ii) were legitimized, a stage aimed at the statistical validation of the concepts adopted in the instrument (Hair et al., 2009). In this process, the 106 statements in the questionnaire were treated as observable variables, while the 22 categories and six functions of the CSF 2.0 were considered analytical constructs. This distinction allowed the analysis to be structured in a way that was coherent with the theoretical organization of the framework. To this end, subsets of variables were grouped into representative blocks of each category or dimension of the instrument, ensuring correspondence between the items of the questionnaire and the constructs evaluated (Hair et al., 2009).

Initially, the presence of outliers was verified, in order to avoid distortions in the subsequent analyses. Next, the analysis of dimensionality, reliability and validity of the indicators was performed. Dimensionality was examined using the Kaiser-Meyer-Olkin (KMO) criterion, adopting a minimum value of 0.50 for each category and dimension (Damásio, 2012). Reliability was measured using Cronbach's alpha (CA), and a value higher than 0.60 was considered adequate (Hair et al., 2009).

Validity was assessed using Pearson's coefficient (r), with a positive correlation between the variables and a p-value lower than 0.05 (Formiga et al., 2018). The simultaneous fulfillment of these parameters ensures internal consistency, statistical adequacy and robustness to the indicators used in the analysis.

3.5 MATURITY ANALYSIS

In the third stage (iii), the maturity of the categories and dimensions evaluated was analyzed. To this end, measures of central tendency (Mean), measure of dispersion (Standard Deviation) and the 95% Confidence Interval were used, allowing to examine not only the mean positioning of the responses, but also the stability and variability of the results obtained. NIST (2024) establishes four maturity levels: Level 1 – Partial (Partial); Level 2 – Risk-Informed; Level 3 – Repeatable; and Level 4 – Adaptive. These levels express progressive stages of institutionalization of cybersecurity risk management practices.

Based on this structure, Bernardo (2024) and Bernardo, Malta and Magalhães (2025) associated the following mean intervals to the levels: ≤ 2.99; ≤ 3.99; ≤ 4.99; and = 5.00, respectively, adding the value ≤ 1.99 as level zero, called "very poor". Thus, this research adopts such parameters, incorporating Level 0: Non-existent, in order to contemplate situations of absence or extreme fragility of the practices evaluated.

In view of the results obtained by category and dimension, the general level of maturity of the Network's Educational Institutions was determined by the lowest level identified among the functions of the CSF 2.0, considering the systemic character of the framework and the need for integration between its dimensions. This criterion is based on the understanding that organizational maturity cannot be higher than its most fragile dimension, since functions must act in an articulated manner.

For the dimensions that presented a lower level of maturity, actions were outlined to increase them, in line with the guidelines established by NIST (2025). The statistical treatment of the data was carried out using the RStudio software, version 2021.09.2 Build 382, enabling the execution of the analyses in a structured and reproducible way.

4 RESULTS AND DISCUSSIONS

Data collection was carried out between 01/20 and 01/23/2026, totaling 118 valid responses. No outliers were identified, according to the criteria established by Hair et al. (2009), which reinforces the consistency of the database analyzed. Thus, the final sample of 118 respondents exceeds the initial estimate of 103 participants, calculated according to the parameters presented by Miot (2011), ensuring adequate statistical margin and greater

robustness to the results obtained. The sample profile of the respondents is presented in Table 1.

Table 1

Profile of the sample of 118 respondents

Aspect	Feature	N.	∑	%	∑%
Age	Between 19 and 29 years old	12	12	10,17	10,17
	Between 30 and 39 years old	52	64	44,07	54,23
	Between 40 and 49 years old	41	105	34,75	88,99
	Between 50 and 65 years old	13	118	11,02	100,00
Gender	Women	15	15	12,71	12,71
	Male	103	118	87,29	100,00
Education	Elementary School	0	0	0,00	0,00
	High School	2	2	1,69	1,69
	Higher Education (Undergraduate)	44	46	37,29	38,98
	Post-Graduation (Specialization)	64	110	54,24	93,22
	Postgraduate (Master's Degree)	8	118	6,78	100,00
	Postgraduate (Doctorate)	0	118	0,00	100,00
	Post-Doctorate	0	118	0,00	100,00
He has an academic background in the area of Technology	No	29	29	24,58	24,58
	Yes	89	118	75,42	100,00
Experienced some kind of digital security incident	No	84	84	71,19	71,19
	Yes	34	118	28,81	100,00
Time (years) of experience in the area of Information Technology	Less than 1 year	13	13	11,02	11,01
	Between 1 and 9 years	30	43	25,42	36,44
	Between 10 and 19 years old	49	92	41,53	77,97
	Between 20 and 29 years old	21	113	17,80	95,77
	Between 30 and 35 years old	5	118	4,24	100,00

Legend: N.: Number (quantitative); ∑: Summation; %: Percentage; ∑%: Sum of the Percentage.
Source: Survey data (2026)

It is observed that most respondents are over 30 years old (89.83%), which indicates consolidated professional maturity. In terms of academic background, 98.31% have completed higher education or post-graduation, demonstrating high intellectual capital in the group analyzed. It is also noteworthy that 75.42% have training in the area of Information Technology, which reinforces the technical adherence of the responses to the dimensions evaluated in the CSF 2.0 instrument.

As for the time of experience in the area of Information Technology, it is verified that 65.57% have more than ten years of experience, indicating consolidated professional trajectory and familiarity with technological management practices. The male predominance (87.29%) reflects a characteristic that is still recurrent in the technology sector, without prejudice to the validity of the analysis, since the selection criterion was linked to the function performed and not to demoFigureic characteristics.

When asked about the occurrence of digital security incidents in the personal sphere, 71.19% stated that they had not experienced such events, while 28.81% reported

occurrence. This distribution may be associated with the level of technical training and professional experience of the respondents, factors that tend to favor greater capacity for prevention, identification and mitigation of cyber risks.

The data presented show that the sample is composed of professionals with consolidated experience, high training and direct work in the technological area, which gives legitimacy to the perceptions expressed about the cybersecurity maturity of the analyzed Network. In addition, considering that the participants are distributed in the different Units of the Network – in their private and social purposes – the answers tend to broadly reflect the organizational context investigated.

Based on the characterization of the sample, the statistical legitimation of the indicators was carried out, considering the criteria of dimensionality, reliability and validity (Hair et al., 2009), operationalized through Chart 1 (Appendix A). The Kaiser-Meyer-Olkin index showed values not lower than 0.50 (Damásio, 2012), Cronbach's alpha exceeded the minimum limit recommended in the literature (Hair et al., 2009) and the Pearson coefficient (r) showed positive correlations with p-value lower than 0.05 (Formiga et al., 2018). These results confirm the statistical adequacy of the instrument applied and support the reliability of subsequent analyses.

After the validation stage, maturity was analyzed using the Mean, Standard Deviation, and 95% Confidence Interval measures of the dimensions and categories of the CSF 2.0 (NIST, 2024), as shown in Table 2.

Table 2

Mean, Standard Deviation and 95% Confidence Interval of the dimensions and categories of the Cybersecurity Framework (CSF 2.0)

Dimension | Category	Average	D.P.	I.C. 95%
GOVERNANCE (GV)	3,86	0,93	[3,70; 4,03]
Organizational Context (GV.OC)	3,99	0,86	[3,84; 4,15]
Risk Management Strategy (GV.RM)	3,85	0,92	[3,69; 4,02]
Roles, Responsibilities and Authorities (GV. RR)	3,84	1,01	[3,66; 4,02]
Politics (GV. PO)	3,89	0,93	[3,72; 4,06]
Supervision (GV. OV)	3,99	0,85	[3,84; 4,15]
Cybersecurity Risk Management in the Supply Chain (GV. SC)	3,77	0,95	[3,60; 3,95]
IDENTIFY (ID)	4,08	0,88	[3,92; 4,23]
Asset Management (ID.AM)	3,99	0,90	[3,83; 4,15]
Risk Assessment (ID.RA)	4,13	0,86	[3,98; 4,29]
Improvement (ID.IM)	4,09	0,88	[3,93; 4,25]
PROTECT (PR)	4,12	0,86	[3,97; 4,28]
Identity Management, Authentication and Access Control (PR. AA)	4,27	0,80	[4,13; 4,42]
Awareness and Training (PR. AT)	3,95	0,91	[3,79; 4,12]
Data Security (PR.DS)	4,22	0,80	[4,07; 4,36]
Platform Security (PR.PS)	4,04	0,87	[3,88; 4,19]
Resilience of Technological Infrastructure (PR. IR)	4,02	0,90	[3,86; 4,18]
DETECT (DE)	4,05	0,91	[3,88; 4,21]

Continuous Monitoring (DE. CM)	4,12	0,89	[3,96; 4,28]
Analysis of Adverse Events (DE. AE)	3,98	0,93	[3,81; 4,15]
REPLY (RS)	4,06	0,88	[3,90; 4,22]
Incident Management (RS. MA)	4,08	0,89	[3,92; 4,24]
Incident Analysis (RS. AN)	4,08	0,90	[3,92; 4,24]
Incident Response (RS.CO) Reporting and Communication	3,99	0,81	[3,84; 4,13]
Incident Mitigation (RS.MI)	4,06	0,88	[3,90; 4,22]
RETRIEVE (RC)	4,05	0,84	[3,90; 4,20]
Execution of the Incident Recovery Plan (RC. RP)	4,08	0,83	[3,93; 4,23]
Incident Recovery Communication (RC.CO)	3,94	0,86	[3,78; 4,10]
Legend: D.P.: Standard Deviation; I.C.: Confidence Interval			

Source: Survey data (2026)

The Cybersecurity Risk Management in the Supply Chain (GV. SC), belonging to the Governance (GV) dimension, has the lowest average (3.77) among all the categories of the CSF 2.0. According to NIST (2024), contemporary technological environments depend on interconnected supply chains, which involve suppliers, developers, system integrators, and external service providers responsible for sustaining technology products and services. Because these interactions are shaped and influenced by technological resources, it is essential to systematically manage the risks associated with this chain.

In the opposite direction, the category Identity Management, Authentication and Access Control (PR. AA), linked to the Protect (PR) dimension, has the highest average (4.27) among the categories analyzed. Authentication aims to verify the identity of users, while access control restricts permissions according to functional attributions (Abouelmehdi et al., 2017).

Santana (2021) points out that the expansion of access control to integrated identity management is a central element in protecting against improper access and unauthorized use of sensitive information. Therefore, a relevant asymmetry is observed between the dimensions analyzed. While respondents perceive a high level of internal protection, associated with authentication and identity control mechanisms, they identify lower maturity in the management of risks related to the supply chain. This difference indicates that internal controls are more consolidated than mechanisms aimed at supervising and prioritizing risks from suppliers and external agents.

Such a scenario suggests that the instituted control is partially comprehensive. When external risk management does not keep pace with the level of internal protection, the organization remains vulnerable to incidents originating outside its direct operational boundaries.

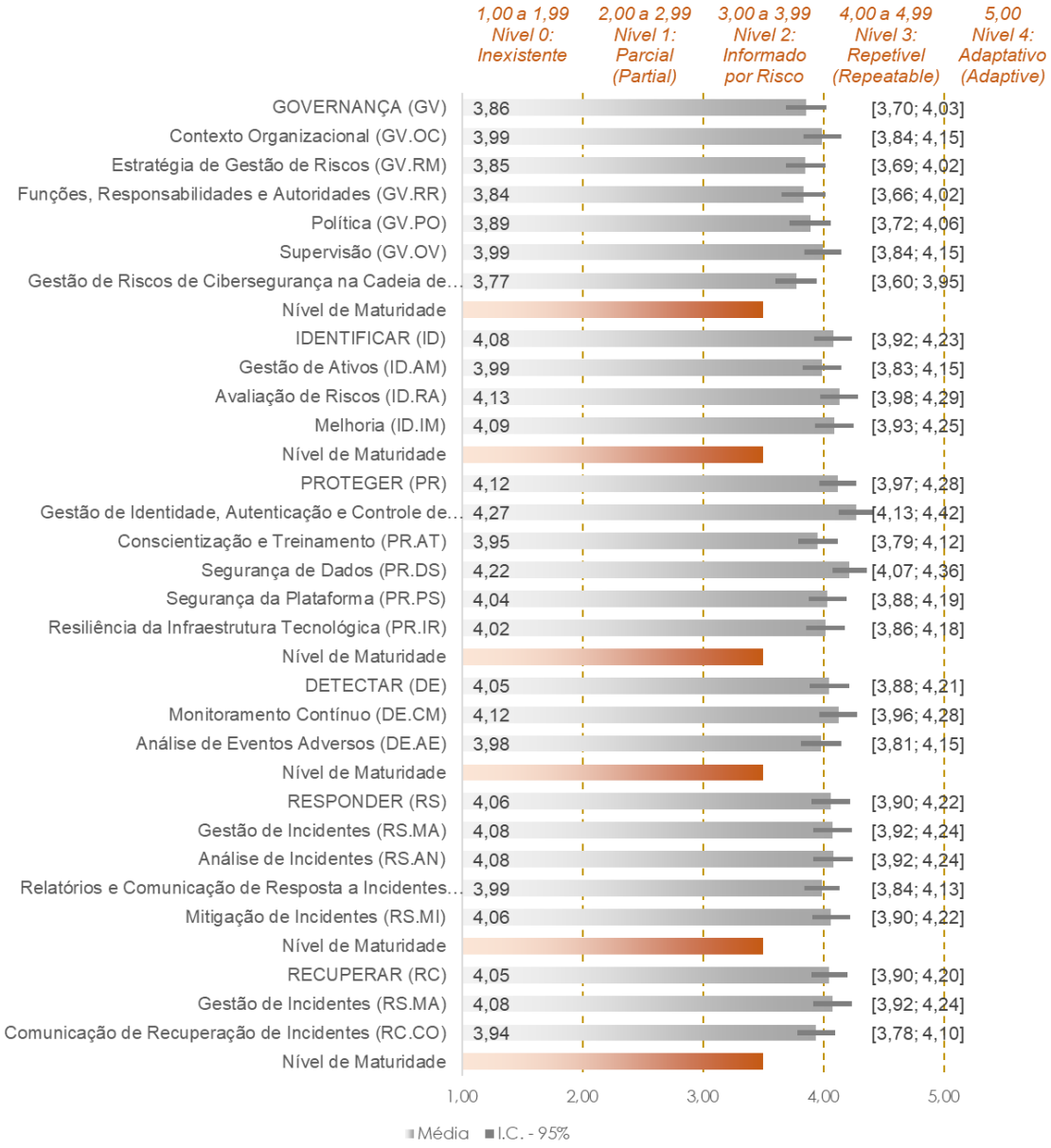
Considering that the supply chain is composed of multiple interdependent actors (NIST, 2024), weaknesses in this domain can compromise the coherence and effectiveness of the global cybersecurity strategy.

Statistical analysis reinforces this interpretation. The confidence interval of the GV category. SC is between 3.60 and 3.95, while the PR category. AA is between 4.13 and 4.42. As there is no overlap between the intervals, the difference observed reveals statistical consistency between the categories analyzed. This evidence strengthens the understanding that maturity in internal protection outweighs maturity in supply chain governance.

These distinctions, presented in Table 2, are complemented by the analysis of the maturity levels of the categories and dimensions of the CSF 2.0, as represented in Figure 1.

Figure 1

Maturity levels of the Cybersecurity Framework



Source: Survey data (2026)

Thus, the Protect (RP) dimension proves to be a relevant aspect for the Institution; however, it is not fully articulated in the context of Governance (GV), since both represent extremes in the cybersecurity spectrum, with averages of 4.12 and 3.86, respectively. Considering that Governance comprises the analysis of the organizational context, the definition of the cybersecurity strategy and the management of Supply Chain risks, as well as the delimitation of roles, responsibilities and authorities (NIST, 2024), it is urgent to examine cybersecurity from a systemic perspective of Governance, as opposed to a restricted and predominantly operational approach centered on the Protect dimension. all dimensions of CSF 2.0 (NIST, 2024) are at Level 2 of maturity, characterized as risk-informed management.

At this stage, risk management practices are recognized and approved by management, but may not yet be formally institutionalized as consolidated organizational policies. Such a scenario indicates the need to strengthen Governance, as it is this dimension that guides the prioritization and integration of other functions in the context of the institutional mission and the expectations of stakeholders (NIST, 2024).

Considering that cybersecurity risks, such as the violation of sensitive data, involve student and staff information (Farias; Nunes, 2024), as well as external agents linked to the Supply Chain, Governance assumes a central role by covering the institution's internal and external environments. This perspective dialogues with the principles of transparency, equity, corporate responsibility and accountability, supported by control mechanisms (Frogeri; Portugal; Guedes, 2022). In this sense, the consolidation of maturity requires integration of all dimensions under the aegis of Governance (NIST, 2024).

For the evolution of the maturity level, it is noteworthy that the Governance (GV) dimension has the lowest average among the dimensions analyzed, totaling 3.86 points (Figure 1). Within this dimension, the Cybersecurity Risk Management in the Supply Chain (GV. SC) registers a mean of 3.77 points and a confidence interval of 95% between 3.60 and 3.95. As it is entirely at Level 2, this category is the most critical in the scope of Governance.

Among the statements in the questionnaire associated with the GV. SC, GV stands out. SC-04: "Suppliers are known and prioritized by criticality" (NIST, 2024, p. 17), whose average was 3.61, the lowest among the statements in this category. This result contributes to the reduction of the global average of GV. SC and suggests a tendency towards a reactive posture, since the value is close to the neutral point of the Likert scale adopted.

In view of this scenario, actions are proposed aimed at advancing the level of maturity of the Governance (GV) dimension, especially with regard to the GV category. SC. In this sense, it is recommended:

i) establish formal criteria for the classification of suppliers by criticality, considering the sensitivity of the data processed, the level of access to institutional systems and the strategic relevance of the services provided;
ii) maintain an updated register of suppliers, prioritizing them according to previously defined criteria (NIST, 2025).

According to NIST (2024), the Supply Chain is a critical area in cybersecurity risk management, as the systems and networks that support the organizational mission involve multiple interdependent actors. The vulnerability in this chain becomes significant precisely because of the technological interconnection between internal and external agents.

In the context of the Network of Basic Education Schools analyzed, composed of 98 units distributed in the national territory, the structured management of this chain is even more necessary. However, as evidenced in the previous analyses from the perspective of the respondents, the prioritization of suppliers by criticality is not yet consolidated (GV. SC-04). The implementation of the proposed actions may contribute to mitigating risks, promoting a proactive posture, and reducing vulnerabilities associated with the chain, not only from the financial perspective of cyber incidents (Sapiński, 2023), but also from a strategic and institutional perspective.

5 CONCLUSION

This research aimed to analyze the level of cybersecurity maturity of a Network of Basic Education Schools. Based on a sample of 118 respondents, an overall maturity level of two was identified, on a five-level scale adopted in this investigation, classified as Risk-Informed. At this stage, risk management practices are recognized by management, although they are not yet fully institutionalized as a formal organizational policy. Such framing was observed in the dimensions identify, protect, detect, respond and recover, as well as in governance, which guides and integrates the other functions of the framework.

The results indicate that, despite the high level of academic training of the respondents (98.31%) and the predominance of work in the area of Information Technology (75.42%), technical qualification does not automatically translate into consolidated maturity in cybersecurity governance. The latter presupposes strategic articulation, clear definition of responsibilities and organizational integration, going beyond the strictly operational domain.

It was found that the Protect dimension presented the highest performance, especially in the Identity Management, Authentication and Access Control category. However, the lower maturity identified in Cybersecurity Risk Management in the Supply Chain, linked to the

Governance dimension, shows relevant structural fragility. Such asymmetry demonstrates that internal technical controls, when not accompanied by strategic management of external actors, can compromise the consistency of the adopted security model.

In educational organizations, the eventual_attachência of incidents involving sensitive data of students, guardians, and employees can generate significant financial, legal, and reputational impacts. In this context, preventive action, supported by governance practices, proves to be more effective than merely reactive interventions.

In light of the findings, it is recommended to strengthen cybersecurity governance, with an emphasis on the classification of suppliers by criticality, considering the sensitivity of the data processed, the level of access granted, and the strategic relevance of the services provided, as well as the maintenance of updated records that allow structured prioritization of these partners.

It is expected that this research will contribute, at the empirical level, to the improvement of the cybersecurity practices of the analyzed Network. In the academic sphere, it is suggested that the study be replicated in other Basic Education Networks, in order to broaden the comparative base and deepen the debate on cybersecurity maturity in the Brazilian educational context.

REFERENCES

Abouelmehdi, K., et al. (2017). Big data security and privacy in healthcare: A review. Journal of Big Data, 113, 73–80.

Andrade, D., et al. (2024). Information security management in a higher education institution based on standards, legal basis for the optimization of administrative resources. Journal of Ecohumanism, 3(8), 1–14.

Araujo, M. S., Albuquerque Jr., A. E., & Passos, F. U. (2025). Modelos de maturidade em gestão da segurança da informação: Análise comparativa na perspectiva da administração pública federal brasileira. Cuadernos de Educación y Desarrollo, 17(5), Article e8480. https://ojs.cuadernoseducacion.com/ojs/index.php/ced/article/view/8480

Belli, L., et al. (2023). Cibersegurança: Uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. FGV Direito Rio.

Bernardo, L. A. (2024). Assessing and strengthening cybersecurity maturity: A NIST-based index approach [Dissertação de mestrado, Instituto Politécnico de Viana do Castelo]. http://repositorio.ipvc.pt/bitstream/20.500.11960/3989/1/Luis_Bernardo.pdf

Bernardo, L. A., Malta, S., & Magalhães, J. (2025). An evaluation framework for cybersecurity maturity aligned with the NIST CSF. Electronics, 14(7).

Bervian, P. A., Cervo, A. L., & Silva, R. (2002). Metodologia científica. Pretence Hall.

Damásio, B. F. (2012). Uso da análise fatorial exploratória em psicologia. Avaliação Psicológica, 11(2), 213–227.

Formiga, N. S., et al. (2018). Evidência da invariância fatorial e validade convergente da escala de suporte organizacional: Estudo com trabalhadores brasileiros. Boletim-Academia Paulista de Psicologia, 38(94), 27–35.

Frogeri, R. F., Portugal, N. S., & Guedes, L. C. V. (2022). O conceito de governança e a governança corporativa. Textos para Discussão, 1(1), 836–850. https://ojs.periodicos.unis.edu.br/textosparadiscussao/article/view/661

Hair, J. F., et al. (2009). Análise multivariada de dados (6ª ed.). Bookman.

Hurel, L. M., & Lobato, L. (2018). Governança da segurança cibernética: Dinâmicas entre setor público e privado no Brasil. Cadernos Adenauer, 19(3), 135–156.

Kjaer, A. M. (2004). Governance (1ª ed.). Polity Press.

Laboratório Nacional de Computação Científica. (2024). A importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos. https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/a-importancia-de-uma-gestao-eficaz-da-seguranca-da-informacao-e-da-conformidade-com-os-requisitos

Maleh, Y., et al. (2021). IT governance and information security: Guides, standards, and frameworks. CRC Press.

Microsoft. (2021, 20 de outubro). Como os ataques cibernéticos estão mudando, de acordo com o novo Relatório de Defesa Digital da Microsoft. https://news.microsoft.com/pt-br/como-os-ataques-ciberneticos-estao-mudando-de-acordo-com-o-novo-relatorio-de-defesa-digital-da-microsoft/

Minayo, M. C. S. (1998). O desafio do conhecimento: Pesquisa qualitativa em saúde (5ª ed.). Hucitec.

Miot, H. A. (2011). Tamanho da amostra em estudos clínicos e experimentais. Jornal Vascular Brasileiro, 10(4), 275–278. https://doi.org/10.1590/S1677-54492011000400001

National Institute of Standards and Technology. (2025). CSF 2.0 implementation examples. https://www.nist.gov/document/csf-20-implementation-examples-xlsx

National Institute of Standards and Technology. (2024). Cybersecurity Framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

Organização para a Cooperação e Desenvolvimento Econômico. (2019). The concept of safety and security education in the context of global education reform.

Oliveira, J. G. L., Santos, J. A., & Pinto, I. M. B. S. (2023). Análise da governança de TI em uma prefeitura do Nordeste do Brasil. Revista Brasileira de Administração Científica, 14(4), 76–87.

Purser, S. (2014). Standards for cyber security. In M. E. Hathaway (Ed.), Best practices in computer network defense: Incident detection and response (pp. 97–106). IOS Press.

Santana, F. J. C. (2021). A segurança da informação na ciência da informação no Brasil [Dissertação de mestrado, Universidade Federal da Bahia].

Santos, D. S., et al. (2023). Tecnologias, cidadania e educação: Estratégias para lidar com os riscos das práticas digitais nas instituições escolares. Revista Amor Mundi, 4(7), 11–22.

Santos, R., Farias, R. M., & Nunes, L. A. (2024). What is the future of Brazil's cybersecurity governance? Cadernos Gestão Pública e Cidadania, 29, 1–21.

Sapiński, A. (2023). The importance and challenges of information security in the digital age: Analysis of the current situation and prospects for development. ASEJ: Scientific Journal of Bielsko-Biala School of Finance and Law, 7(1), 52.

Silva, K., et al. (2023). Conceitos de governança aplicados na governança universitária: Uma revisão sistemática. Revista de Gestão e Secretariado, 14(4), 6113–6131.

Souza, F. M., & Brito, R. P. (2021). Governança da informação na educação pública: Riscos e vulnerabilidades frente à LGPD. Revista de Administração Pública e Gestão Social, 13(1), 87–102. https://doi.org/10.21118/rbpgs.v13i1.1234

Organização das Nações Unidas para a Educação, a Ciência e a Cultura. (2023). Review of progress in the basic education sector to 2024. https://sol.sbc.org.br/index.php/wei/article/view/24932/24753

Yin, R. K. (2014). Estudo de caso: Planejamento e métodos (5ª ed.). Bookman.

ANNEXES

Table 1

Statistics of legitimation of indicators

Categoria da Dimensão	KMO	AC	Seq Afirm	r de Pearson										p-Valor									
				[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
Dimensão (função) GOVERNANÇA (GV)																							
Contexto Organizacional (GV.OC)	0,79	0,88	[1] 1	1,00	0,66	0,55	0,61	0,46						0,00	0,00	0,00	0,00	0,00					
			[2] 2	0,66	1,00	0,75	0,59	0,57						0,00	0,00	0,00	0,00	0,00					
			[3] 3	0,55	0,75	1,00	0,57	0,48						0,00	0,00	0,00	0,00	0,00					
			[4] 4	0,61	0,59	0,57	1,00	0,69						0,00	0,00	0,00	0,00	0,00					
			[5] 5	0,46	0,57	0,48	0,69	1,00						0,00	0,00	0,00	0,00	0,00					
Estratégia de Gestão de Riscos (GV.RM)	0,89	0,92	[1] 6	1,00	0,67	0,64	0,58	0,43	0,51	0,45				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[2] 7	0,67	1,00	0,61	0,68	0,58	0,65	0,65				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[3] 8	0,64	0,61	1,00	0,60	0,54	0,53	0,57				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[4] 9	0,58	0,68	0,60	1,00	0,71	0,73	0,70				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[5] 10	0,43	0,58	0,54	0,71	1,00	0,74	0,60				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[6] 11	0,51	0,65	0,53	0,73	0,74	1,00	0,70				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[7] 12	0,45	0,65	0,57	0,70	0,60	0,70	1,00				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
Funções, Responsabilidades e Autoridades (GV.RR)	0,74	0,84	[1] 13	1,00	0,69	0,63	0,51							0,00	0,00	0,00	0,00						
			[2] 14	0,69	1,00	0,70	0,39							0,00	0,00	0,00	0,00						
			[3] 15	0,63	0,70	1,00	0,58							0,00	0,00	0,00	0,00						
			[4] 16	0,51	0,39	0,58	1,00							0,00	0,00	0,00	0,00						
Política (GV.PO)	0,51	0,82	[1] 17	1,00	0,69									0,00	0,00								
			[2] 18	0,69	1,00									0,00	0,00								
Supervisão (GV.OV)	0,76	0,92	[1] 19	1,00	0,81	0,81								0,00	0,00	0,00							
			[2] 20	0,81	1,00	0,77								0,00	0,00	0,00							
			[3] 21	0,81	0,77	1,00								0,00	0,00	0,00							
Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (GV.SC)	0,93	0,96	[1] 22	1,00	0,75	0,77	0,68	0,68	0,59	0,72	0,65	0,75	0,69	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[2] 23	0,75	1,00	0,72	0,69	0,69	0,63	0,63	0,63	0,71	0,61	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[3] 24	0,77	0,72	1,00	0,73	0,78	0,67	0,74	0,67	0,74	0,74	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[4] 25	0,68	0,69	0,73	1,00	0,78	0,61	0,67	0,70	0,74	0,60	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[5] 26	0,68	0,69	0,78	0,78	1,00	0,64	0,62	0,67	0,72	0,69	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[6] 27	0,59	0,63	0,67	0,61	0,64	1,00	0,73	0,72	0,64	0,63	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[7] 28	0,72	0,63	0,74	0,67	0,62	0,73	1,00	0,82	0,77	0,74	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[8] 29	0,65	0,63	0,67	0,70	0,67	0,72	0,82	1,00	0,74	0,71	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[9] 30	0,75	0,71	0,74	0,74	0,72	0,64	0,77	0,74	1,00	0,79	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[10] 31	0,69	0,61	0,74	0,60	0,69	0,63	0,74	0,71	0,79	1,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Dimensão (função) IDENTIFICAR (ID)																							
Gestão de Ativos (ID.AM)	0,92	0,94	[1] 32	1,00	0,74	0,67	0,57	0,58	0,60	0,69				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[2] 33	0,74	1,00	0,78	0,65	0,65	0,72	0,65				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[3] 34	0,67	0,78	1,00	0,73	0,68	0,73	0,72				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[4] 35	0,57	0,65	0,73	1,00	0,66	0,72	0,68				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[5] 36	0,58	0,65	0,68	0,66	1,00	0,73	0,69				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[6] 37	0,60	0,72	0,73	0,72	0,73	1,00	0,67				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
			[7] 38	0,69	0,65	0,72	0,68	0,69	0,67	1,00				0,00	0,00	0,00	0,00	0,00	0,00	0,00			
Avaliação de Riscos (ID.RA)	0,92	0,96	[1] 39	1,00	0,72	0,73	0,79	0,62	0,72	0,69	0,67	0,73	0,64	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[2] 40	0,72	1,00	0,78	0,77	0,72	0,72	0,69	0,70	0,62	0,59	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[3] 41	0,73	0,78	1,00	0,82	0,80	0,76	0,69	0,72	0,66	0,56	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[4] 42	0,79	0,77	0,82	1,00	0,76	0,71	0,64	0,70	0,67	0,61	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[5] 43	0,62	0,72	0,80	0,76	1,00	0,71	0,70	0,72	0,56	0,62	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[6] 44	0,72	0,72	0,76	0,71	0,71	1,00	0,81	0,75	0,66	0,57	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[7] 45	0,69	0,69	0,69	0,64	0,70	0,81	1,00	0,78	0,68	0,65	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[8] 46	0,67	0,70	0,72	0,70	0,72	0,75	0,78	1,00	0,62	0,66	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[9] 47	0,73	0,62	0,66	0,67	0,56	0,66	0,68	0,62	1,00	0,77	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
			[10] 48	0,64	0,59	0,56	0,61	0,62	0,57	0,65	0,66	0,77	1,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Melhoria (ID.IM)	0,84	0,91	[1] 49	1,00	0,72	0,70	0,70							0,00	0,00	0,00	0,00						
			[2] 50	0,72	1,00	0,77	0,70							0,00	0,00	0,00	0,00						
			[3] 51	0,70	0,77	1,00	0,75							0,00	0,00	0,00	0,00						
			[4] 52	0,70	0,70	0,75	1,00							0,00	0,00	0,00	0,00						
Dimensão (função) PROTEGER (PR)																							
Gestão de Identidade, Autenticação e Controle de Acesso (PR.AA)	0,89	0,93	[1] 53	1,00	0,82	0,75	0,75	0,57	0,63					0,00	0,00	0,00	0,00	0,00	0,00				
			[2] 54	0,82	1,00	0,76	0,81	0,60	0,62					0,00	0,00	0,00	0,00	0,00	0,00				
			[3] 55	0,75	0,76	1,00	0,73	0,63	0,69					0,00	0,00	0,00	0,00	0,00	0,00				
			[4] 56	0,75	0,81	0,73	1,00	0,66	0,59					0,00	0,00	0,00	0,00	0,00	0,00				
			[5] 57	0,57	0,60	0,63	0,66	1,00	0,68					0,00	0,00	0,00	0,00	0,00	0,00				
			[6] 58	0,63	0,62	0,69	0,59	0,68	1,00					0,00	0,00	0,00	0,00	0,00	0,00				
Conscientização e Treinamento (PR.AT)	0,51	0,88	[1] 59	1,00	0,79									0,00	0,00								
			[2] 60	0,79	1,00									0,00	0,00								
Segurança de Dados (PR.DS)	0,81	0,92	[1] 61	1,00	0,76	0,78	0,76							0,00	0,00	0,00	0,00						
			[2] 62	0,76	1,00	0,86	0,70							0,00	0,00	0,00	0,00						
			[3] 63	0,78	0,86	1,00	0,67							0,00	0,00	0,00	0,00						
			[4] 64	0,76	0,70	0,67	1,00							0,00	0,00	0,00	0,00						
Segurança da Plataforma (PR.PS)	0,84	0,89	[1] 65	1,00	0,68	0,54	0,66	0,49	0,50					0,00	0,00	0,00	0,00	0,00	0,00				
			[2] 66	0,68	1,00	0,84	0,58	0,56	0,70					0,00	0,00	0,00	0,00	0,00	0,00				
			[3] 67	0,54	0,84	1,00	0,51	0,52	0,65					0,00	0,00	0,00	0,00	0,00	0,00				
			[4] 68	0,66	0,58	0,51	1,00	0,40	0,41					0,00	0,00	0,00	0,00	0,00	0,00				
			[5] 69	0,49	0,56	0,52	0,40	1,00	0,56					0,00	0,00	0,00	0,00	0,00	0,00				
			[6] 70	0,50	0,70	0,65	0,41	0,56	1,00					0,00	0,00	0,00	0,00	0,00	0,00				
Resiliência da Infraestrutura Tecnológica (PR.IR)	0,78	0,87	[1] 71	1,00	0,46	0,70	0,58							0,00	0,00	0,00	0,00						
			[2] 72	0,46	1,00	0,65	0,72							0,00	0,00	0,00	0,00						
			[3] 73	0,70	0,65	1,00	0,74							0,00	0,00	0,00	0,00						
			[4] 74	0,58	0,72	0,74	1,00							0,00	0,00	0,00	0,00						
Dimensão (função) DETECTAR (DE)																							
Monitoramento Contínuo (DE.CM)	0,87	0,90	[1] 75	1,00	0,71	0,73	0,59	0,63						0,00	0,00	0,00	0,00	0,00					
			[2] 76	0,71	1,00	0,69	0,54	0,66						0,00	0,00	0,00	0,00	0,00					
			[3] 77	0,73	0,69	1,00	0,67	0,66						0,00	0,00	0,00	0,00	0,00					
			[4] 78	0,59	0,54	0,67	1,00	0,62						0,00	0,00	0,00	0,00	0,00					
			[5] 79	0,63	0,66	0,66	0,62	1,00						0,00	0,00	0,00	0,00	0,00					

Análise de Eventos Adversos (DE.AE)	0,88	0,94	[1] 80	1,00	0,78	0,77	0,64	0,69	0,69					0,00	0,00	0,00	0,00	0,00	0,00				
			[2] 81	0,78	1,00	0,80	0,56	0,61	0,61					0,00	0,00	0,00	0,00	0,00	0,00				
			[3] 82	0,77	0,80	1,00	0,76	0,73	0,79					0,00	0,00	0,00	0,00	0,00	0,00				
			[4] 83	0,64	0,56	0,76	1,00	0,79	0,77					0,00	0,00	0,00	0,00	0,00	0,00				
			[5] 84	0,69	0,61	0,73	0,79	1,00	0,79					0,00	0,00	0,00	0,00	0,00	0,00				
			[6] 85	0,69	0,61	0,79	0,77	0,79	1,00					0,00	0,00	0,00	0,00	0,00	0,00				
Dimensão (função) RESPONDER (RS)																							
Gestão de Incidentes (RS.MA)	0,89	0,96	[1] 86	1,00	0,76	0,77	0,80	0,87						0,00	0,00	0,00	0,00	0,00					
			[2] 87	0,76	1,00	0,82	0,83	0,81						0,00	0,00	0,00	0,00	0,00					
			[3] 88	0,77	0,82	1,00	0,85	0,81						0,00	0,00	0,00	0,00	0,00					
			[4] 89	0,80	0,83	0,85	1,00	0,89						0,00	0,00	0,00	0,00	0,00					
			[5] 90	0,87	0,81	0,81	0,89	1,00						0,00	0,00	0,00	0,00	0,00					
Análise de Incidentes (RS.AN)	0,85	0,93	[1] 91	1,00	0,83	0,80	0,71							0,00	0,00	0,00	0,00						
			[2] 92	0,83	1,00	0,87	0,72							0,00	0,00	0,00	0,00						
			[3] 93	0,80	0,87	1,00	0,74							0,00	0,00	0,00	0,00						
			[4] 94	0,71	0,72	0,74	1,00							0,00	0,00	0,00	0,00						
Relatórios e Comunicação de Resposta a Incidentes (RS.CO)	0,51	0,91	[1] 95	1,00	0,83									0,00	0,00								
			[2] 96	0,83	1,00									0,00	0,00								
Mitigação de Incidentes (RS.MI)	0,51	0,83	[1] 97	1,00	0,71									0,00	0,00								
			[2] 98	0,71	1,00									0,00	0,00								
Dimensão (função) RECUPERAR (RC)																							
Execução do Plano de Recuperação de Incidentes (RC.RP)	0,89	0,94	[1] 99	1,00	0,75	0,72	0,60	0,66	0,63					0,00	0,00	0,00	0,00	0,00	0,00				
			[2] 100	0,75	1,00	0,80	0,68	0,76	0,72					0,00	0,00	0,00	0,00	0,00	0,00				
			[3] 101	0,72	0,80	1,00	0,67	0,70	0,76					0,00	0,00	0,00	0,00	0,00	0,00				
			[4] 102	0,60	0,68	0,67	1,00	0,65	0,77					0,00	0,00	0,00	0,00	0,00	0,00				
			[5] 103	0,66	0,76	0,70	0,65	1,00	0,79					0,00	0,00	0,00	0,00	0,00	0,00				
			[6] 104	0,63	0,72	0,76	0,77	0,79	1,00					0,00	0,00	0,00	0,00	0,00	0,00				
Comunicação de Recuperação de Incidentes (RC.CO)	0,51	0,86	[1] 105	1,00	0,76									0,00	0,00								
			[2] 106	0,76	1,00									0,00	0,00								

Legend: KMO: Kaiser-Meyer-Olkin; AC: Cronbach's alpha; Seq Aaffirm: Sequential of the instrument's statements

Source: Survey data (2026)