ReGeo ISSN: 2177-3246

MATURIDADE EM CIBERSEGURANÇA EM UMA REDE DE ESCOLAS DE EDUCAÇÃO BÁSICA

CYBERSECURITY MATURITY IN A BASIC EDUCATION SCHOOL NETWORK

MADUREZ EN CIBERSEGURIDAD EN UNA RED DE ESCUELAS DE EDUCACIÓN BÁSICA

10.56238/revgeov17n2-149

Flávio Medeiros Mariz
Mestre em Governança, Tecnologia e Inovação
Instituição: Universidade Católica de Brasília (UCB)
E-mail: flaviomariz@gmail.com

Rosalvo Ermes Streit
Doutor em Administração
Instituição: Universidade Federal do Rio Grande do Sul (UFRGS)
E-mail: rosalvo.streit@gmail.com

Hércules Antonio do Prado
Doutor em Computação
Instituição: Universidade Federal do Rio Grande do Sul (UFRGS)
E-mail: prado.hercules@gmail.com

Ana Paula Bernardi da Silva
Doutora em Engenharia Elétrica
Instituição: Universidade de Brasília (UnB)
E-mail: anap.bernardi@gmail.com

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 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.

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.

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 INTRODUÇÃO

A crescente digitalização no ambiente educacional trouxe inúmeros benefícios, mas também impôs desafios significativos, sobretudo diante do aumento de ataques cibernéticos e da manipulação indevida de dados sensíveis em instituições de ensino (Santos et al., 2023). Entendem-se como dados sensíveis, nesse contexto, informações pessoais de funcionários, alunos e seus responsáveis, bem como seus históricos financeiros (Santos; Farias; Nunes, 2024).

O relatório da Microsoft (2024) aponta que as instituições educacionais costumam operar com uma combinação de sistemas antigos e novos, ao mesmo tempo em que fazem uso intensivo de redes descentralizadas e de dispositivos pessoais, elementos que ampliam as vulnerabilidades e dificultam a gestão estruturada de riscos cibernéticos.

Assim, a conjuntura tecnológica híbrida composta por sistemas legados e tecnologias recentes aliada à exposição constante desses ambientes à internet (Microsoft, 2024), torna os dados sensíveis manipulados pelas instituições educacionais suscetíveis a ataques cibernéticos (Santos et al., 2023; Microsoft, 2024). Esse cenário anuncia a necessidade de tratativas orientadas à segurança digital das instituições educacionais, sendo essa denominada cibersegurança.

No âmbito desta pesquisa, compreende-se que "[...] a cibersegurança é o conjunto de normas, práticas e processos que permitem proteger sistemas críticos, informações particularmente importantes e, sobretudo, pessoas de potenciais riscos e ameaças cibernéticas" (Belli et al., 2023, p. 9).

Contudo, a cibersegurança deve ser contemplada por uma perspectiva mais ampla, os autores Andrade et al. (2024) afiançam que as escolas têm adotado medidas pontuais de segurança, mas demandam um modelo estruturado de governança capaz de integrar estratégia, responsabilidades e mecanismos de supervisão institucional. A governança estabelece princípios orientados ao ambiente interno e externo da instituição (Frogeri; Portugal; Guedes, 2022); porquanto, abrange a organização em sua totalidade, bem como a sociedade na qual está inserida. Desse modo, enquanto a cibersegurança remete à proteção de dados sensíveis, a governança estabelece a necessidade de contemplar o ambiente interno e externo. Por conseguinte, o alinhamento entre ambas considera a segurança digital da instituição e seu entorno, sendo materializado por meio de abordagens estruturadas, denominadas frameworks.

Frameworks de cibersegurança têm o objetivo primordial de prevenir ou mitigar ataques, reduzindo o risco de ameaças (Purser, 2014), aliados a princípios de governança. Adicionalmente, um framework assume níveis de maturidade, os quais determinam o grau de conformidade mediante padrões pré-estabelecidos, sendo a medição desses níveis uma ação que orienta melhorias dos processos e padrões adotados (Araujo; Albuquerque Jr.; Passos, 2025).

Ante o exposto, a maturidade, expressa por um framework de cibersegurança, apoia a instituição a identificar sua posição em relação a determinados níveis, visando à melhoria da segurança

digital, sendo que essa aferição contempla a governança. Entretanto, observa-se a ausência de diagnósticos sistemáticos acerca do nível de maturidade em cibersegurança em Redes de Escolas de Educação Básica, especialmente sob a perspectiva integrada da governança.

Diante desse contexto, formula-se a seguinte questão de pesquisa: qual é o nível de maturidade em cibersegurança de uma Rede de Escolas de Educação Básica à luz do Cybersecurity Framework 2.0?

Justifica-se esta investigação pela relevância social e institucional da proteção de dados sensíveis no ambiente educacional, bem como pela necessidade de diagnósticos que subsidiem decisões estratégicas e políticas organizacionais voltadas ao fortalecimento da governança da cibersegurança. Assim, o objetivo deste estudo é analisar o nível de maturidade em cibersegurança de uma Rede de Escolas de Educação Básica, com base no Cybersecurity Framework 2.0 do National Institute of Standards and Technology (NIST), por meio da validação estatística dos indicadores e da mensuração das dimensões do framework, de forma específica, mensurável e alcançável.

Mediante esse intento, esta investigação é dividida em seções. Além desta introdução, a seção seguinte aborda o contexto da segurança digital no âmbito escolar, apresenta o local de aplicação desta pesquisa, bem como o framework de cibersegurança adotado para o exame da maturidade, o qual contempla a governança. Em sequência, os caminhos metodológicos perpassados por esta investigação são apresentados, sendo esses sucedidos pela explanação dos resultados. Por fim, as considerações finais são anunciadas.

2 REFERENCIAL TEÓRICO

2.1 CIBERSEGURANÇA NO CONTEXTO EDUCACIONAL

De acordo com Santos, Farias e Nunes (2024), muitas instituições lidam diariamente com dados sensíveis, tais como informações pessoais de clientes, históricos financeiros e registros de funcionários. No contexto educacional, essa realidade assume maior complexidade, pois envolve dados de crianças e adolescentes, público especialmente vulnerável no ambiente digital. Assim, informações pessoais de alunos e de seus responsáveis tornam-se ainda mais relevantes sob a perspectiva da proteção de dados. Quando inexistem mecanismos adequados de segurança, esses registros passam a constituir alvos potenciais de ataques cibernéticos, vazamentos e usos indevidos, comprometendo não apenas a integridade institucional, mas também direitos individuais.

Nesse sentido, Hurel e Lobato (2018) observaram que a inserção de tecnologias nas escolas ocorreu, em muitos casos, sem planejamento de infraestrutura ou capacitação adequada, ampliando a exposição a riscos digitais. Essa constatação dialoga com o diagnóstico apresentado pelo Laboratório Nacional de Computação Científica (LNCC, 2024), segundo o qual o setor educacional brasileiro figura entre os mais vulneráveis a ataques cibernéticos. Tal vulnerabilidade, conforme evidenciado,

decorre da ausência de políticas institucionais consistentes voltadas à segurança digital, indicando que o problema não se restringe à dimensão técnica, mas envolve falhas de gestão e de planejamento estratégico.

Adicionalmente, o relatório da UNESCO (2023) aponta que muitas escolas brasileiras ainda operam com infraestrutura precária, conexões instáveis e ausência de políticas estruturadas de proteção de dados. Essa precariedade manifesta-se de forma ainda mais intensa em regiões rurais e periféricas, onde os recursos tecnológicos são escassos e a manutenção de sistemas digitais enfrenta limitações estruturais.

Souza e Brito (2021) corroboram esse cenário ao alertarem para riscos institucionais decorrentes da ausência de diretrizes claras e da fragilidade técnica, fatores que comprometem a capacidade de resposta a incidentes, como violações e vazamentos de dados. Observa-se, portanto, convergência entre os estudos quanto à fragilidade estrutural do ambiente educacional frente às ameaças digitais.

Sob a perspectiva econômica, Sapiński (2023) demonstra que os impactos de incidentes cibernéticos ultrapassam a esfera operacional. Com base em levantamentos realizados em 2020, o autor indica que os custos médios de uma violação de dados alcançaram aproximadamente US$ 3,86 milhões. Além disso, o custo global estimado de perdas associadas a ataques cibernéticos ultrapassou US$ 1,5 trilhão anuais, evidenciando a magnitude econômica e social desses incidentes. Esses dados reforçam que a cibersegurança não pode ser tratada apenas como questão técnica, mas como componente estratégico essencial à sustentabilidade institucional.

Observa-se convergência entre Hurel e Lobato (2018), Souza e Brito (2021), UNESCO (2023) e LNCC (2024) quanto à vulnerabilidade estrutural do setor educacional, seja por insuficiência de planejamento tecnológico, fragilidade institucional, precariedade de infraestrutura ou ausência de políticas consolidadas. Tal consenso evidencia que o desafio ultrapassa a conectividade e exige uma abordagem sistêmica.

Nessa direção, a Organização para a Cooperação e Desenvolvimento Econômico (OECD, 2019) sustenta que é necessário assegurar acesso seguro e educação digital adequada, respeitando as especificidades regionais e socioculturais.

Portanto, a responsabilidade pela proteção das informações recai sobre a instituição e seus gestores, que devem adotar medidas estruturadas para garantir a integridade e a segurança dos dados, prevenindo acessos não autorizados e vazamentos. Considerando os riscos imputados a alunos e funcionários, decorrentes da tratativa de dados sensíveis (Farias; Nunes, 2024), a vulnerabilidade institucional apontada pelo LNCC (2024), a precariedade estrutural evidenciada pela UNESCO (2023), a ausência de planejamento destacada por Hurel e Lobato (2018) e o impacto financeiro indicado por Sapiński (2023), torna-se necessário tratar a cibersegurança sob uma perspectiva mais ampla e

integrada. Nesse contexto, emerge a governança como dimensão estruturante capaz de articular estratégia, responsabilidade institucional e gestão de riscos.

2.2 GOVERNANÇA ORGANIZACIONAL E CIBERSEGURANÇA

De acordo com Kjaer (2004), o termo governança remete ao ato de pilotar, conduzir ou elaborar regras, indicando uma noção de direção e orientação estratégica.

Historicamente, sua consolidação no campo organizacional relaciona-se à necessidade de regulação decorrente de escândalos financeiros ocorridos em empresas dos Estados Unidos, na década de 1980, quando investidores passaram a reagir contra acionistas e gestores que conduziam organizações de forma dissonante aos interesses institucionais e societários (Oliveira; Santos; Pinto, 2023). Assim, a governança emerge como resposta à demanda por maior controle, transparência e alinhamento estratégico nas organizações.

No âmbito organizacional contempore, Frogeri, Portugal e Guedes (2022) associam a governança a princípios estruturantes como transparência, equidade, responsabilidade corporativa e prestação de contas, operacionalizados por meio de mecanismos formais de controle e supervisão. Tais princípios contemplam tanto o ambiente interno quanto o externo da instituição, evidenciando que a governança não se limita a processos administrativos, mas envolve a relação da organização com seus stakeholders e com a sociedade. Nessa perspectiva, governança assume caráter sistêmico, ultrapassando a gestão operacional e incorporando dimensões estratégicas e normativas.

Conforme Silva et al. (2023), governança apresenta conotação multidimensional, pois abrange a organização em sua completude e o contexto social no qual está inserida, observa-se, entretanto, que embora haja consenso na literatura quanto aos princípios estruturantes da governança, sua incorporação à cibersegurança ainda ocorre de maneira gradual nas instituições educacionais. Em muitos casos, as práticas permanecem restritas a controles operacionais, como definição de acessos e medidas técnicas isoladas, sem integração plena à estratégia institucional e aos processos decisórios de alto nível. É nesse contexto que os frameworks de cibersegurança assumem relevância. Purser (2014) afirma que tais frameworks têm como objetivo primordial prevenir ou mitigar ataques, reduzindo o risco de ameaças.

Complementarmente, Maleh et al. (2021) ressaltam que esses instrumentos visam elevar a proteção dos ativos organizacionais frente às ameaças cibernéticas. Contudo, quando articulados à governança, os frameworks deixam de ser meramente instrumentos técnicos e passam a constituir ferramentas estratégicas, capazes de integrar políticas, responsabilidades, gestão de riscos e supervisão institucional. Dessa forma, a aproximação entre governança e cibersegurança revela-se fundamental para a consolidação de práticas estruturadas e sustentáveis no ambiente educacional.

2.3 FRAMEWORK NIST E NÍVEIS DE MATURIDADE

Nesta pesquisa destaca-se o Cybersecurity Framework 2.0 (CSF), denominado em português Framework de Cibersegurança, elaborado pelo National Institute of Standards and Technology (NIST, 2024). O instrumento foi projetado para ser utilizado por organizações de diferentes portes e setores, incluindo indústria, governo, academia e entidades sem fins lucrativos. Sua proposta consiste em oferecer diretrizes estruturadas para identificação, gestão e mitigação de riscos cibernéticos, integrando dimensões técnicas e estratégicas.

O CSF 2.0 é estruturado em seis funções, também denominadas dimensões: identificar, proteger, detectar, responder, recuperar e governança. As cinco primeiras funções compõem o ciclo operacional de gestão de riscos, enquanto a governança assume caráter transversal, orientando as demais dimensões. Conforme o NIST (2024), a dimensão governança envolve a compreensão do contexto organizacional, o estabelecimento da estratégia de cibersegurança, a gestão de riscos da cadeia de suprimentos, a definição de funções, responsabilidades e autoridades, bem como a supervisão das políticas institucionais. A dimensão identificar estabelece que os riscos de cibersegurança da organização devem ser compreendidos de forma sistêmica, incluindo a análise de ativos, vulnerabilidades e ameaças. Além disso, prevê a identificação de oportunidades de melhoria para políticas, planos e processos que sustentam a gestão de riscos (NIST, 2024).

A dimensão proteger prioriza a implementação de medidas de segurança destinadas a mitigar riscos previamente identificados, incluindo o controle de acesso e a restrição de usuários a níveis apropriados de autorização, conforme discutido por Abouelmehdi et al. (2017) e Santana (2021). Já a dimensão detectar pressupõe que possíveis ataques e comprometimentos devam ser encontrados e analisados em tempo oportuno (NIST, 2024). Na sequência lógica do framework, a dimensão responder estabelece a tomada de medidas frente a incidentes previamente detectados, contemplando ações de contenção, análise, mitigação, elaboração de relatórios e comunicação institucional (NIST, 2024).

Por fim, a dimensão recuperar determina que ativos e operações afetados sejam restaurados de forma estruturada, permitindo o restabelecimento das atividades e a redução dos impactos decorrentes do incidente. Observa-se, assim, que o CSF 2.0 não se limita a controles técnicos, mas organiza um ciclo contínuo de gestão de riscos orientado pela governança. No que concerne aos níveis de maturidade, o CSF 2.0 (NIST, 2024) estabelece quatro estágios evolutivos: Nível 1 – Parcial (Partial); Nível 2 – Informado por Risco (Risk-Informed); Nível 3 – Repetível (Repeatable); e Nível 4 – Adaptativo (Adaptive). A maturidade, nesse contexto, está associada ao grau de institucionalização das práticas de gestão de riscos e à sua integração aos processos organizacionais.

Conforme Araujo, Albuquerque Jr. e Passos (2025, p. 4), “maturidade é o grau de conformidade de um processo em relação a padrões de excelência, o que torna importante fazer sua aferição para

orientar a melhoria das práticas organizacionais.” Essa definição evidencia que a mensuração da maturidade não constitui exercício meramente classificatório, mas instrumento orientador de aprimoramento institucional, embora o CSF 2.0 seja amplamente reconhecido como referência internacional, observa-se que sua aplicação empírica em Redes de Escolas de Educação Básica ainda é pouco explorada na literatura nacional, especialmente sob a perspectiva da mensuração estruturada da maturidade associada à governança.

2.4 LACUNA TEÓRICA E DIRECIONAMENTO DA PESQUISA

À luz do exposto, considerando a importância da governança e da maturidade em cibersegurança, aliadas à necessidade de enfrentamento de ataques direcionados a dados sensíveis (Farias; Nunes, 2024), esta pesquisa situa a análise da maturidade no âmbito das Instituições de Ensino. Conforme discutido anteriormente, tais instituições apresentam fragilidades estruturais e organizacionais (LNCC, 2024; UNESCO, 2023), além de impactos financeiros potencialmente significativos decorrentes de incidentes cibernéticos (Sapiński, 2023).

Esse cenário evidencia que a cibersegurança, quando dissociada de uma perspectiva estratégica e de governança, tende a permanecer restrita a medidas operacionais isoladas. Embora a literatura nacional e internacional aborde amplamente temas como proteção de dados, frameworks de cibersegurança e princípios de governança organizacional, observa-se que a interseção entre esses elementos ainda é pouco explorada sob a perspectiva da mensuração sistemática da maturidade em contextos educacionais. Em especial, há escassez de estudos empíricos aplicados a Redes de Educação Básica brasileiras que utilizem o Cybersecurity Framework 2.0 como instrumento estruturante de avaliação, integrando governança e gestão de riscos em uma análise consolidada.

Dessa forma, identifica-se lacuna na literatura quanto à aferição estruturada do nível de maturidade em cibersegurança em organizações educacionais com múltiplas unidades administrativas, cuja complexidade operacional demanda coordenação estratégica e alinhamento institucional. A ausência de diagnósticos sistemáticos dificulta o planejamento de ações corretivas e o fortalecimento das políticas institucionais de segurança digital, sobretudo em redes com ampla dispersão territorial.

Portanto, assume-se como lócus desta pesquisa uma Rede de Escolas de Educação Básica composta por 98 unidades distribuídas no território nacional. A escolha desse contexto justifica-se pela necessidade de compreender como práticas de governança e gestão de riscos se manifestam em estruturas educacionais amplas e descentralizadas. Ao direcionar a análise para esse ambiente específico, busca-se contribuir para o preenchimento da lacuna identificada, oferecendo subsídios teóricos e empíricos que orientem o aprimoramento institucional da maturidade em cibersegurança.

3 METODOLOGIA

3.1 DELINEAMENTO DA PESQUISA

No que concerne à tipificação desta investigação, trata-se de um Estudo de Caso (Yin, 2014), com natureza exploratória-descritiva e abordagem quantitativa. Mediante busca por elevar a experiência acerca da maturidade em cibersegurança (exploratória), a qual deve ser realizada com rigor na apresentação dos achados (descritiva), têm-se que "[...] a pesquisa exploratória realiza descrições precisas da situação e quer descobrir as relações existentes entre seus elementos e componentes" (Bervian; Cervo; Silva, 2002, p. 63).

Não obstante, é quantitativa pelo uso de métodos matemáticos para permitir a observação do fenômeno de forma neutra (Minayo, 1998), possibilitando a mensuração objetiva dos indicadores e a análise sistemática dos níveis de maturidade identificados.

Essa abordagem favorece a consistência analítica dos resultados, ao permitir o tratamento estatístico das variáveis e a interpretação fundamentada dos dados coletados, em consonância com o propósito de avaliar, de maneira estruturada, a maturidade em cibersegurança no contexto investigado.

3.2 LÓCUS, POPULAÇÃO E AMOSTRA

O lócus da pesquisa é uma Rede de Escolas de Educação Básica. A população foi constituída por 139 funcionários atuantes na área de Tecnologia da Informação, considerando-se que esses profissionais desempenham papel central na gestão, manutenção e proteção dos sistemas institucionais. A amostra estimada foi de 103 respondentes, conforme cálculo amostral realizado a partir dos parâmetros N = 139, $Z\alpha = 1{,}96$ (95 % de confiança), e = 0,05, p = 0,5 e q = 0,5 (Miot, 2011).

A adoção desses parâmetros visou assegurar nível adequado de precisão estatística e representatividade dos dados coletados. Junto ao questionário, criado por meio do Google Forms, foi disponibilizado o Termo de Consentimento Livre e Esclarecido (TCLE), sendo sua leitura obrigatória para a continuidade das respostas. Tal procedimento garantiu que os participantes fossem devidamente informados quanto aos objetivos da pesquisa, ao caráter voluntário da participação e à confidencialidade das informações fornecidas.

3.3 INSTRUMENTO DE COLETA DE DADOS

Os procedimentos metodológicos desta investigação foram operacionalizados em três etapas: i) coleta de dados; ii) legitimação de indicadores; e iii) análise da maturidade. A primeira etapa consistiu na aplicação do questionário baseado no Cybersecurity Framework 2.0 (CSF 2.0) do National Institute of Standards and Technology (NIST, 2024), instrumento estruturado para avaliação de práticas relacionadas à gestão de riscos em cibersegurança.

O questionário é composto por 106 afirmativas, organizadas em 22 categorias, as quais estão distribuídas em seis funções (dimensões): governança, identificar, proteger, detectar, responder e recuperar. Essa organização permite examinar de forma sistemática os diferentes componentes do framework, contemplando tanto aspectos estratégicos quanto operacionais da cibersegurança. As afirmativas foram apresentadas em escala do tipo Likert de cinco pontos, com as âncoras discordo totalmente, neutro e concordo totalmente. Tal estrutura possibilita mensurar o grau de aderência das práticas institucionais aos parâmetros estabelecidos pelo CSF 2.0, permitindo posterior tratamento estatístico das respostas.

3.4 VALIDAÇÃO ESTATÍSTICA DOS INDICADORES

Após a coleta de dados, procedeu-se à legitimação dos indicadores (ii), etapa destinada à validação estatística dos conceitos adotados no instrumento (Hair et al., 2009). Nesse processo, as 106 afirmativas do questionário foram tratadas como variáveis observáveis, enquanto as 22 categorias e as seis funções do CSF 2.0 foram consideradas construtos analíticos. Tal distinção permitiu estruturar a análise de forma coerente com a organização teórica do framework. Para tanto, subconjuntos de variáveis foram agrupados em blocos representativos de cada categoria ou dimensão do instrumento, assegurando correspondência entre os itens do questionário e os construtos avaliados (Hair et al., 2009).

Inicialmente, verificou-se a presença de observações atípicas (outliers), a fim de evitar distorções nas análises subsequentes. Em seguida, realizou-se a análise de dimensionalidade, confiabilidade e validade dos indicadores. A dimensionalidade foi examinada por meio do critério de Kaiser-Meyer-Olkin (KMO), adotando-se valor mínimo de 0,50 para cada categoria e dimensão (Damásio, 2012). A confiabilidade foi aferida pelo Alfa de Cronbach (AC), considerando-se adequado valor superior a 0,60 (Hair et al., 2009).

A validade foi avaliada mediante o coeficiente de Pearson (r), esperando-se correlação positiva entre as variáveis e p-valor inferior a 0,05 (Formiga et al., 2018). O atendimento simultâneo desses parâmetros assegura consistência interna, adequação estatística e robustez aos indicadores utilizados na análise.

3.5 ANÁLISE DA MATURIDADE

Na terceira etapa (iii), procedeu-se à análise da maturidade das categorias e dimensões avaliadas. Para tanto, foram utilizadas medidas de tendência central (Média), medida de dispersão (Desvio Padrão) e o Intervalo de Confiança de 95%, permitindo examinar não apenas o posicionamento médio das respostas, mas também a estabilidade e a variabilidade dos resultados obtidos. O NIST (2024) estabelece quatro níveis de maturidade: Nível 1 – Parcial (Partial); Nível 2 –

Informado por Risco (Risk-Informed); Nível 3 – Repetível (Repeatable); e Nível 4 – Adaptativo (Adaptive). Esses níveis expressam estágios progressivos de institucionalização das práticas de gestão de riscos em cibersegurança.

Com base nessa estrutura, Bernardo (2024) e Bernardo, Malta e Magalhães (2025) associaram aos níveis os seguintes intervalos de médias: ≤ 2,99; ≤ 3,99; ≤ 4,99; e = 5,00, respectivamente, acrescentando o valor ≤ 1,99 como nível zero, denominado "muito ruim". Assim, esta pesquisa adota tais parâmetros, incorporando o Nível 0: Inexistente, de modo a contemplar situações de ausência ou fragilidade extrema das práticas avaliadas.

Diante dos resultados apurados por categoria e dimensão, o nível geral de maturidade das Instituições de Ensino da Rede foi determinado pelo menor nível identificado entre as funções do CSF 2.0, considerando o caráter sistêmico do framework e a necessidade de integração entre suas dimensões. Esse critério parte do entendimento de que a maturidade organizacional não pode ser superior à sua dimensão mais frágil, uma vez que as funções devem atuar de forma articulada.

Para as dimensões que apresentaram menor nível de maturidade foram delineadas ações com vistas à sua elevação, em consonância com as diretrizes estabelecidas pelo NIST (2025). O tratamento estatístico dos dados foi realizado por meio do software RStudio, versão 2021.09.2 Build 382, possibilitando a execução das análises de forma estruturada e reprodutível.

4 RESULTADOS E DISCUSSÕES

A coleta de dados foi realizada entre os dias 20 e 23/01/2026, totalizando 118 respostas válidas. Não foram identificados outliers, conforme critérios estabelecidos por Hair et al. (2009), o que reforça a consistência do banco de dados analisado. Assim, a amostra final de 118 respondentes supera a estimativa inicial de 103 participantes, calculada segundo os parâmetros apresentados por Miot (2011), assegurando margem estatística adequada e maior robustez aos resultados obtidos. O perfil amostral dos respondentes é apresentado por meio da Tabela 1.

Tabela 1: Perfil da amostra de 118 respondentes

Aspecto	Característica	N.	∑	%	∑%
Idade	Entre 19 e 29 anos	12	12	10,17	10,17
	Entre 30 e 39 anos	52	64	44,07	54,23
	Entre 40 e 49 anos	41	105	34,75	88,99
	Entre 50 e 65 anos	13	118	11,02	100,00
Gênero	Feminino	15	15	12,71	12,71
	Masculino	103	118	87,29	100,00
Formação	Ensino Fundamental	0	0	0,00	0,00
	Ensino Médio	2	2	1,69	1,69
	Ensino Superior (Graduação)	44	46	37,29	38,98
	Pós-Graduação (Especialização)	64	110	54,24	93,22
	Pós-Graduação (Mestrado)	8	118	6,78	100,00
	Pós-Graduação (Doutorado)	0	118	0,00	100,00
	Pós-Doutorado	0	118	0,00	100,00
Possui formação acadêmica na área de Tecnologia	Não	29	29	24,58	24,58
	Sim	89	118	75,42	100,00
Passou por algum tipo de incidente de segurança digital	Não	84	84	71,19	71,19
	Sim	34	118	28,81	100,00
Tempo (anos) de atuação na área de Tecnologia da Informação	Menos de 1 ano	13	13	11,02	11,01
	Entre 1 e 9 anos	30	43	25,42	36,44
	Entre 10 e 19 anos	49	92	41,53	77,97
	Entre 20 e 29 anos	21	113	17,80	95,77
	Entre 30 e 35 anos	5	118	4,24	100,00

Legenda: N.: Número (quantitativo); ∑: Somatório; %: Percentual; ∑%: Somatório do Percentual.
Fonte: Dados da pesquisa (2026)

Observa-se que a maioria dos respondentes possui idade superior a 30 anos (89,83%), o que indica maturidade profissional consolidada. Em termos de formação acadêmica, 98,31% possuem Ensino Superior completo ou Pós-Graduação, demonstrando elevado capital intelectual no grupo analisado. Destaca-se ainda que 75,42% possuem formação na área de Tecnologia da Informação, o que reforça a aderência técnica das respostas às dimensões avaliadas no instrumento CSF 2.0.

Quanto ao tempo de atuação na área de Tecnologia da Informação, verifica-se que 65,57% possuem mais de dez anos de experiência, indicando trajetória profissional consolidada e familiaridade com práticas de gestão tecnológica. A predominância masculina (87,29%) reflete uma característica ainda recorrente no setor de tecnologia, sem prejuízo à validade da análise, uma vez que o critério de seleção esteve vinculado à função desempenhada e não a características demográficas.

Quando questionados acerca da ocorrência de incidentes de segurança digital em âmbito pessoal, 71,19% afirmaram não ter experienciado tais eventos, enquanto 28,81% relataram ocorrência. Essa distribuição pode estar associada ao nível de formação técnica e à experiência profissional dos respondentes, fatores que tendem a favorecer maior capacidade de prevenção, identificação e mitigação de riscos cibernéticos.

Os dados apresentados evidenciam que a amostra é composta por profissionais com experiência consolidada, formação elevada e atuação direta na área tecnológica, o que confere legitimidade às percepções expressas acerca da maturidade em cibersegurança da Rede analisada. Além disso, considerando que os participantes estão distribuídos nas diferentes Unidades da Rede — em suas

finalidades privada e social —, as respostas tendem a refletir de maneira abrangente o contexto organizacional investigado.

A partir da caracterização da amostra, prosseguiu-se à legitimação estatística dos indicadores, considerando os critérios de dimensionalidade, confiabilidade e validade (Hair et al., 2009), operacionalizados por meio do Quadro 1 (Anexo A). O índice de Kaiser-Meyer-Olkin apresentou valores não inferiores a 0,50 (Damásio, 2012), o Alfa de Cronbach superou o limite mínimo recomendado na literatura (Hair et al., 2009) e o coeficiente de Pearson (r) demonstrou correlações positivas com p-valor inferior a 0,05 (Formiga et al., 2018). Esses resultados confirmam a adequação estatística do instrumento aplicado e sustentam a confiabilidade das análises subsequentes.

Superada a etapa de validação, procedeu-se à análise da maturidade por meio das medidas de Média, Desvio Padrão e Intervalo de Confiança de 95% das dimensões e categorias do CSF 2.0 (NIST, 2024), conforme apresentado no Tabela 2.

Tabela 2: Média, Desvio Padrão e Intervalo de Confiança de 95% das dimensões e categorias do Framework de Cibersegurança (CSF 2.0)

Dimensão | Categoria	**Média**	**D.P.**	**I.C. 95%**
GOVERNANÇA (GV)	3,86	0,93	[3,70; 4,03]
Contexto Organizacional (GV.OC)	3,99	0,86	[3,84; 4,15]
Estratégia de Gestão de Riscos (GV.RM)	3,85	0,92	[3,69; 4,02]
Funções, Responsabilidades e Autoridades (GV.RR)	3,84	1,01	[3,66; 4,02]
Política (GV.PO)	3,89	0,93	[3,72; 4,06]
Supervisão (GV.OV)	3,99	0,85	[3,84; 4,15]
Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (GV.SC)	3,77	0,95	[3,60; 3,95]
IDENTIFICAR (ID)	4,08	0,88	[3,92; 4,23]
Gestão de Ativos (ID.AM)	3,99	0,90	[3,83; 4,15]
Avaliação de Riscos (ID.RA)	4,13	0,86	[3,98; 4,29]
Melhoria (ID.IM)	4,09	0,88	[3,93; 4,25]
PROTEGER (PR)	4,12	0,86	[3,97; 4,28]
Gestão de Identidade, Autenticação e Controle de Acesso (PR.AA)	4,27	0,80	[4,13; 4,42]
Conscientização e Treinamento (PR.AT)	3,95	0,91	[3,79; 4,12]
Segurança de Dados (PR.DS)	4,22	0,80	[4,07; 4,36]
Segurança da Plataforma (PR.PS)	4,04	0,87	[3,88; 4,19]
Resiliência da Infraestrutura Tecnológica (PR.IR)	4,02	0,90	[3,86; 4,18]
DETECTAR (DE)	4,05	0,91	[3,88; 4,21]
Monitoramento Contínuo (DE.CM)	4,12	0,89	[3,96; 4,28]
Análise de Eventos Adversos (DE.AE)	3,98	0,93	[3,81; 4,15]
RESPONDER (RS)	4,06	0,88	[3,90; 4,22]
Gestão de Incidentes (RS.MA)	4,08	0,89	[3,92; 4,24]
Análise de Incidentes (RS.AN)	4,08	0,90	[3,92; 4,24]
Relatórios e Comunicação de Resposta a Incidentes (RS.CO)	3,99	0,81	[3,84; 4,13]
Mitigação de Incidentes (RS.MI)	4,06	0,88	[3,90; 4,22]
RECUPERAR (RC)	4,05	0,84	[3,90; 4,20]
Execução do Plano de Recuperação de Incidentes (RC.RP)	4,08	0,83	[3,93; 4,23]
Comunicação de Recuperação de Incidentes (RC.CO)	3,94	0,86	[3,78; 4,10]
Legenda: D.P..: Desvio Padrão; I.C.: Intervalo de Confiança			

Fonte: Dados da pesquisa (2026)

A categoria Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (GV.SC), pertencente à dimensão Governança (GV), apresenta a menor média (3,77) dentre todas as categorias

do CSF 2.0. Segundo o NIST (2024), os ambientes tecnológicos contemporâneos dependem de cadeias de suprimentos interconectadas, que envolvem fornecedores, desenvolvedores, integradores de sistemas e provedores externos de serviços responsáveis pela sustentação de produtos e serviços de tecnologia. Por serem essas interações moldadas e influenciadas por recursos tecnológicos, torna-se indispensável a gestão sistemática dos riscos associados a essa cadeia.

Em sentido oposto, a categoria Gestão de Identidade, Autenticação e Controle de Acesso (PR.AA), vinculada à dimensão Proteger (PR), apresenta a maior média (4,27) entre as categorias analisadas. A autenticação tem por finalidade verificar a identidade dos usuários, enquanto o controle de acesso restringe permissões conforme as atribuições funcionais (Abouelmehdi et al., 2017).

Santana (2021) ressalta que a ampliação do controle de acesso para uma gestão integrada de identidade constitui elemento central na proteção contra acessos indevidos e uso não autorizado de informações sensíveis. Observa-se, portanto, uma assimetria relevante entre as dimensões analisadas. Enquanto os respondentes percebem elevado nível de proteção interna, associado aos mecanismos de autenticação e controle de identidade, identificam menor maturidade na gestão de riscos relacionados à cadeia de suprimentos. Essa diferença indica que os controles internos encontram-se mais consolidados do que os mecanismos voltados à supervisão e priorização de riscos provenientes de fornecedores e agentes externos.

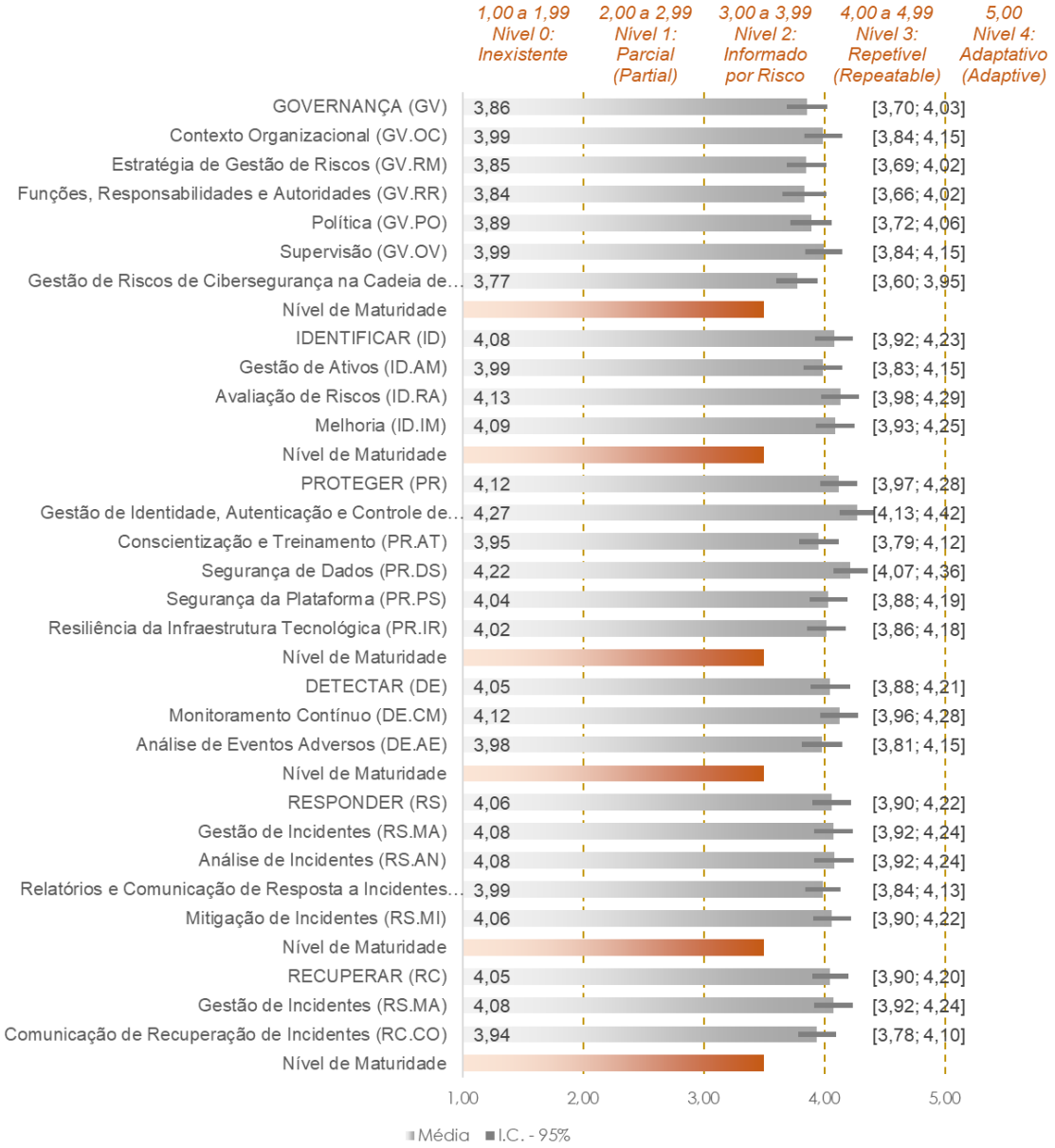
Tal cenário sugere que o controle instituído é parcialmente abrangente. Quando a gestão de riscos externos não acompanha o nível de proteção interna, a organização permanece vulnerável a incidentes originados fora de seus limites operacionais diretos.

Considerando que a cadeia de suprimentos é composta por múltiplos atores interdependentes (NIST, 2024), fragilidades nesse domínio podem comprometer a coerência e a efetividade da estratégia global de cibersegurança.

A análise estatística reforça essa interpretação. O intervalo de confiança da categoria GV.SC situa-se entre 3,60 e 3,95, enquanto o da categoria PR.AA encontra-se entre 4,13 e 4,42. Como não há sobreposição entre os intervalos, a diferença observada revela consistência estatística entre as categorias analisadas. Essa evidência fortalece a compreensão de que a maturidade em proteção interna supera a maturidade na governança da cadeia de suprimentos.

Essas distinções, apresentadas na Tabela 2, são complementadas pela análise dos níveis de maturidade das categorias e dimensões do CSF 2.0, conforme representado no Gráfico 1.

Gráfico 1: Níveis de maturidade do Framework de Cibersegurança



Fonte: Dados da pesquisa (2026)

Assim, a dimensão Proteger (PR) revela-se um aspecto relevante para a Instituição; contudo, não se encontra plenamente articulada no contexto da Governança (GV), uma vez que ambas representam extremos no espectro da cibersegurança, com médias de 4,12 e 3,86, respectivamente. Considerando que a Governança compreende a análise do contexto organizacional, a definição da estratégia de cibersegurança e a gestão de riscos da Cadeia de Suprimentos, bem como a delimitação de funções, responsabilidades e autoridades (NIST, 2024), torna-se premente examinar a cibersegurança sob uma perspectiva sistêmica de Governança, em contraposição a uma abordagem restrita e predominantemente operacional centrada na dimensão Proteger.Conforme evidenciado no Gráfico 1, todas as dimensões do CSF 2.0 (NIST, 2024) situam-se no Nível 2 de maturidade, caracterizado como gestão informada por risco.

Nesse estágio, as práticas de gestão de riscos são reconhecidas e aprovadas pela administração, mas ainda podem não estar formalmente institucionalizadas como políticas organizacionais consolidadas. Tal cenário indica a necessidade de fortalecimento da Governança, pois é essa dimensão que orienta a priorização e a integração das demais funções no contexto da missão institucional e das expectativas das partes interessadas (NIST, 2024).

Considerando que riscos de cibersegurança, como a violação de dados sensíveis, envolvem informações de alunos e funcionários (Farias; Nunes, 2024), bem como agentes externos vinculados à Cadeia de Suprimentos, a Governança assume papel central ao abranger os ambientes interno e externo da instituição. Essa perspectiva dialoga com os princípios de transparência, equidade, responsabilidade corporativa e prestação de contas, sustentados por mecanismos de controle (Frogeri; Portugal; Guedes, 2022). Nesse sentido, a consolidação da maturidade demanda integração de todas as dimensões sob a égide da Governança (NIST, 2024).

Para evolução do nível de maturidade, destaca-se que a dimensão Governança (GV) apresenta a menor média dentre as dimensões analisadas, perfazendo 3,86 pontos (Gráfico 1). No interior dessa dimensão, a categoria Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (GV.SC) registra média de 3,77 pontos e intervalo de confiança de 95% entre 3,60 e 3,95. Por situar-se integralmente no Nível 2, essa categoria configura-se como a mais crítica no âmbito da Governança.

Entre as afirmativas do questionário associadas à categoria GV.SC, destaca-se a GV.SC-04: “Os fornecedores são conhecidos e priorizados por criticidade” (NIST, 2024, p. 17, tradução nossa), cuja média foi de 3,61, a menor dentre as afirmativas dessa categoria. Esse resultado contribui para a redução da média global da GV.SC e sugere tendência a uma postura reativa, uma vez que o valor se encontra próximo ao ponto neutro da escala Likert adotada.

Diante desse cenário, propõem-se ações voltadas ao avanço do nível de maturidade da dimensão Governança (GV), especialmente no que concerne à categoria GV.SC. Nesse sentido, recomenda-se:

i) estabelecer critérios formais para a classificação de fornecedores por criticidade, considerando a sensibilidade dos dados processados, o nível de acesso aos sistemas institucionais e a relevância estratégica dos serviços prestados;
ii) manter registro atualizado dos fornecedores, priorizando-os conforme os critérios previamente definidos (NIST, 2025).

Segundo o NIST (2024), a Cadeia de Suprimentos constitui área crítica na gestão de riscos de cibersegurança, pois os sistemas e redes que sustentam a missão organizacional envolvem múltiplos atores interdependentes. A vulnerabilidade nessa cadeia torna-se significativa justamente pela interconexão tecnológica entre agentes internos e externos.

No contexto da Rede de Escolas de Educação Básica analisada, composta por 98 unidades distribuídas no território nacional, a gestão estruturada dessa cadeia revela-se ainda mais necessária. Todavia, conforme evidenciado nas análises precedentes sob a perspectiva dos respondentes, a priorização de fornecedores por criticidade ainda não se encontra consolidada (GV.SC-04). A implementação das ações propostas poderá contribuir para mitigar riscos, promover postura proativa e reduzir vulnerabilidades associadas à cadeia, não apenas sob a ótica financeira dos incidentes cibernéticos (Sapiński, 2023), mas também sob a perspectiva estratégica e institucional.

5 CONCLUSÃO

Esta pesquisa teve como objetivo analisar o nível de maturidade em cibersegurança de uma Rede de Escolas de Educação Básica. Com base em uma amostra de 118 respondentes, identificou-se nível geral de maturidade dois, em uma escala de cinco níveis adotada nesta investigação, classificado como Informado por Risco. Nesse estágio, as práticas de gestão de riscos são reconhecidas pela administração, embora ainda não estejam plenamente institucionalizadas como política organizacional formal. Tal enquadramento foi observado nas dimensões identificar, proteger, detectar, responder e recuperar, bem como na governança, que orienta e integra as demais funções do framework.

Os resultados indicam que, apesar do elevado nível de formação acadêmica dos respondentes (98,31%) e da predominância de atuação na área de Tecnologia da Informação (75,42%), a qualificação técnica não se traduz automaticamente em maturidade consolidada em governança da cibersegurança. Esta última pressupõe articulação estratégica, definição clara de responsabilidades e integração organizacional, ultrapassando o domínio estritamente operacional.

Verificou-se que a dimensão Proteger apresentou desempenho mais elevado, especialmente na categoria Gestão de Identidade, Autenticação e Controle de Acesso. Contudo, a menor maturidade identificada na Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos, vinculada à dimensão Governança, evidencia fragilidade estrutural relevante. Tal assimetria demonstra que controles técnicos internos, quando não acompanhados de gestão estratégica sobre atores externos, podem comprometer a consistência do modelo de segurança adotado.

Em organizações educacionais, a eventual_attachência de incidentes envolvendo dados sensíveis de discentes, responsáveis e colaboradores pode gerar impactos financeiros, jurídicos e reputacionais significativos. Nesse contexto, a atuação preventiva, sustentada por práticas de governança, mostra-se mais efetiva do que intervenções meramente reativas.

À luz dos achados, recomenda-se o fortalecimento da governança da cibersegurança, com ênfase na classificação de fornecedores por criticidade, considerando a sensibilidade dos dados tratados, o nível de acesso concedido e a relevância estratégica dos serviços prestados, bem como na manutenção de registros atualizados que permitam priorização estruturada desses parceiros.

Espera-se que esta investigação contribua, no plano empírico, para o aprimoramento das práticas de cibersegurança da Rede analisada. No âmbito acadêmico, sugere-se a replicação do estudo em outras Redes de Educação Básica, a fim de ampliar a base comparativa e aprofundar o debate sobre maturidade em cibersegurança no contexto educacional brasileiro.

REFERÊNCIAS

ABOUELMEHDI, K. et al., Big data security and privacy in healthcare: A review. Journal of Big Data, v. 113, p. 73-80, 2017.

ANDRADE, D. et al., Information Security Management in a Higher Education Institution Based on Standards, Legal Basis for the Optimization of Administrative Resources. Journal of Ecohumanism, v. 3, n. 8, p. 1-14, 2024.

ARAUJO, M. S.; ALBUQUERQUE JR., A. E.; PASSOS, F. U. Modelos de maturidade em gestão da segurança da informação: análise comparativa na perspectiva da administração pública federal brasileira. Cuadernos de Educación y Desarrollo, v. 17, n. 5, p. e8480-e8480, 2025. Disponível em: https://ojs.cuadernoseducacion.com/ojs/index.php/ced/article/view/8480. Acesso em: 16 jan. 2026.

BELLI, Luca et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV Direito Rio, 2023.

BERNARDO, L. A. Assessing and Strengthening Cybersecurity Maturity: A NIST-Based Index Approach. 2024. 103f. Dissertação de Mestrado. Instituto Politécnico de Viana do Castelo – Mestrado em Governança, 2024. Disponível em: http://repositorio.ipvc.pt/bitstream/20.500.11960/3989/1/Luis_Bernardo.pdf. Acesso em: 19. jan. 2026.

BERNARDO, L. A.; MALTA, S.; MAGALHÃES, J. An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF. Electronics, v. 14, n. 7, 2025.

BERVIAN, P. A.; CERVO, A. L.; SILVA, R. Metodologia científica. São Paulo: Pretence Hall, 2002.

DAMÁSIO, B. F. Uso da análise fatorial exploratória em psicologia. Avaliação Psicológica, v. 11, n. 2, p. 213-227, 2012.

FORMIGA, N. S. et al. Evidência da invariância fatorial e validade convergente da escala de suporte organizacional: estudo com trabalhadores brasileiros. Boletim-Academia Paulista de Psicologia, v. 38, n. 94, p. 27-35, 2018.

FROGERI, R. F.; PORTUGAL, N. S.; GUEDES, L. C. V. O conceito de Governança e a Governança Corporativa. Textos para Discussão, v. 1, n. 1, p. 836-850, 2022. Disponível em: https://ojs.periodicos.unis.edu.br/textosparadiscussao/article/view/ 661. Acesso em: 16 jan. 2026.

HAIR, J. F. et al. Análise multivariada de dados. 6. ed. Porto Alegre: Bookman, 2009.

HUREL, L. M.; LOBATO, L. Governança da segurança cibernética: dinâmicas entre setor público e privado no Brasil. Cadernos Adenauer, v. 19, n. 3, p. 135-156, 2018.

KJAER, Anne Mette. Governance. 1. ed. Cambridge; Malden: Polity Press, 2004.

LNCC. A importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos. Laboratório Nacional de Computação Científica, 2024. Disponível em: 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. Acesso em: 05 mai. 2025.

MALEH, Y. et al. IT Governance and Information Security: Guides, Standards, and Frameworks. CRC Press, 2021.

MICROSOFT. Como os ataques cibernéticos estão mudando, de acordo com o novo Relatório de Defesa Digital da Microsoft. Microsoft, 20 out. 2021. Disponível em: https://news.microsoft.com/pt-br/como-os-ataques-ciberneticos-estao-mudando-de-acordo-com-o-novo-relatorio-de-defesa-digital-da-microsoft/. Acesso em: 20 fev. 2026.

MINAYO, M. C. S. O desafio do conhecimento: pesquisa qualitativa em saúde. 5. ed. São Paulo: Hucitec, 1998.

MIOT, H. A. Tamanho da amostra em estudos clínicos e experimentais. Jornal Vascular Brasileiro, v. 10, n. 4, p. 275-78, 2011. https://doi.org/10.1590/S1677-54492011000400001

NIST – National Institute of Standards and Technology. CSF 2.0 Implementation Examples, 2025. Disponível em: https://www.nist.gov/document/csf-20-implementation-examples-xlsx. Acesso em: 15 jan. 2026.

NIST – National Institute of Standards and Technology. Cybersecurity Framework (CSF) 2.0, 2024. Disponível em: https://doi.org/10.6028/NIST.CSWP.29. Acesso em: 10 fev. 2026.

OECD. The Concept of Safety and Security Education in the Context of Global Education Reform. Organização para a Cooperação e Desenvolvimento Econômico, 2019.

OLIVEIRA, J. G. L.; SANTOS, J. A.; PINTO, I. M. B. S. Análise da governança de TI em uma prefeitura do Nordeste do Brasil. Revista Brasileira de Administração Científica, v. 14, n. 4, p. 76-87, 2023.c

PURSER, S. Standards for Cyber Security. In: HATHAWAY, M.E. (Ed.). Best Practices in Computer Network Defense: Incident Detection and Response. Washington, DC: IOS Press, 2014. p. 97-106.

SANTANA, F. J. C. A segurança da informação na ciência da informação no Brasil. 2021. Dissertação (Mestrado em Ciência da Informação) – Instituto de Ciência da Informação, Universidade Federal da Bahia, Salvador, 2021.

SANTOS, D. S. et al., Tecnologias, cidadania e educação: estratégias para lidar com os riscos das práticas digitais nas instituições escolares. Revista Amor Mundi, v. 4, n. 7, p. 11-22, out. 2023.

SANTOS, R.; FARIAS, R. M.; NUNES, L. A. What is the future of Brazil's cybersecurity governance? Cadernos Gestão Pública e Cidadania, v. 29, p. 1-21, 2024.

SAPIŃSKI, A. 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, v. 7, n. 1, p. 52, mar. 2023.

SILVA, K. et al. Conceitos de governança aplicados na governança universitária: uma revisão sistemática. Revista de Gestão e Secretariado, v. 14, n. 4, p. 6113-6131, 2023.

SOUZA, F. M.; BRITO, R. P. Governança da informação na educação pública: riscos e vulnerabilidades frente à LGPD. Revista de Administração Pública e Gestão Social, 2021, v. 13, n. 1, 87–102. Disponível em: https://doi.org/10.21118/rbpgs.v13i1.1234. Acesso em 23 mai. 2025.

UNESCO. Review of Progress in the Basic Education Sector to 2024. Organização das Nações Unidas para a Educação, a Ciência e a Cultura, 2023. Disponível em: https://sol.sbc.org.br/index.php/wei/article/view/24932/24753. Acesso em: 05 mai. 2025.

YIN, R. K. Estudo de Caso: planejamento e métodos. 5ed. São Paulo: Bookman, 2014.

ANEXOS

Quadro 1 – Estatística de legitimação de indicadores

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								

Legenda: KMO: Kaiser-Meyer-Olkin; AC: Alfa de Cronbach; Seq Afirm: Sequencial das afirmativas do instrumento
Fonte: Dados da pesquisa (2026)