



## MATURIDADE DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO EM INSTITUIÇÃO BRASILEIRA DE EDUCAÇÃO BÁSICA

Flávio Medeiros Mariz<sup>1</sup>; Rosalvo Ermes Streit<sup>2</sup> Ana Paula Bernardi da Silva<sup>3</sup>, Hércules  
Antonio do Prado<sup>4</sup>

<sup>1</sup>Mestrado em Governança, Tecnologia e Inovação – Universidade Católica de Brasília;

<sup>2</sup>Mestrado em Governança, Tecnologia e Inovação – Universidade Católica de Brasília.

<sup>3</sup>Mestrado em Governança, Tecnologia e Inovação – Universidade Católica de Brasília;

<sup>4</sup>Mestrado em Governança, Tecnologia e Inovação – Universidade Católica de Brasília.

E-mail: flaviomariz@gmail.com; rosalvo.streit@gmail.com; ana.bernardi@p.ucb.br;  
herculesp@p.ucb.br.

### RESUMO

A digitalização das escolas ampliou os riscos ao tratamento de dados e tornou a Governança da Segurança da Informação (GSI) uma dimensão estratégica das políticas educacionais. Esta pesquisa determinou o nível de maturidade em GSI de uma Rede de Escolas de Educação Básica. Em estudo quantitativo e exploratório-descritivo, aplicou-se o questionário do Cybersecurity Framework 2.0 do NIST, com 106 afirmativas em escala Likert, traduzido e validado, a 118 profissionais de Tecnologia da Informação. Os indicadores atenderam aos critérios de KMO, Alfa de Cronbach e r de Pearson, e o nível foi definido pela Média e pelo intervalo de confiança de 95%. A Rede situa-se no nível 2, Informado por Risco, com a região Norte no nível 1, Parcial, e a Governança como a dimensão mais frágil. As ações de elevação foram consolidadas em um manual de diagnóstico e em uma aplicação web derivada, que automatiza a tabulação e o acompanhamento.

**Palavras-chave:** Governança da Segurança da Informação. Educação Básica. LGPD. Políticas de Segurança. Capacitação.

### INTRODUÇÃO

A transformação digital das instituições educacionais brasileiras trouxe, além de modernização, vulnerabilidades associadas ao tratamento inadequado de dados. O setor de educação foi o terceiro mais visado por ataques cibernéticos no segundo trimestre de 2024 (Microsoft, 2024). No Brasil, a Lei Geral de Proteção de Dados Pessoais (Brasil, 2018) impõe às instituições de ensino obrigações complexas (Pereira & Lima, 2022), especialmente no tratamento de dados de menores de idade.

Nesse cenário, a Governança da Segurança da Informação (GSI) transcende a perspectiva meramente técnica e se estabelece como abordagem sistêmica que articula identificação, proteção, detecção, resposta e recuperação de incidentes cibernéticos, alinhada aos objetivos educacionais. Modelos de maturidade permitem avaliar as práticas de segurança da informação e orientar melhorias (Araujo et al., 2025). Contudo, uma revisão conduzida nesta pesquisa nas bases Lens, Scopus e Mendeley, da qual resultaram 15 estudos, não identificou artigos que tratem do uso sistemático de um *framework* de GSI orientado à Educação Básica, o que corrobora a escassez de pesquisa empírica sobre riscos de cibersegurança apontada para o ensino superior por Bittencourt et al. (2024). Aferições de maturidade com o Cybersecurity Framework (CSF) do National Institute of Standards and Technology (NIST) existem em outros contextos, como em empresas de Portugal (Bernardo, 2024; Bernardo et al., 2025), avaliadas com o CSF 1.1.



Diante dessa lacuna, adotou-se o CSF 2.0 (NIST, 2024), versão que destaca a governança e se aplica a organizações de todos os portes e setores, para responder à questão: qual é o nível de maturidade em GSI de uma Rede de Escolas de Educação Básica? O objetivo geral foi determinar o nível de maturidade em GSI dessa Rede, em estudo piloto.

## OBJETIVO

O objetivo geral foi determinar o nível de maturidade em Governança da Segurança da Informação de uma Rede de Escolas de Educação Básica. Como objetivos específicos, buscou-se: (a) identificar, no âmbito da cibersegurança, a perspectiva de profissionais de Tecnologia da Informação da Rede; (b) examinar, no âmbito das perspectivas apreendidas, as dimensões da cibersegurança por região geográfica; e (c) avaliar o nível de maturidade em GSI da Rede.

## MÉTODO

Trata-se de pesquisa quantitativa, de caráter exploratório-descritivo. O lócus é uma Rede de Escolas de Educação Básica com 98 Unidades, privadas e sociais, nas cinco regiões do Brasil. O instrumento foi o questionário do CSF 2.0 (NIST, 2024), com 106 afirmativas em 22 categorias e seis funções, aqui denominadas dimensões: Governança (GV), Identificar (ID), Proteger (PR), Detectar (DE), Responder (RS) e Recuperar (RC). As afirmativas, respondidas em escala do tipo Likert de cinco pontos, foram traduzidas para o português, submetidas a validação nomológica por especialista em GSI conhecedor do CSF 2.0 e a pré-teste com especialistas em Segurança da Informação. A aplicação ocorreu por meio do Google Forms, de 20 a 23 de janeiro de 2026, mediante Termo de Consentimento Livre e Esclarecido e conforme a Resolução nº 510/2016 do Conselho Nacional de Saúde.

A população compreendeu os 139 profissionais de Tecnologia da Informação da Rede, 98 nas Unidades e 41 na área corporativa; a amostra mínima estimada foi de 103 respondentes (confiança de 95%; erro de 5%) e obtiveram-se 118 respostas, sem *outliers* (Hair et al., 2009). Os 28 indicadores (22 categorias e seis dimensões) foram constituídos conforme Hair et al. (2009): dimensionalidade pelo critério de Kaiser-Meyer-Olkin, com KMO não inferior a 0,50 (Damásio, 2012); confiabilidade pelo Alfa de Cronbach superior a 0,51 (Gliem & Gliem, 2003); e validade pelo *r* de Pearson positivo com *p*-valor inferior a 0,05 (Formiga et al., 2018). Calcularam-se, no RStudio, Média, desvio-padrão e intervalo de confiança de 95% (IC 95%) por categoria, dimensão e região.

Como o CSF 2.0 não traz mecanismo para mensurar seus quatro níveis (Bernardo et al., 2025), a Média foi associada a eles, acrescidos de um nível zero introduzido nesta pesquisa conforme os cinco níveis de Bernardo (2024) e Bernardo et al. (2025): 0, Inexistente (1,00 a 1,99); 1, Parcial (2,00 a 2,99); 2, Informado por Risco (3,00 a 3,99); 3, Repetível (4,00 a 4,99); e 4, Adaptativo (5,00). Uma dimensão só alcança um nível quando sua Média e seu IC 95% permanecem na faixa correspondente, e a maturidade geral é o menor nível entre as seis dimensões. As ações de elevação foram extraídas dos exemplos de implementação do CSF 2.0 (NIST, 2025), conforme o nível atual de cada região.

## RESULTADOS

Todos os 28 indicadores atenderam ao crivo estatístico (KMO de 0,51, nas categorias com duas afirmativas, a 0,95; Alfa de Cronbach de 0,82 a 0,97; *r* de Pearson positivo com *p*-valor inferior a 0,05). A Tabela 1 apresenta as Médias das dimensões por região e na Rede.

Quanto às dimensões por região (objetivo b), a região Norte apresentou as menores Médias em cinco das seis dimensões e em 12 das 22 categorias. Nessa região (*n* = 6), os intervalos são amplos: Detectar (Média de 3,64; IC 95% de 2,76 a 4,51) e Proteger (3,73; 2,96 a 4,51) alcançam a faixa do



nível um, o que a posiciona no nível 1, Parcial; três dos seis respondentes atuam há menos de 12 meses, o que sugere alta rotatividade. As regiões Centro-Oeste, Nordeste, Sudeste e Sul situam-se no nível 2, Informado por Risco. Foram delineadas 19 ações para a região Norte, visando ao nível dois, e, visando ao nível três, 44 para o Centro-Oeste, 51 para o Nordeste, 30 para o Sudeste e 45 para o Sul.

**Tabela 1**

*Médias das dimensões do CSF 2.0 por região e na Rede, IC 95% e nível de maturidade*

| Dimensão                   | C.-Oeste | Nordeste | Norte    | Sudeste  | Sul      | Rede     | IC 95% (Rede) | Nível    |
|----------------------------|----------|----------|----------|----------|----------|----------|---------------|----------|
| Respondentes (n)           | 29       | 29       | 6        | 23       | 31       | 118      | –             | –        |
| Governança (GV)            | 3,91     | 3,77     | 3,76     | 3,95     | 3,87     | 3,86     | [3,70; 4,03]  | 2        |
| Identificar (ID)           | 4,02     | 4,11     | 4,09     | 4,14     | 4,05     | 4,08     | [3,92; 4,23]  | 2        |
| Proteger (PR)              | 4,21     | 4,03     | 3,73     | 4,16     | 4,17     | 4,12     | [3,97; 4,28]  | 2        |
| Detectar (DE)              | 4,14     | 3,93     | 3,64     | 4,09     | 4,11     | 4,05     | [3,88; 4,21]  | 2        |
| Responder (RS)             | 4,04     | 4,13     | 3,78     | 4,16     | 4,00     | 4,06     | [3,90; 4,22]  | 2        |
| Recuperar (RC)             | 3,99     | 4,12     | 3,73     | 4,13     | 4,04     | 4,05     | [3,90; 4,20]  | 2        |
| <b>Nível de maturidade</b> | <b>2</b> | <b>2</b> | <b>1</b> | <b>2</b> | <b>2</b> | <b>–</b> | <b>–</b>      | <b>2</b> |

*Nota.* C.-Oeste = Centro-Oeste; n = número de respondentes; IC 95% = intervalo de confiança de 95%; nível 1 = Parcial; nível 2 = Informado por Risco. O nível é atribuído pela Média e pelo IC 95%, e a maturidade geral é o menor nível entre as dimensões.

Fonte: Dados da pesquisa (2026).

Quanto ao nível da Rede (objetivo c), Governança tem a menor Média (3,86), influenciada pelas categorias Gestão de Riscos de Cibersegurança na Cadeia de Suprimentos (3,77) e Funções, Responsabilidades e Autoridades (3,84), e Proteger, a maior (4,12); apenas as categorias Gestão de Identidade, Autenticação e Controle de Acesso (4,27) e Segurança de Dados (4,22) mantêm o IC 95% acima de 4,00, alcançando o nível três. Como cada dimensão permanece no nível dois, a Rede situa-se no nível 2, Informado por Risco: as práticas de gestão de riscos são aprovadas pela administração, mas podem não estar estabelecidas como política organizacional (NIST, 2024).

## CONCLUSÃO

Em resposta à questão de pesquisa, a maturidade em GSI da Rede corresponde ao nível 1, Parcial, na região Norte, e ao nível 2, Informado por Risco, nas demais regiões e na Rede como um todo. A Rede dedica-se à proteção, mas tende a negligenciar a governança; a elevação ao nível três exige a promoção da GSI com maior amplitude organizacional. As ações delineadas devem ser adotadas regionalmente e promovidas de forma constante, repetível e proativa.

No plano científico, a pesquisa contribui para reduzir a lacuna de estudos sobre o uso de *framework* de GSI na Educação Básica e disponibiliza o questionário do CSF 2.0 traduzido e com indicadores validados. No plano tecnológico, gerou o Produto Técnico-Tecnológico *Manual para Diagnóstico da Maturidade em Governança da Segurança da Informação em Instituições de Educação Básica*, tipificado como Manual/Protocolo, com instrumento de diagnóstico, protocolo de aplicação institucional e guia de análise e planejamento de ações. Como desdobramento, o manual foi implementado em uma aplicação web que automatiza a coleta anônima por ciclos, a tabulação e o crivo estatístico, o plano de elevação com as ações do manual, o registro das ações adotadas e a evolução entre ciclos.



As limitações compreendem a impossibilidade de generalização, a perspectiva restrita aos profissionais de tecnologia e o número reduzido de respondentes na região Norte (seis). Sugere-se aplicar o instrumento a todos os funcionários da Rede e a outras redes de Educação Básica.

## REFERÊNCIAS

- 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), e8480. <https://ojs.cuadernoseducacion.com/ojs/index.php/ced/article/view/8480>
- 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.ipv.pt/bitstream/20.500.11960/3989/1/Luis\\_Bernardo.pdf](http://repositorio.ipv.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), 1364. <https://doi.org/10.3390/electronics14071364>
- Bittencourt, O. T., Carvalho, R. L. de, Barbosa, G. V., & Santos, G. F. do. (2024). Segurança cibernética nas universidades: Uma revisão sistemática da literatura sobre a gestão de segurança da informação no ensino superior. *InterSciencePlace*, 19, 160–174. <https://www.interscienceplace.org/index.php/isp/article/view/723/246>
- Brasil. (2018). *Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União. [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)
- Damásio, B. F. (2012). Uso da análise fatorial exploratória em psicologia. *Avaliação Psicológica*, 11(2), 213–227.
- Formiga, N. S., Miranda, A. L. B. B., Araújo, I. T. de, Pastana, S. T. G., & Mafra, A. L. (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.
- Gliem, J. A., & Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. In *Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education* (pp. 82–88).
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Análise multivariada de dados* (6ª ed.). Bookman.
- Microsoft. (2024, 10 de outubro). *Cyber Signals, 8ª edição: Educação sob cerco – como os cibercriminosos têm escolas como alvo*. <https://news.microsoft.com/source/latam/features/seguranca/cyber-signals-8a-edicao-educacao-sob-cerco-como-os-cibercriminosos-tem-como-alvo-escolas/>
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. <https://doi.org/10.6028/NIST.CSWP.29>
- National Institute of Standards and Technology. (2025). *CSF 2.0 implementation examples*. <https://www.nist.gov/document/csf-20-implementation-examples-xlsx>
- Pereira, M. R., & Lima, T. C. (2022). A proteção de dados de menores de idade à luz da LGPD: Desafios para as instituições de ensino. *Revista Brasileira de Direito da Criança e do Adolescente*, 18(1), 109–127. <https://doi.org/10.11606/issn.2359-5702.v18i1p109-127>

**Financiamento:** Não houve financiamento.