# SEGURANÇA CIBERNÉTICA NO BRASIL: EVOLUÇÃO DOS ATAQUES E ESTUDO DE CASO EM UMA ESCOLA DE PORTO NACIONAL (TO)

Sabriny Neres Rodrigues - Estudante do Curso Superior de Bacharelado em Sistemas de Informação – IFTO Porto Nacional. e-mail: sabriny.rodrigues@estudante.ifto.edu.br;
Luciano Correia Franco - Docente do Curso Superior de Bacharelado em Sistemas de Informação – IFTO Porto Nacional. Orientador. e-mail: lucianofranco@ifto.edu.br.

## 1 INTRODUÇÃO

O avanço contínuo das Tecnologias da Informação e Comunicação (TIC) tem proporcionado benefícios expressivos, como maior conectividade, acesso facilitado à informação e automação de processos em diversos setores. No entanto, esse progresso também ampliou os desafios relacionados à segurança digital, uma vez que o aumento da acessibilidade e da agilidade nos processos exige maior atenção à proteção de dados e à segurança dos usuários. Conforme destacam Ferreira e André (2018), desde o início dos anos 2000, os desafios da cibersegurança no Brasil têm se intensificado, com ataques cada vez mais sofisticados explorando vulnerabilidades em redes, sistemas e dispositivos conectados. Nesse contexto, Leal (2011) defende que a segurança da informação deve ser abordada com foco na gestão de riscos, mediante a implementação de políticas adequadas de proteção.

Entre os setores mais vulneráveis a essas ameaças estão as instituições educacionais, especialmente as públicas de pequeno e médio porte, que frequentemente carecem de políticas robustas de segurança, de treinamentos para conscientização de usuários e de protocolos formais de resposta a incidentes. Ataques como *phishing*, *malware* e *ransomware* representam riscos significativos à integridade e confidencialidade das informações escolares. O Tribunal de Contas da União (2012) enfatiza que boas práticas em segurança da informação são essenciais para proteger dados sensíveis e garantir a continuidade dos serviços nas instituições públicas.

Pesquisas recentes, como a de Souza, Gomes e Silva (2023), evidenciam que dispositivos IoT presentes nas escolas — incluindo *smart* TVs, câmeras de vigilância e lousas digitais — compartilham vulnerabilidades comuns, como *firmware* desatualizado e uso de credenciais padrão, aumentando a superfície de ataque. Esses problemas, longe de serem casos isolados, integram um cenário sistêmico que demanda soluções integradas e sustentáveis.

Diante desse panorama, este estudo busca suprir a carência de pesquisas sobre vulnerabilidade cibernética no ambiente escolar, com foco na Escola Estadual Girassol de Tempo Integral Irmã Aspásia, situada em Porto Nacional. Por se tratar de uma instituição pública de pequeno porte, ela exemplifica a realidade de muitas escolas que permanecem à margem de políticas públicas estruturadas de segurança digital. A pesquisa procura responder às seguintes questões: quais estratégias a escola utiliza para proteção digital e quais seus impactos na integridade das informações? Quais são as ameaças mais frequentes? Quais os mecanismos de ação dos atacantes? E, por fim, como prevenir e reagir diante de uma ameaça materializada? Estas respostas podem contribuir para a

formulação de diretrizes capazes de fortalecer a segurança digital nas instituições públicas de ensino, e promover um ambiente educacional mais seguro e resiliente frente aos desafios tecnológicos.

## 2 OBJETIVO

Analisar o histórico e a evolução dos principais incidentes de ataques cibernéticos no Brasil e a percepção dos usuários de uma escola pública de Porto Nacional – TO, contribuindo para a formulação de diretrizes capazes de fortalecer a segurança digital nas instituições públicas de ensino.

## 3 MATERIAL E MÉTODOS

Este trabalho caracteriza-se como uma pesquisa descritiva, aplicada, documental e bibliográfica, estruturada como estudo de caso na Escola Estadual Girassol de Tempo Integral Irmã Aspásia, em Porto Nacional – TO. A investigação adotou abordagem quantitativa, com aplicação de *survey* estruturado via questionário digital, conforme a proposta metodológica de Minayo (2010) e as diretrizes de Gil (2008) e Barbin (2006), visando levantar dados objetivos sobre percepções, práticas e experiências relacionadas à segurança cibernética no ambiente escolar.

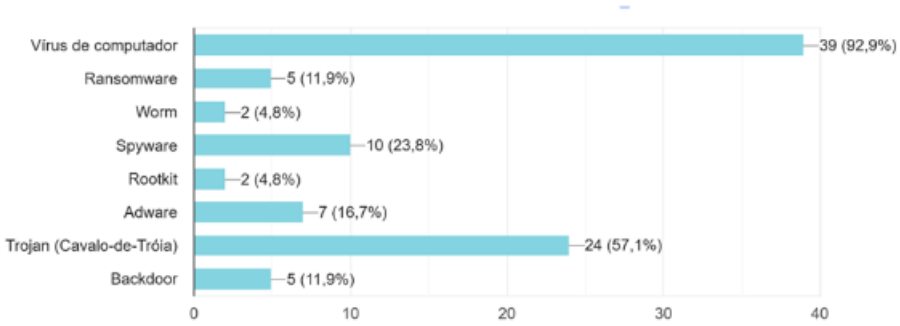
A amostra foi composta por 42 servidores públicos educacionais, selecionados mediante critérios de inclusão relacionados à atuação com Tecnologias da Informação e Comunicação (TICs) e consentimento formal. O questionário abordou três dimensões: (1) conhecimento sobre segurança cibernética; (2) práticas digitais seguras; e (3) experiências com ameaças e ataques virtuais.

Os dados foram analisados por meio de estatística descritiva, com apresentação em gráficos e tabelas, possibilitando identificar padrões comportamentais e lacunas no conhecimento dos participantes. A metodologia adotada confere validade científica e aplicabilidade prática aos resultados, contribuindo para o fortalecimento das estratégias de proteção cibernética no contexto educacional.

## 4 RESULTADOS E DISCUSSÃO

As respostas ao questionário foram organizadas em 14 gráficos e uma tabela-síntese, permitindo mapear tanto o nível de conhecimento técnico quanto o comportamento digital dos participantes. A análise mostra que, embora a maioria tenha ouvido falar sobre segurança da informação, o conhecimento técnico é limitado, especialmente em ameaças modernas como *ransomware* (reconhecido por apenas 11,9% dos docentes) e ataques DoS/DDoS (4,8%). Esse dado corrobora a afirmação de Oliveira *et al*. (2019) de que “o termo técnico muitas vezes não é assimilado pelo usuário comum, o que dificulta a detecção e resposta a incidentes”.

**Figura 1 –** Conhecimento dos servidores de termos associados a códigos maliciosos.




Fonte: elaborado pela autora, 2025.

Além disso, 54,8% dos entrevistados afirmaram já ter sido vítimas ou conhecer alguém que sofreu um ataque cibernético, relatando casos de *links* fraudulentos, roubo de credenciais e compras em sites falsos. Essa tendência confirma o que Pereira e Costa (2020) definem como engenharia social: ataques que exploram a confiança e o comportamento humano mais do que falhas técnicas.

Um dos pontos críticos revelados foi a gestão de senhas: parte expressiva dos participantes ainda utiliza senhas fracas ou repetidas, expondo-se a riscos. Segundo o Relatório de Segurança Cibernética no Brasil (Brasil, 2023), mais de 60% dos incidentes em órgãos públicos envolvem credenciais vulneráveis.

A frequência de atualização de *softwares* também preocupa: muitos docentes realizam atualizações apenas esporadicamente, permitindo que vulnerabilidades conhecidas permaneçam exploráveis. Conforme Costa e Souza (2022), “atualizações não apenas corrigem falhas, mas adaptam os sistemas aos padrões de ataque mais recentes”.

Por fim, quanto ao uso de *softwares* originais, parte significativa acredita que a instituição adota apenas programas licenciados, mas estudos como o de Silva e Morais (2024) mostram que, em muitas escolas, há setores operando com *softwares* piratas, o que eleva exponencialmente o risco de infecção. Sugestões propostas pelo estudo:

1. Implantar políticas internas formais de segurança da informação, alinhadas à NBR 27002.
2. Treinamentos periódicos para docentes e servidores sobre identificação de ameaças, criação de senhas seguras e uso responsável das TICs.
3. Atualização contínua de sistemas e *softwares*, com uso exclusivo de programas licenciados.
4. Protocolos claros de resposta a incidentes, *backups* regulares e planos de contingência.
5. Capacitação sobre LGPD, destacando responsabilidades legais na proteção de dados de alunos e funcionários.

Com base nesses resultados, conclui-se que o fortalecimento da cultura de segurança digital na escola é essencial e deve envolver ação coordenada entre gestão, professores e órgãos públicos,

garantindo confidencialidade, integridade e disponibilidade das informações, conforme os pilares da segurança da informação.

## 5 CONSIDERAÇÕES FINAIS

Os resultados indicaram lacunas importantes, como o uso frequente de senhas fracas, baixa atualização de *softwares*, falta de conhecimento aprofundado sobre ameaças como *phishing* e *malwares*, além da ausência de protocolos institucionais para lidar com incidentes cibernéticos. A maioria dos docentes reconhece a importância da segurança digital, mas poucos adotam medidas efetivas ou receberam treinamento específico.

Concluiu-se que a segurança cibernética na escola está em estágio inicial, evidenciando a necessidade de políticas de capacitação, infraestrutura adequada e uma cultura organizacional focada na proteção digital. O estudo ressalta a urgência de incluir a segurança cibernética nas políticas educacionais e recomenda aprofundar futuras pesquisas sobre formação docente e análises comparativas entre escolas para fortalecer a proteção digital no sistema educacional brasileiro.

## 6 AGRADECIMENTOS

Agradecemos a Escola Estadual Girassol de Tempo Integral Irmã Aspásia e ao IFTO, em Porto Nacional, pelo apoio na execução do projeto, que viabilizou a realização desta pesquisa.

## REFERÊNCIAS

BARBIN, A. ***Pesquisa Quantitativa: Planejamento e Execução***. São Paulo: Atlas, 2006.

BRASIL, MC. ***Relatório de Segurança Cibernética no Brasil – 2023***. Disponível em: https://www.gov.br/mcom. Acesso em: 09 fev. 2025.

COSTA, R.; SOUZA, A. ***Inteligência Artificial na Prevenção de Ataques Cibernéticos: Tendências e Desafios***. *Journal of Advanced Cybersecurity*, v. 10, n. 4, p. 134-150, 2022.

FERREIRA, L.; LIMA, M. ***Impacto Legal dos Ataques Cibernéticos no Brasil: A LGPD em Foco***. Direito Digital, v. 6, n. 2, p. 88-105, 2021.

GIL, A. C. ***Métodos e Técnicas de Pesquisa Social***. 6. ed. São Paulo: Atlas, 2008.

LEAL, M. ***Segurança da Informação: Uma Abordagem Focada em Gestão de Risco***. Olinda: Tarcísio, 2011. 150 p.

MINAYO, M. C. ***Desafio do Conhecimento: Pesquisa Qualitativa em Saúde***. 11. ed. São Paulo: Hucitec, 2010.

OLIVEIRA, J. et al. ***Ameaças Cibernéticas no Ambiente Escolar: Um Estudo de Caso. Educação e Tecnologia***, v. 12, n. 4, p. 78-95, 2019.

PEREIRA, A.; COSTA, R. ***Engenharia Social e Ataques Cibernéticos: Como Proteger as Instituições Educacionais***. Revista de Segurança Digital, v. 7, n. 1, p. 23-40, 2020.

BRASIL, TCU. ***Boas Práticas em Segurança da Informação***. Brasília: TCU, 2023.