TECNOLOGIA E CUIDADO: INCLUSÃO DIGITAL E SEGURANÇA DA INFORMAÇÃO NO COLÉGIO TIRADENTES – DIAGNÓSTICO DE INFRAESTRUTURA E CURRICULARIZAÇÃO DA EXTENSÃO

TECHNOLOGY AND CARE: DIGITAL INCLUSION AND INFORMATION SECURITY AT COLÉGIO TIRADENTES – INFRASTRUCTURE ASSESSMENT AND EXTENSION CURRICULARIZATION

Amanda Carvalho Siqueira Tomaz[1]

Ana Clara Santana da Silva[2]

Mateus Haffermann Farias[3]

Ronivaldo da Silva Lima[4]

Sabrina Cabral Santos[5]

Tatiana Aparecida Caliman Lima[6]

Andréia Mendonça dos Santos Lima[7]

Ilma Rodrigues de Souza Fausto[8]

RESUMO EXPANDIDO

O projeto de curricularização da extensão intitulado “Tecnologia e Cuidado: Inclusão Digital e Segurança da Informação” foi desenvolvido no Colégio Tiradentes da Polícia Militar – CTPM IV, localizado em Ji-Paraná, com a participação de estudantes do curso de Análise e Desenvolvimento de Sistemas do Instituto Federal de Rondônia (IFRO).

[1] Acadêmica do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email amanda.tomaz@estudante.ifro.edu.br

[2] Acadêmica do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email anaclarasantanadasilva37@gmail.com

[3] Acadêmica do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email mateushaffmain@gmail.com

[4] Acadêmica do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email ronivaldo.slima@gmail.com

[5] Acadêmica do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email sabrinacabral659@gmail.com

[6] Acadêmica do curso uperior de Tecnologia em Análise e Desenvolvimento de Sistemas - Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO. Email tatiana.caliman.lima@gmail.com

[7] Orientadora, Professora EBTT em Regime de Dedicação Exclusiva no Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO E-mail: andreiamendonsa@ifro.edu.br

[8] Orientadora, Professora EBTT em Regime de Dedicação Exclusiva no Instituto de Educação, Ciência e Tecnologia de Rondônia - IFRO/Campus - Ji-Paraná-RO - Orientadora, Doutora, *e-mail*: ilma.rodrigues@ifro.edu.br.

A proposta surgiu da necessidade de aproximar os conhecimentos técnicos adquiridos na formação acadêmica à realidade social, promovendo melhorias na infraestrutura tecnológica da escola, capacitação digital de servidores e alunos e implementação de boas práticas de segurança da informação. Essa iniciativa está alinhada aos princípios da extensão universitária, que preconizam a integração entre ensino, pesquisa e extensão, e contribui para a formação cidadã dos estudantes, conforme estabelece a Resolução CNE/CES nº 7/2018. A justificativa para a execução do projeto fundamenta-se na urgência de promover a equidade educacional por meio da inclusão digital e da segurança da informação. Estudos recentes apontam que a falta de infraestrutura tecnológica adequada e a ausência de formação docente específica constituem barreiras significativas para a efetiva integração das Tecnologias Digitais da Informação e Comunicação (TDICs) no ensino (Silva & Pacheco, 2025; Loureiro et al., 2023). Nesse contexto, a curricularização da extensão representa uma oportunidade ímpar para que os estudantes desenvolvam competências técnicas e socioemocionais em situações reais, fortalecendo sua formação integral e contribuindo para o desenvolvimento da comunidade. Segundo Fontenele (2024), a extensão universitária deve ser compreendida como uma prática pedagógica transformadora, capaz de articular saberes acadêmicos e populares, promovendo mudanças concretas na sociedade. Outro aspecto relevante é a segurança da informação, tema cada vez mais presente no ambiente educacional, especialmente após a vigência da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). A implementação de boas práticas de segurança digital nas escolas é fundamental para proteger dados sensíveis e garantir a privacidade dos usuários, evitando vulnerabilidades que possam comprometer a integridade das informações (Gomes & Andriola, 2023). De acordo com Stallings (2020), a segurança da informação deve ser tratada como um componente estratégico da gestão de tecnologia, envolvendo políticas, processos e ferramentas que assegurem a confidencialidade, integridade e disponibilidade dos dados. A fundamentação teórica do projeto está ancorada em três pilares: inclusão digital, segurança da informação e curricularização da extensão. A inclusão digital é entendida como um processo de democratização do acesso às tecnologias da informação e comunicação, essencial para a equidade educacional. Castells (2003) destaca que o acesso à informação é um dos principais fatores de desenvolvimento social na era digital, sendo indispensável para a participação cidadã e para a redução das desigualdades. A curricularização da extensão, por sua vez, é um mecanismo que possibilita aos estudantes vivenciar experiências práticas, aproximando-os da realidade social e fortalecendo sua formação cidadã (Santos & Almeida, 2025). A Meta 1 do projeto consistiu no levantamento detalhado de hardware, software e rede do laboratório de informática do CTPM IV, com o objetivo de identificar pontos críticos e propor soluções para otimizar o uso dos recursos disponíveis. Essa etapa foi realizada por meio de uma visita técnica em 06 de outubro de 2025, conduzida por seis alunos do curso de Análise e Desenvolvimento de Sistemas, sob a coordenação da professora responsável pelo projeto. A metodologia envolveu observação direta, testes de funcionamento dos equipamentos e entrevistas com docentes e equipe administrativa, permitindo uma análise abrangente das condições atuais do laboratório. Os resultados do levantamento revelaram um cenário desafiador. Em relação à infraestrutura, constatou-se que a escola possui acesso à

internet com velocidade contratada de 1GB, porém os switches instalados são Fast Ethernet (/100), o que limita a taxa de transferência e compromete o desempenho da rede. Além disso, os cabos de rede são do tipo CAT4, com aproximadamente cinco anos de uso, apresentando sinais de desgaste e mau contato em algumas conexões. A organização dos cabos de energia e rede mostrou-se inadequada, gerando riscos de acidentes e interferências no funcionamento dos equipamentos. Embora haja nobreaks instalados, não foi possível verificar seu funcionamento completo durante a visita. No que se refere aos equipamentos, os computadores disponíveis são da marca Positivo, com monitores Samsung. Diversos gabinetes apresentam desgaste físico e sinais de uso prolongado, indicando a necessidade de manutenção preventiva. Foi identificado um número significativo de máquinas com problemas de inicialização, ausência de sistema operacional ou falhas de disco rígido, o que reduz consideravelmente a disponibilidade de recursos para as aulas práticas. Algumas estações possuem hardware instalado, mas não estão operacionais devido a defeitos em HDs ou ausência de manutenção adequada. A análise do software e da segurança digital revelou fragilidades importantes. Não há restrições de acesso a sites ou downloads, expondo a rede a riscos de segurança. Além disso, não foi identificada a presença de antivírus instalado ou atualizado nas máquinas em funcionamento, aumentando a vulnerabilidade a ataques cibernéticos. Outro ponto crítico é a ausência de política de backup, tanto local quanto em nuvem, o que compromete a integridade dos dados em caso de falhas ou incidentes. Também não existem perfis de usuário com restrições, permitindo acessos irrestritos que podem resultar em uso inadequado dos recursos. Esses achados evidenciam que, embora a escola disponha de recursos básicos para atividades de informática, a falta de manutenção periódica e atualização tecnológica compromete a eficiência do laboratório. A discrepância entre a velocidade contratada da internet e a capacidade dos dispositivos de rede é um fator limitante para o desempenho das atividades online. Além disso, a ausência de práticas de segurança digital coloca em risco dados sensíveis, especialmente considerando as exigências da LGPD. Outro aspecto preocupante é a falta de políticas de gestão de TI, como controle de acessos, atualização de sistemas e capacitação dos usuários, o que reforça a necessidade de ações integradas que envolvam não apenas a manutenção física dos equipamentos, mas também a implementação de medidas de segurança e formação continuada. Com base no diagnóstico, foram propostas ações para reverter esse cenário. Entre as recomendações, destacam-se a substituição de HDs e SSDs danificados, instalação de sistemas operacionais e antivírus, troca de pasta térmica e limpeza interna dos gabinetes, teste e substituição de cabos de rede com mau contato e reorganização dos cabos com identificação por etiquetas. No âmbito da segurança, sugere-se a aplicação de boas práticas de segurança da informação, criação de perfis de usuário com restrições básicas e implementação de política de backup local e em nuvem. Além disso, serão realizadas oficinas com servidores e alunos sobre uso seguro da internet, ferramentas digitais e pesquisa com inteligência artificial, visando à formação de uma cultura de boas práticas digitais.

Para viabilizar essas ações, foi elaborada uma lista de materiais e serviços com custo estimado de R$ 5.000,00, incluindo SSDs e HDs para substituição, cabos SATA e de rede, ferramentas para manutenção, materiais para limpeza e organização e impressão de materiais didáticos para as oficinas. A execução dessas medidas deverá

resultar em melhorias significativas na infraestrutura tecnológica do laboratório, aumento da disponibilidade de equipamentos para uso pedagógico, redução de riscos relacionados à segurança da informação e fortalecimento da integração entre ensino e extensão, promovendo a formação cidadã dos estudantes. A Meta 1 do projeto revelou um cenário desafiador, mas também uma oportunidade de transformação. A intervenção planejada não se limita à manutenção física dos equipamentos; ela envolve a implementação de políticas de segurança, capacitação de usuários e promoção da inclusão digital. Essa abordagem integrada está em consonância com os princípios da extensão universitária e contribui para a construção de uma escola mais segura, eficiente e preparada para os desafios da era digital. Ao aproximar os estudantes da realidade social e permitir que eles apliquem seus conhecimentos em situações concretas, o projeto reafirma o papel da extensão como prática pedagógica transformadora, capaz de promover mudanças significativas na comunidade e na formação acadêmica.

Palavras-chave: Inclusão digital; Segurança da informação; Infraestrutura tecnológica; Levantamento de hardware; Rede de computadores; Educação tecnológica; LGPD;

Expanded Abstract

The extension curricularization project entitled *"Technology and Care: Digital Inclusion and Information Security"* was developed at Colégio Tiradentes da Polícia Militar – CTPM IV, located in Ji-Paraná, with the participation of students from the Systems Analysis and Development program at the Federal Institute of Rondônia (IFRO). The proposal arose from the need to bridge the gap between technical knowledge acquired in academic training and real-world social contexts, promoting improvements in the school's technological infrastructure, digital training for staff and students, and the implementation of best practices in information security. This initiative aligns with the principles of university extension, which advocate for the integration of teaching, research, and outreach, and contributes to students' civic education, as established by Resolution CNE/CES No. 7/2018. The rationale for implementing the project is based on the urgency of promoting educational equity through digital inclusion and information security. Recent studies indicate that the lack of adequate technological infrastructure and the absence of specific teacher training are significant barriers to the effective integration of Digital Information and Communication Technologies (DICTs) in education (Silva & Pacheco, 2025; Loureiro et al., 2023). In this context, extension curricularization represents a unique opportunity for students to develop technical and socio-emotional skills in real-life situations, strengthening their comprehensive education and contributing to community development. According to Fontenele (2024), university extension should be understood as a transformative pedagogical practice capable of articulating academic and popular knowledge, promoting tangible changes in society. Another relevant aspect is information security, an increasingly critical topic in educational environments, especially after the enactment of the General Data Protection Law (Law No. 13,709/2018). Implementing sound digital security practices in schools is essential to protect sensitive data and ensure user privacy, preventing vulnerabilities that could compromise information integrity (Gomes & Andriola, 2023). As Stallings (2020) points out, information security must be treated as a strategic component of technology management, involving policies, processes, and tools that guarantee data confidentiality, integrity, and availability. The theoretical foundation of the project rests on three pillars: digital inclusion, information security, and extension

curricularization. Digital inclusion is understood as the process of democratizing access to information and communication technologies, which is essential for educational equity. Castells (2003) emphasizes that access to information is one of the main drivers of social development in the digital age, being indispensable for civic participation and reducing inequalities. Extension curricularization, in turn, is a mechanism that enables students to experience practical situations, bringing them closer to social realities and strengthening their civic education (Santos & Almeida, 2025). Project Goal 1 consisted of a detailed survey of hardware, software, and network infrastructure in the CTPM IV computer lab, aiming to identify critical points and propose solutions to optimize resource utilization. This stage was carried out through a technical visit on October 6, 2025, conducted by six students from the Systems Analysis and Development program under the supervision of the project coordinator. The methodology involved direct observation, equipment functionality tests, and interviews with teachers and administrative staff, allowing for a comprehensive analysis of the lab's current conditions. The survey results revealed a challenging scenario. Regarding infrastructure, it was found that the school has contracted internet speed of 1Gbps; however, the installed switches are Fast Ethernet (/100), which limits data transfer rates and compromises network performance. Additionally, the network cables are CAT4, approximately five years old, showing signs of wear and poor contact in some connections. Cable management for power and network lines was inadequate, creating accident risks and interference with equipment operation. Although uninterruptible power supplies (UPS) were present, their full functionality could not be verified during the visit. As for equipment, the available computers are Positivo brand with Samsung monitors. Several cases show physical wear and signs of prolonged use, indicating the need for preventive maintenance. A significant number of machines were found with boot issues, missing operating systems, or hard drive failures, which considerably reduces resource availability for practical classes. Some workstations have installed hardware but are non-operational due to defective hard drives or lack of proper maintenance. The analysis of software and digital security revealed critical weaknesses. There are no restrictions on website access or downloads, exposing the network to security risks. Furthermore, no antivirus software was identified as installed or updated on functioning machines, increasing vulnerability to cyberattacks. Another critical point is the absence of a backup policy, both locally and in the cloud, which compromises data integrity in case of failures or incidents. User profiles with access restrictions are also nonexistent, allowing unrestricted access that can lead to improper resource use. These findings show that, although the school has basic resources for computer-based activities, the lack of regular maintenance and technological updates compromises the lab's efficiency. The discrepancy between contracted internet speed and the capacity of network devices is a limiting factor for online activities. Moreover, the absence of digital security practices puts sensitive data at risk, especially considering LGPD requirements. Another concerning aspect is the lack of IT management policies, such as access control, system updates, and user training, reinforcing the need for integrated actions that involve not only physical equipment maintenance but also the implementation of security measures and continuous education. Based on the diagnosis, actions were proposed to reverse this scenario. Recommendations include replacing damaged HDDs and SSDs, installing operating systems and antivirus software, replacing thermal paste and cleaning internal components, testing and replacing faulty network cables, and reorganizing cables with proper labeling. In terms of security, the application of best practices in information security, creation of user profiles with basic restrictions, and implementation of local and cloud backup policies are suggested. Additionally, workshops will be held for staff and students on safe internet use, digital tools, and AI-based research, aiming to foster a culture of sound digital practices. The implementation of these measures is expected to result in significant improvements in the lab's technological infrastructure, increased availability of equipment for

educational use, reduced risks related to information security, and strengthened integration between teaching and extension, promoting students' civic education. In summary, Goal 1 of the project revealed a challenging scenario but also an opportunity for transformation. The planned intervention goes beyond physical equipment maintenance; it involves implementing security policies, user training, and promoting digital inclusion. This integrated approach aligns with the principles of university extension and contributes to building a safer, more efficient school prepared for the challenges of the digital age.

Keywords: Digital inclusion; Information security; Technological infrastructure; Hardware assessment; Computer networks; Educational technology; LGPD compliance.

REFERÊNCIAS

BRASIL. Resolução CNE/CES nº 7, de 18 de dezembro de 2018.

BRASIL. MEC. Capacitação em tecnologia digital para professores da rede pública. Brasília, 2024.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2003.

DORNELLES DIAS, Adriano Valter et al. *Inclusão digital: garantindo acesso e qualidade na educação*. Porto Alegre: Editora Universitária, 2024.

FONTENELE, Iolanda Carvalho. *A curricularização da extensão no Brasil: história, concepções e desafios*. Fortaleza: EdUECE, 2024.

GOMES, Carlos Adriano Santos; ANDRIOLA, Wagner Bandeira. *Percurso histórico do uso de tecnologias digitais na escola pública brasileira*. Fortaleza: UFC, 2023.

IMPERATORE, Simone Loureiro Brum; PEDDE, Valdir. *Curricularização da extensão universitária no Brasil: questões estruturais e conjunturais*. Porto Alegre: UFRGS, 2023.

SANTOS, Sandra de Faria; ALMEIDA, Luciane Pinho de. *Extensão universitária em seus processos de institucionalidade e curricularização*. Belo Horizonte: UFMG, 2025.

SILVA, Aderson Pereira da; PACHECO, Clécia Simone Gonçalves Rosa. *A Inclusão Digital na Educação: desafios e oportunidades*. Curitiba: Appris, 2025.

STALLINGS, William. *Segurança de redes e sistemas de computadores*. 6. ed. São Paulo: Pearson, 2020.