# SEGURANÇA DE DADOS NA PERIFERIA: PROJETO DE EXTENSÃO UNIVERSITÁRIA PARA ENSINO E CONSCIENTIZAÇÃO EM COMUNIDADES VULNERÁVEIS

## DATA SECURITY IN THE PERIPHERY: UNIVERSITY EXTENSION PROJECT FOR TEACHING AND AWARENESS IN VULNERABLE COMMUNITIES

**Caique Zaneti Kirilo[1], [i]**
**Vinicius De Jesus Silva[2], [ii]**
**Jéssica Franzon Cruz do Espírito Santo[3], [iii]**
**Arthur Gustavo de Araújo Ferreira[4], [iv]**
**Vivian de Oliveira Preto[5], [v]**
**Tiago Augusto Orcajo Demay Cordeiro[6], [vi]**
**Hebert de Oliveira Silva[7], [vii]**
**Emerson Costa Santos[8], [viii]**

## RESUMO

O projeto tem como intuito relatar a experiência de um projeto de extensão universitária que foi voltado à conscientização sobre segurança de dados em uma comunidade periférica de São Paulo. A pesquisa foi conduzida por estudantes de Ciência de Dados em parceria com a ONG Vozes das Periferias. O projeto buscou enfrentar a vulnerabilidade de crianças e adolescentes diante de ameaças como golpes virtuais, desinformação e invasões de privacidade. Foi utilizado design thinking e mapas de empatia para estruturar oficinas adaptadas às necessidades locais, transformando conceitos técnicos complexos em conteúdos acessíveis. Os resultados mostraram que a personalização do conteúdo, a partir da realidade comunitária, potencializou a compreensão e a capacidade de prevenção contra riscos digitais, além de fortalecer a cidadania digital, e para os universitários, a iniciativa trouxe ganhos acadêmicos e sociais, ao integrar teoria, prática e responsabilidade comunitária.

**Palavras-chave:** Segurança de Dados; Cidadania Digital; Letramento Digital

[1]Doutorando e Docente no curso de graduação na Faculdade SENAI-SP de Ciência de Dados, E-mail: caique.zaneti@sp.senai.br
[2]Graduando e Discente do curso de graduação na Faculdade SENAI-SP de Ciência de Dados, E-mail: viniciusdejesussilva12@gmail.com
[3]Mestranda e Docente no curso de graduação na Faculdade SENAI-SP de Ciência de Dados, E-mail: jessica.santo@sp.senai.br
[4]Doutor e Docente no curso de graduação na Faculdade SENAI-SP de Ciência de Dados, E-mail: arthur.ferreira@sp.senai.br
[5] Mestre e Coordenadora dos cursos superiores de Tecnologia em Ciência de Dados e Segurança Cibernética da Faculdade SENAI-SP, E-mail: vpreto@sp.senai.br
[6]Mestre e Docente no curso de graduação na Faculdade SENAI-SP de Segurança Cibernética, E-mail: tiago.demay@sp.senai.br
[7]Doutorando e Docente no curso de graduação na Faculdade SENAI-SP de Segurança Cibernética, E-mail: hebert.oliveira@sp.senai.br
[8]Doutorando e Diretor do Campus Paulo Antônio Skaf, E-mail: emerson@sp.senai.br

## ABSTRACT

The project reports the experience of a university extension initiative focused on digital literacy and raising awareness about data security in peripheral communities of São Paulo. Conducted by Data Science students in partnership with the NGO Vozes das Periferias, the work sought to address the vulnerability of children and adolescents to threats such as online scams, disinformation, and privacy breaches. Grounded in literature on social engineering, malware, and defense practices, the project employed design thinking and empathy maps to structure workshops tailored to local needs, translating complex technical concepts into accessible content and practical activities. The results showed that customizing the content based on the community's reality enhanced both understanding and the ability to prevent digital risks, while also strengthening digital citizenship. The initiative brought academic and social benefits for the university students by integrating theory, practice, and community responsibility.


**Keywords:** Data Security; Digital Citizenship; Digital Literacy.

## 1 INTRODUÇÃO

O processo de digitalização da sociedade tem transformado as interações sociais, o acesso à informação e as oportunidades, atingindo todas as camadas da população, porém, o avanço da inclusão digital, especialmente em comunidades periféricas, frequentemente ocorre de forma desacompanhada de uma educação crítica sobre os riscos inerentes ao ambiente online, expondo crianças e adolescentes a um ecossistema, onde ali tornam-se particularmente vulneráveis a ameaças como golpes, desinformação, exposição indevida e diversas formas de abuso.
Quando falamos de acesso à tecnologia e sobre o conhecimento relacionado à segurança digital, existe uma lacuna criada por problemas sociais enraizados que demandam ações educativas direcionadas.
Este projeto tem como proposta relatar a experiência de uma iniciativa onde estudantes universitários de Ciência de Dados da Escola Senai Paulo Antônio Skaf desenvolveram e aplicaram um programa de conscientização em segurança digital para jovens de uma comunidade em São Paulo, em parceria com a ONG Vozes das Periferias.

### 1.1 Problema de pesquisa

A expansão do acesso digital em comunidades vulneráveis não tem sido acompanhada por uma educação proporcional sobre os riscos online. Essa defasagem cria um cenário em que crianças e adolescentes, apesar de conectados, permanecem despreparados para identificar e se proteger de ameaças como golpes, desinformação e violação de privacidade. O problema central é, portanto, a carência de iniciativas educacionais acessíveis que capacitem este público para um uso seguro e consciente da tecnologia.

### 1.2 Objetivo

O objetivo deste trabalho é descrever e analisar um projeto de extensão universitária

voltado à promoção da conscientização sobre segurança de dados para crianças e adolescentes em situação de vulnerabilidade social, por meio de workshops desenvolvidos e ministrados por discentes do ensino superior.

### 1.3 Justificativa

Este projeto se justifica pela necessidade de mitigar a vulnerabilidade digital de jovens em comunidades periféricas, promovendo a cidadania digital por meio da educação. A iniciativa possui relevância acadêmica e social ao aplicar o conhecimento universitário para gerar impacto real, fortalecendo o papel da instituição de ensino na comunidade e oferecendo um modelo prático e replicável para futuras ações de extensão.

## 2 REVISÃO DE LITERATURA

### 2.1 Engenharia Social: O Fator Humano como Alvo

A segurança digital, quando analisada por um amplo espectro de conectividade, exige a compreensão de um cenário de ameaças em constante evolução, que exploram principalmente as vulnerabilidades humanas.

A base para muitos ataques cibernéticos é a engenharia social, que é definida como a arte da manipulação psicológica com o intuito de enganar indivíduos, levando-os a realizar ações especificamente vantajosas para o golpista ou a divulgar informações confidenciais. Esses ataques não visam apenas falhas técnicas em sistemas computacionais, a engenharia social foca no "fator humano", ela explora falhas do sistema social, como confiança, urgência e medo para induzir o comportamento desejado na vítima (MITNICK; SIMON, 2003).

Ao falarmos sobre tipos de ataques que envolvem engenharia social, podemos citar o phishing como uma das táticas mais prevalentes e danosas, caracterizando-se por tentativas fraudulentas, comumente via e-mail, de obter dados sensíveis como senhas e informações bancárias (JAKOBSSON; MYERS, 2007).

O phishing se desdobra em algumas modalidades específicas, como o Smishing, que utiliza mensagens de texto (SMS) como vetor de ataque, e o Vishing (ou Voice Phishing), que emprega chamadas telefônicas para aplicar o golpe. Outra técnica relevante é o Baiting (isca), na qual o atacante oferece algo atrativo, como um dispositivo USB infectado deixado em local público ou um link para download de conteúdo exclusivo, para atrair a vítima a comprometer seu sistema (MITNICK; SIMON, 2003).

### 2.2 Ameaças por Software Malicioso

Software malicioso é um programa desenvolvido para executar ações danosas em um dispositivo, um dos tipos mais comuns são os Vírus, que se anexam a arquivos legítimos e precisam da ação do usuário para se propagar.

Existem também os Worms, que se replicam e se espalham automaticamente por redes. Um tipo particularmente destrutivo é o ransomware, um malware que criptografa os arquivos da vítima e exige um pagamento de resgate para liberá-los (KASPERSKY, 2021).

Cavalo de Troia é o nome de um software malicioso que se disfarça de software legítimo para criar uma porta de acesso ao sistema para o invasor (STALLINGS, 2012).

### 2.3 Estratégias de Defesa e Boas Práticas

Diante dessas ameaças, a literatura de segurança da informação enfatiza a importância de uma defesa em camadas (ANDERSON, 2020). A Segurança na Nuvem, por exemplo, opera em um modelo de responsabilidade compartilhada, onde o provedor é responsável pela segurança da nuvem, mas o usuário é responsável pela segurança de seus dados e acessos na nuvem (AWS, 2023). Isso reforça a necessidade de práticas robustas por parte do usuário, como a implementação da Autenticação Multifator (MFA). A MFA adiciona uma camada crítica de proteção ao exigir duas ou mais formas de verificação de identidade, tornando o acesso não autorizado significativamente mais difícil. A combinação de ferramentas tecnológicas e, principalmente, a educação e conscientização contínua dos usuários são apontadas como a estratégia mais eficaz para a mitigação dos riscos digitais (NIST, 2020).

## 3 METODOLOGIA

A metodologia deste projeto foi estruturada como uma pesquisa-ação, partindo de um planejamento, seguida da execução de uma intervenção em um ambiente comunitário de caráter educacional.

A primeira fase consistiu no planejamento e imersão, onde os estudantes universitários realizaram um levantamento sobre os principais riscos digitais e golpes virtuais que afetam a população brasileira, em particular a parcela mais carente da população.

Foi estabelecida uma parceria com a ONG Vozes das Periferias, que foi fundamental para a aproximação com a comunidade da Favela do Haiti e para a compreensão do contexto social e tecnológico dos jovens que seriam o público-alvo do projeto.

A fase de imersão foi aprofundada por meio de uma visita técnica à Favela do Haiti, que funcionou como um diagnóstico contextual para o projeto, ela foi conduzida por representantes da ONG Vozes das Periferias e a equipe de estudantes realizou uma observação participante da dinâmica local, analisando os projetos de revitalização comunitária e engajando em diálogos com os moradores para compreender suas perspectivas.

As informações qualitativas coletadas nesta etapa foram sistematizadas na elaboração de um Mapa de Empatia, que permitiu mapear os desafios, aspirações e as vulnerabilidades nos padrões de uso de tecnologias digitais pelo público-alvo.

Figura 1 - Visita na favela do Haiti

*Fonte: Autores*

Durante a visita, foi realizada uma análise da infraestrutura física da ONG para verificar a viabilidade de execução dos workshops no local e de confirmar as condições logísticas favoráveis, e neste momento, a equipe observou um ambiente com forte capital social e cultural, um espaço dinâmico e propício para o desenvolvimento de atividades educacionais.

Figura 2 - Ambiente educacional dentro da comunidade

*Fonte: Autores*

A fase de desenvolvimento do conteúdo foi segmentada em quatro grupos, cada um responsável por um eixo temático específico. A preparação de todos os grupos partiu de uma abordagem de design thinking, utilizando o Mapa de Empatia para aprofundar a compreensão sobre o público-alvo e garantir que o material didático fosse relevante e acessível. O Grupo 1, focado em Smishing e Segurança na Nuvem, direcionou seu conteúdo para a proto-persona "Maria", uma empreendedora digital iniciante. O mapa de empatia revelou que suas principais dores eram a falta de conhecimento tecnológico e o medo de cair em golpes online, enquanto sua necessidade era a capacitação para proteger seu negócio digital. Com base nesse diagnóstico, o grupo elaborou um plano de aula com foco em ferramentas práticas, como a configuração da Autenticação Multifator (MFA), o uso de aplicativos para filtragem de SMS , a instalação de antivírus e atividades didáticas como a simulação de ataques de smishing e o uso de gerenciadores de senha.

O Grupo 2, responsável pelos temas Baiting e Vishing, teve como objetivo conscientizar a comunidade sobre golpes e promover a prevenção. Seu mapa de empatia considerou a comunidade de forma mais ampla, identificando dores como a exclusão digital e a falta de informações claras sobre prevenção. Para atender a essa necessidade , o grupo estruturou um plano de aula detalhado que definia os conceitos de engenharia social , baiting (usando exemplos como pen drives infectados) e vishing (com exemplos de falsas ligações de banco). A metodologia de ensino proposta culminava em uma dinâmica prática, na qual os participantes, divididos em grupos , analisariam cenários realistas de ambos os tipos de golpe para aprender a identificar as fraudes e agir de forma segura.

O Grupo 3, encarregado de Phishing, tipos de Malware e Autenticação, planejou sua abordagem a partir da proto-persona "Ana Paula", uma usuária que expressava insegurança ao lidar com tecnologia e dificuldade em entender a linguagem técnica sobre fraudes. A intenção do grupo era, portanto, traduzir conceitos complexos de forma acessível e prática. O conteúdo foi planejado para cobrir os principais tipos de ameaças, como phishing, vírus, worms, cavalos de troia e ransomware, além de explicar a importância e os métodos de autenticação segura.

O Grupo 4, abordando Engenharia Social e Coleta de Informações (Information Gathering), focou na proto-persona "Sr. João", um homem mais velho com menos familiaridade com o ambiente digital. O mapa de empatia indicou que ele era suscetível a promessas de ganhos fáceis, já tendo sofrido perdas financeiras com golpes. A metodologia do grupo foi, então, direcionada para a necessidade de uma educação acessível para o reconhecimento de armadilhas digitais. O objetivo era capacitar os participantes a identificarem técnicas de engenharia social em situações cotidianas, como compras online e recebimento de promoções, para que pudessem realizar transações com mais segurança.

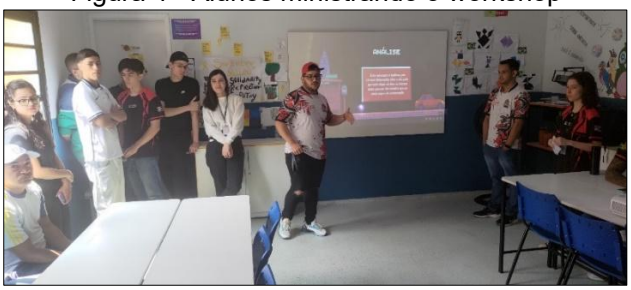
Figura 3 - Miro dos grupos para organização dos workshops

*Fonte: Autores*

## 4 RESULTADOS E DISCUSSÕES

O resultado primário do projeto foi o desenvolvimento de um programa de letramento digital customizado e a sua subsequente implementação na comunidade-alvo. A metodologia de design instrucional contextualizado, informada pela elaboração de Mapas de Empatia, permitiu a criação de quatro módulos de workshops temáticos que abordavam diretamente as vulnerabilidades identificadas em proto-personas representativas, como a de uma empreendedora iniciante e a de um residente mais velho com pouca familiaridade digital. A aderência do conteúdo às realidades locais constitui um resultado significativo, validando a abordagem centrada no usuário como fundamental para a eficácia de intervenções socioeducativas.

Figura 4 - Alunos ministrando o workshop



*Fonte: Autores*

A execução dos workshops na comunidade representa o segundo resultado central, a abordagem pedagógica empregada combinou exposição teórica com metodologias de aprendizagem ativa, incluindo a análise de estudos de caso e dinâmicas práticas com simulações de ataques de vishing e baiting.

Figura 5 - Alunos respondendo dúvidas da população

*Fonte: Autores*

A implementação bem-sucedida da intervenção discute a viabilidade do modelo de extensão universitária como mecanismo para a transferência de conhecimento técnico. A experiência demonstrou a capacidade dos discentes de traduzir conceitos complexos de cibersegurança em conteúdo acessível, promovendo o letramento digital.

Figura 6 - Alunos interagindo com as crianças da comunidade

*Fonte: Autores*

## 5 CONCLUSÃO

O estudo conclui que a metodologia de pesquisa-ação, combinada com uma abordagem de design instrucional centrada no usuário, foi eficaz para traduzir conhecimento técnico complexo em uma intervenção educacional de alto impacto e relevância social. A experiência valida o modelo de extensão como uma ferramenta de duplo benefício: por um lado, capacita a comunidade com letramento para a cidadania digital e, por outro, enriquece a formação acadêmica dos estudantes com competências práticas e sociais. O projeto serve, portanto, como um modelo replicável para futuras iniciativas que visem reduzir a desigualdade informacional e promover a inclusão digital segura.

## REFERÊNCIAS

AMAZON WEB SERVICES (AWS). Shared Responsibility Model. Seattle, 2023. Disponível em: https://aws.amazon.com/compliance/shared-responsibility-model/. Acesso em: 27 set. 2025.

ANDERSON, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. 3. ed. Hoboken: Wiley, 2020.

JAKOBSSON, Markus; MYERS, Steven. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Hoboken: Wiley-Interscience, 2007.

KASPERSKY. IT Threat Evolution in Q2 2021. Moscou, 2021. Disponível em: https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/. Acesso em: 27 set. 2025.

MITNICK, Kevin; SIMON, William L. A arte de enganar: como hackers e espiões usam a engenharia social para obter informações sigilosas. São Paulo: Pearson Education do Brasil, 2003.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). Gaithersburg: NIST, 2020.

STALLINGS, William. Cryptography and Network Security: Principles and Practice. 6. ed. Boston: Pearson, 2012.

**SOBRE O(S)AUTOR(ES)**

[i] **Caique Zaneti Kirilo (Autor 1)**

Possui bacharelado em Ciência da Computação (2012-2015); Mestrado em Engenharia de Produção com ênfase em Inteligência Artificial e Seis Sigma na linha de pesquisa de Métodos Quantitativos em Engenharia de Produção focada em Processos decisórios baseados em lógicas não clássicas (2016-2017); É Doutorando em Engenharia da Informação pela Universidade Federal do ABC. Atua como Professor Universitário e Pesquisador integrante do Grupo de Pesquisa de Engenharia de Software aplicada à criação de Sistemas Críticos, atuando também como orientador em programas de iniciação cientifica de alunos da graduação. https://orcid.org/0000-0001-5667-0861

[ii] **Vinicius De Jesus Silva (Autor 2)**

Graduando em Ciência de Dados pela Faculdade SENAI São Paulo – Campus Paulo Antônio Skaf. Atualmente sou estagiário na área de Ciência de Dados. Sou formado como Técnico em Logística e possuo experiência prévia em automação, machine learning, Python e análise de dados, atuando no desenvolvimento de soluções voltadas ao tratamento, modelagem e visualização de informações para apoio à tomada de decisão.
https://orcid.org/0009-0002-8151-9439

[iii] **Jéssica Franzon Cruz do Espírito Santo (Autor 3)**

Possui graduação (Bacharelado) em Ciência da Computação (2018-2021) pela Universidade Paulista (UNIP); Pós-graduada em Gestão Educacional na Perspectiva Inclusiva (2022) pela Universidade Federal de Pelotas (UFPEL) e Pós-graduada em Psicopedagogia (2024) pela Faculdade das Américas (FAM); É Mestranda em Engenharia da Informação pela Universidade Federal do ABC. Atua como Professora na Faculdade Senai no campus Paulo Antônio Skaf no curso de Ciência de Dados.
https://orcid.org/0000-0002-2812-3673

[iv] **Arthur Gustavo de Araujo Ferreira (Autor 4)**

Bacharel em Física com ênfase computacional pela Universidade de São Paulo (USP), mestre e doutor em Ciências pela mesma instituição. Atualmente atua como professor na Escola SENAI de Informática, em São Caetano do Sul. Possui ampla experiência em pesquisa e aplicações industriais de Ressonância Magnética Nuclear (RMN), com foco no estudo de meios porosos e computação quântica. Na indústria, tem atuação consolidada nas áreas de petrofísica e materiais cimentícios, realizando análises de RMN, modelagem estatística e machine learning aplicada à caracterização de materiais. Na educação, seu foco está voltado para ciência de dados, inteligência artificial e computação quântica.
https://orcid.org/0000-0002-6676-384X

[v] **Vivian de Oliveira Preto (Autor 5)**

Graduada em Tecnologia Gráfica (Faculdade SENAI Theobaldo de Nigris) e Mestre em Educação (UNESP/Marília). Coordenadora dos cursos superiores de Tecnologia em Ciência de Dados e Segurança Cibernética da Faculdade SENAI Mecatrônica (Campus Paulo Antônio Skaf).
https://orcid.org/0009-0006-0193-5571

[vi] **Tiago Augusto Orcajo Demay Cordeiro (Autor 6)**

Mestre em Engenharia de Computação (Poli-USP), pós-graduado em Computação em Nuvem e graduado em Engenharia Eletrônica (IMT). Atua no Insper (Laboratório de Redes e Supercomputação) e como professor de Computação em Nuvem. Pesquisa em redes, segurança com IA e HPC.
https://orcid.org/0000-0002-4991-478

[vii] **Hebert de Oliveira Silva (Autor 7)**

Mestre e Doutorando em Tecnologia da Informação pela UNICAMP; Coordenador de Cibersegurança no Grupo Hapvida e professor (IBMEC, Impacta, UNIP e SENAI Informática). Atuação em Blue/Red Team, governança e resposta a incidentes, com foco em aprendizado federado, IA e segurança em CPS/IoT. Autor de livros e artigos em IEEE, ACM e Elsevier.
https://orcid.org/0000-0002-0186-5925

[viii] **Emerson Costa Santos (Autor 8)**

Supervisor de Operações do SENAI-SP. Atua com planejamento, gestão e avaliação das Escolas e Faculdades do SENAI. Professor Convidado da Sheridan College Institute of Technology and Advanced Learning - Canadá. Doutorando em Sociologia, Mestre em Engenharia Elétrica e Engenheiro Mecânico. Pesquisador do Centro de Inteligência Artificial (C4AI-USP), Indústria 4.0 e suas tecnologias habilitadoras (CECS-UFABC) e Expert Independente da WorldSkills International. Atuou como Especialista em Educação Profissional, Docente de Educação Profissional nas áreas de Manutenção Industrial, Automação, Ferramentaria de Moldes para Metais e Educação de Jovens e Adultos. https://orcid.org/0000-0002-4730-9983