O PAPEL DA SEGURANÇA CIBERNÉTICA PARA A PROMOÇÃO DO APRENDIZADO SIGNIFICATIVO E DE PRÁTICAS SOCIAIS TRANSFORMADORAS NO MUNDO DIGITAL

THE ROLE OF CYBERSECURITY IN PROMOTING MEANINGFUL LEARNING AND TRANSFORMATIVE SOCIAL PRACTICES IN THE DIGITAL WORLD

ConfiguraçõesJosé Roberto da Silva Júnior [1], Roberta Pasqualli [2]

[1] Professor de Língua Portuguesa da Secretaria de Educação e Esportes de Pernambuco. Licenciado em Letras e em Pedagogia. Especialista em Informática na Educação (IFAM). E-mail: robertojuniorgnose@gmail.com.
[2] Doutora em Educação pela Universidade Federal do Rio Grande do Sul e professora do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina. E-mail: roberta.pasqualli@ifsc.edu.br.

Resumo: Esta pesquisa tem como objetivo analisar conceitos, ferramentas e práticas metodológicas que possibilitem mudanças positivas na formação e atuação de gestores, bem como no modo de gerir ambientes de aprendizagem. A abordagem qualitativa foi utilizada como fundamento e a pesquisa bibliográfica, por meio de uma revisão teórica baseada nos pensamentos de Demo (2011), Moran, Masetto e Behrens (2010), Ribble (2015), Santos (2022), Zimmer (2023) e outros documentos normativos orientaram as discussões sobre a implementação de políticas de segurança da informação. Ao concluirmos a produção desta investigação, ficou claro que só há uma estratégia educacional que garanta os princípios da segurança da informação quando os professores são capacitados a promover um trabalho de conscientização a partir da prática pedagógica no ambiente virtual. Constatou-se que a segurança da informação potencializa, entre outras diversas vantagens ao aprendizado, a autonomia, autoestima, conhecimento básico da legislação, criatividade, vivência em pesquisa, construção de objetos virtuais, compartilhamento do conhecimento em comunidade, iniciativa, raciocínio lógico e, consequentemente, produtividade. Por fim, essa postura de uso consciente e solidário de recursos digitais estabelece algumas mudanças na forma como o mundo e a educação são vistos na relação professor-estudante-conhecimento.
Palavras-chaves: Autonomia. Segurança cibernética. Tecnologias Digitais de Informação e Comunicação.

Abstract: This research aims to analyze concepts, tools and methodological practices that enable positive changes in the training and performance of managers, as well as in the way of managing learning environments. The qualitative approach was used as a foundation and bibliographical research, through a theoretical review based on the thoughts of Demo (2011), Moran, Masetto and Behrens (2010), Ribble (2015), Santos (2022), Zimmer (2023) and other normative documents guided discussions on the implementation of information security policies. When we concluded the production of this investigation, it became clear that there is only an educational strategy that guarantees the principles of information security when teachers are trained to promote awareness-raising work based on pedagogical practice in the virtual environment. It was found that information security enhances, among other advantages for learning, autonomy, self-esteem, basic knowledge of legislation, creativity, experience in research, construction of virtual objects, sharing of knowledge in the community, initiative, logical reasoning and, consequently, productivity. Finally, this stance of conscious and supportive use of digital resources establishes some changes in the way the world and education are seen in the teacher-student-knowledge relationship.
Keywords: Autonomy. Cyber security. Digital Information and Communication Technologies.

Recebido: 04/2024, Publicado: 06/2025 - ISSN: 2358-260X - DOI: 10.37951/2358-260X.2025v13i1.7600

CONSIDERAÇÕES INICIAIS

Atualmente, a utilização de Tecnologias Digitais de informação e Comunicação (TDIC) tem se tornado uma parte substancial da vida do ser humano. Assim sendo, a escola deve se posicionar diante desse cenário, assegurando que a formação dos estudantes aconteça de forma integral, preparando-os para participar ativamente do processo de transformação digital. Para isso, é necessário ensinar habilidades que permitam aos estudantes controlar suas próprias vidas, por meio da construção da personalidade do cidadão digital. Isso envolve a formação de um indivíduo completo que utiliza as TDIC de forma consciente, reconhecendo suas responsabilidades e direitos na internet.

As discussões apresentadas nesta investigação têm origem na seguinte problemática: Como a segurança cibernética pode garantir o aprendizado significativo por meio das redes e tecnologias digitais da informação na escola? Essa questão foi abordada por meio do seguinte objetivo geral: analisar conceitos, ferramentas e práticas metodológicas que possibilitem mudanças positivas na formação e atuação de gestores, bem como no modo de gerir ambientes de aprendizagem. A partir deste objetivo, foram definidos os seguintes objetivos específicos: estudar a eficácia das políticas de segurança da informação existentes nas escolas em garantir um ambiente virtual seguro e propício ao aprendizado significativo; identificar os principais perigos enfrentados pelas escolas na implementação de medidas de segurança cibernética e como esses desafios impactam o uso efetivo das redes e tecnologias digitais para o aprendizado; e apresentar as melhores práticas em segurança cibernética

voltadas para o ambiente educacional, com o objetivo de fornecer diretrizes específicas para promover o aprendizado significativo por meio das redes e tecnologias digitais da informação nas escolas.

Para a concretização desta investigação, foram escolhidos os procedimentos da pesquisa bibliográfica, com base em uma revisão teórica fundamentada nos pensamentos de Demo (2011), Moran, Masetto e Behrens (2010), Ribble (2015), Santos (2022), Zimmer (2023) e outros documentos normativos que orientam a implementação de políticas de segurança da informação nas escolas. A abordagem de caráter qualitativo foi adotada, pois é útil para analisar as relações, opiniões e discursos presentes nas principais documentações sobre o tema, por meio da interpretação e do exame crítico dos textos.

Na primeira parte, esta pesquisa se dedicou à contextualização da discussão sobre o uso das TDIC na educação e à construção do cidadão digital. Na segunda seção, desenvolveu-se um debate sobre as principais ameaças e riscos digitais associados às práticas escolares. Na terceira parte, foram apresentadas as principais ferramentas de segurança da informação como garantia do aprendizado significativo e da transformação social. Por fim, são apresentadas as considerações finais e as referências utilizadas.

CONTEXTUALIZANDO O USO DAS TECNOLOGIAS DIGITAIS NA EDUCAÇÃO E A CONSTRUÇÃO DO CIDADÃO DIGITAL

Por volta de 1980, Seymour Papert, matemático, iniciou a discussão sobre o uso de computadores na educação sob uma perspectiva construtivista. Ele defendia o uso desse equipamento para a criação de projetos que ensinassem muito além da computação: a criação de soluções para problemas sociais reais. Hoje, não limitamos a ideia de tecnologia apenas ao computador, pois a vida em sociedade mudou significativamente com o advento de outras TDIC, utilizadas no processo de armazenamento e manipulação de dados e informações.

A escola, assim como todas as áreas e instituições da sociedade, vem enfrentando as consequências negativas do uso das TDIC sem orientação adequada e/ou sem finalidade educativa. Por isso, os estudantes precisam desenvolver habilidades e competências para o século XXI, ou seja, combinar capacidades, conhecimentos e atitudes esperados para a vida em sociedade na atualidade, o que inclui a capacidade de atuar como cidadãos responsáveis no mundo virtual.

A Base Nacional Comum Curricular (BNCC), documento que orienta a construção dos currículos nos estados e municípios, deixa clara a preocupação em colocar o professor como orientador do processo educativo. Por isso, ele deve estimular o protagonismo estudantil no uso das TDIC, por meio do pensamento computacional e suas características importantes: análise e desenvolvimento de soluções para problemas; identificação de problemas; análise lógica e organização de dados; e reutilização de soluções anteriores em novos problemas. Diante disso, fica evidente que precisamos desenvolver práticas educativas que integrem o uso da tecnologia em sala de aula, tornando a aprendizagem mais eficiente, atrativa, dinâmica e contemporânea.

Nesse sentido, Moran, Behrens e Masetto (2010) defendem que o professor deve garantir algumas características no uso das tecnologias digitais em sala de aula: ações pedagógicas planejadas para promover a interação, a prática e a reflexão sobre os recursos e suas finalidades; discussões sobre a empatia que deve existir entre estudantes e professores; estabelecimento de parcerias entre estudantes e professores em relação à avaliação; e estímulo à criatividade e ao diálogo ao longo da busca por soluções.

Dessa forma, o uso da tecnologia na educação vai além da diversão e do domínio técnico por estudantes e professores. Deve promover a cidadania digital por meio da reflexão, o que transcende a posição passiva de consumidor de softwares, estimulando a participação ativa na criação de informações e na busca pelo sentido

dos dados disponíveis nos ambientes virtuais.

Comparando o ambiente escolar com o digital, Demo (2011) destaca que os ambientes escolares tendem a criar uma experiência fragmentada, que não reflete os desafios da vida comunitária dos estudantes. Por essa razão, a promoção da consciência cidadã no uso das TDIC vai muito além de oferecer tablets e computadores aos professores e alunos. Exige o protagonismo pessoal em todos os ambientes de atuação: físico, virtual e híbrido.

Em consonância com as ideias já apresentadas, Ribble (2015) afirma que a cidadania digital pode ser entendida como a capacidade dos usuários da internet de serem responsáveis e de conhecerem o que pode ou não ser feito em ambientes virtuais, incluindo os atos criminosos e suas respectivas consequências legais. Além disso, Ribble (2015) apresenta alguns conhecimentos trazidos pela cidadania digital, parafraseados abaixo:

a) O acesso a recursos digitais não é uma realidade em todas as comunidades; b) O comércio eletrônico deve ser desenvolvido de forma consciente, com preocupação em consumir apenas o necessário e com cuidado ao fornecer dados para pagamento; c) A comunicação digital, pela sua rapidez, oferece a possibilidade de conhecer outras culturas de comunicação, mas também facilita o compartilhamento indevido de informações; d) A alfabetização digital orienta o uso correto das tecnologias para o desenvolvimento intelectual; e) A etiqueta digital defende a preservação da ética na internet, evitando mal-entendidos e problemas jurídicos; f) A lei digital refere-se aos direitos e deveres dos que utilizam a tecnologia, bem como à responsabilidade digital, respeitando opiniões, liberdades e privilégios, além de demonstrar comprometimento com toda a comunidade virtual; g) A saúde e bem-estar digital referem-se aos cuidados de quem está constantemente conectado; h) A segurança da informação é essencial para todos que utilizam a internet.

Assim, a adoção da internet e das tecnologias digitais em sala de aula oferece diversas possibilidades positivas que aceleram a obtenção de resultados. No entanto, o cidadão digital também precisa conhecer os riscos por trás dessas facilidades e atuar de forma consciente para promover sua própria segurança e a de todos ao seu redor nas redes.

AS PRINCIPAIS AMEAÇAS E RISCOS DIGITAIS ASSOCIADOS ÀS PRÁTICAS DIGITAIS NA ESCOLA

De acordo com Santos (2022), a adoção de recursos tecnológicos conectados à internet oferece diversos benefícios, mas também traz riscos. Por isso, conhecer os princípios e características da cidadania digital, apresentados na seção anterior, é extremamente importante para reduzir os problemas de segurança da informação que podem afetar a vida profissional, pessoal e educacional no ambiente escolar inovador.

Nesse contexto, é fundamental compreender os principais conceitos relacionados às vulnerabilidades e ameaças, amplamente divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR) em seus canais de comunicação.

De acordo com o CERT.BR (2024), as vulnerabilidades possibilitam a concretização de ataques por ameaças, que as exploram de forma individual. Podemos classificá-las como brechas ou falhas que aumentam a possibilidade de ataque. As ameaças aumentam os riscos para os ativos, exploram as vulnerabilidades e podem comprometer o sistema de segurança utilizado. Exemplos incluem *malwares* e ataques cibernéticos.

O CERT.BR (2024) também apresenta os códigos maliciosos (ou *malwares*) como programas criados com a finalidade de realizar intervenções ilícitas em dispositivos informatizados, como smartphones, computadores, roteadores, entre outros. Os principais exemplos são:

a) Vírus: O *malware* mais conhecido na informática. Infecta e danifica tanto os arquivos pessoais quanto os do sistema operacional, pois depende de um software hospedeiro. Exemplos: vírus de *boot*, vírus de *script*, vírus

de macro.

b) Cavalo de troia: Programa malicioso que se disfarça como um *software* inofensivo, mas que permite que um invasor (*cracker*) controle o sistema operacional.

c) *Ransomware*: Sequestra os arquivos do usuário, apagando os originais e criptografando os dados. Solicita pagamento de resgate para restaurar o acesso aos arquivos.

d) *Rootkit*: Programa malicioso que modifica aplicativos do sistema para esconder ou camuflar arquivos e programas mal-intencionados.

e) *Backdoor*: Abre brechas no sistema, preparando-o para ataques futuros.

f) *Worm*: Programa malicioso que se autoexecuta, infectando computadores, pendrives ou redes internas sem a necessidade de ação do usuário.

g) *Bot*: Similar ao *worm*, é usado para obter controle total de um computador. É autoexecutável, infecta o *host* e estabelece conexão com o criminoso (*cracker*).

h) *Spyware: Malware* que captura dados do usuário e os envia aos invasores. Monitora hábitos para vendê-los. Divide-se em *keyloggers* (capturam dados digitados) e *screenloggers* (capturam a tela do computador).

i) *Crack*: Programa malicioso usado para quebrar senhas e licenças de softwares limitados para testes. Frequentemente encontrado em sites fraudulentos que prometem liberar o uso de *softwares* proprietários, como Windows ou Photoshop, mas que, na verdade, trazem funções prejudiciais.

Além dos *malwares*, o CERT.BR (2024) também destaca os ataques cibernéticos, técnicas usadas por criminosos virtuais para obter e alterar dados, invadindo sistemas em diversas escalas. Exemplos incluem:

a) Engenharia social: Manipulação psicológica para obter dados confidenciais. Esses ataques exploram vulnerabilidades decorrentes da superexposição de dados pelos usuários. Exemplos: *phishing*, *pharming*, *spam*, *hoax* e desafios perigosos.

b) *Spam*: Envio de propagandas não solicitadas com fins comerciais, tanto por e-mail quanto por redes sociais. Exemplos incluem correntes, pornografia e boatos (*hoaxes*).

c) *Phishing*: Ataques por meio de páginas e e-mails falsos que "pescam" dados pessoais, geralmente usando links chamativos que levam a sites fraudulentos.

d) *Pharming*: Evolução do *phishing*, corrompe o DNS de um site legítimo para redirecionar o usuário a um servidor malicioso.

e) *Botnet*: Rede de computadores infectados por *bots*, usada para invadir outras máquinas, formando uma rede zumbi.

f) Negação de serviço (DoS/DDoS): Ataque que sobrecarrega um servidor, site ou serviço com mais solicitações do que ele pode processar, causando sua queda.

g) Força bruta: Método que tenta adivinhar nomes de usuário e senhas por tentativa e erro, buscando acessar sistemas ou serviços com os privilégios da vítima.

Portanto, para que haja aprendizado significativo e seguro por meio das tecnologias digitais, é essencial reduzir o número de vulnerabilidades, ameaças, *malwares* e ataques. Para isso, estudantes, professores e demais profissionais precisam conhecer cada um dos termos abordados nesta seção, a fim de escolher a melhor política de segurança da informação.

SEGURANÇA CIBERNÉTICA COMO GARANTIA DO APRENDIZADO SIGNIFICATIVO E DA TRANSFORMAÇÃO SOCIAL A PARTIR DA ESCOLA

Em seu guia de segurança da informação para educadores, Zimmer (2023) destaca que, assim como a maioria das instituições governamentais e privadas, a escola precisa cuidar adequadamente dos dados pessoais de seus estudantes, professores e colaboradores em geral, uma vez que qualquer roubo ou adulteração de informações pode provocar danos financeiros e jurídicos.

Por essa razão, embora não seja possível eliminar completamente os riscos relacionados à segurança da informação - que visa proteger tanto as informações

internas quanto externas -, torna-se necessário estabelecer uma política consistente de segurança da informação na escola.

As discussões sobre segurança da informação apresentadas ao longo desta seção consideram a norma internacional ISO/IEC 27001 como o padrão mais reconhecido para o gerenciamento de segurança da informação. De acordo com a ABNT (2006), a NBR ISO/IEC 27002:2005 especifica às práticas de segurança da informação com o objetivo de preservar três características essenciais: confidencialidade, integridade e disponibilidade.

a) Confidencialidade: Capacidade de um sistema de impedir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas, sejam elas usuários, máquinas, sistemas ou processos. Exemplo prático para a escola: a criptografia, que codifica e decodifica dados transformando uma mensagem em códigos secretos com uma chave criptográfica para impedir o acesso de terceiros.

b) Integridade: Capacidade de garantir que a informação manipulada está correta, fidedigna e não foi corrompida. Trata-se da preservação da exatidão e completude da informação. Exemplo prático: a função de hash, um algoritmo matemático que transforma um bloco de dados em uma sequência fixa de caracteres, garantindo que os dados não foram modificados durante a transmissão em rede.

c) Disponibilidade: Propriedade que garante que uma informação esteja acessível e utilizável sob demanda por uma entidade autorizada. Exemplo prático: o *backup* ou cópia de segurança, que protege arquivos pessoais ou corporativos contra-ataques de *ransomware* e falhas nos dispositivos de armazenamento. Pode ser feito em dispositivos físicos ou na nuvem, garantindo a disponibilidade dos dados.

Além desses recursos, a escola pode adotar outros mecanismos, como:

a) *Firewall*: Dispositivo físico ou lógico que protege a rede interna (LAN ou intranet) contra invasões vindas da rede externa (internet), monitorando o tráfego e identificando possíveis ataques de acordo com políticas definidas.

b) Anti*malware*: Programas usados na prevenção contra ataques de *malwares*. Exemplos: antivírus, *antispyware*, *antirootkit*, *antitrojan*.

Ademais, para evitar danos e proteger os dados, é necessário um conjunto de mecanismos de segurança que o usuário pode adotar. No entanto, mesmo com técnicas avançadas de segurança, a postura do usuário é fundamental, tornando indispensável a discussão sobre procedimentos de segurança.

Dessa forma, a construção de uma estratégia educacional que garanta os princípios da segurança da informação se concretiza por meio da capacitação dos professores e da promoção de um trabalho de conscientização no ambiente virtual. Isso permitirá que os estudantes aprendam sobre os cuidados necessários ao expor dados pessoais nas redes, os riscos da engenharia social — que engana os usuários para obter informações confidenciais (como *phishing* e *pharming*) —, a navegação e pesquisa seguras, e a adoção de uma política de senhas para aumentar a segurança dos sistemas.

CONSIDERAÇÕES FINAIS

A presente pesquisa demonstrou que, mesmo com o acesso à internet e às tecnologias ainda sendo precário em muitas escolas no Brasil, a tendência é que o uso desses recursos aumente ao longo dos anos. Por isso, é necessário que, além de expandir o acesso às tecnologias, as escolas protejam os dados pessoais de seus estudantes, professores e colaboradores, pois qualquer roubo ou adulteração de informações pode resultar em danos financeiros e jurídicos que afetam negativamente a reputação da instituição e o trabalho pedagógico do professor.

Observou-se que o uso de tecnologia nas escolas potencializa várias habilidades necessárias para o cidadão digital, como autonomia, autoestima, conhecimento básico de legislação, criatividade, pesquisa,

compartilhamento de conhecimento em comunidade, iniciativa, raciocínio lógico e, consequentemente, produtividade. Essa postura consciente e solidária no uso de recursos digitais promove mudanças na maneira como o mundo e a educação são percebidos.

No entanto, a escola deve destacar os riscos associados à adoção das TDIC, ampliando a visão dos estudantes por meio de multiletramentos que envolvam práticas sociais na comunidade digital. Isso é crucial, pois hackers desonestos estão sempre em busca de dados sensíveis, usando técnicas enganosas e propagando spam, sites falsos, desafios perigosos e conteúdos inadequados, o que prejudica o desenvolvimento global dos estudantes da educação básica.

Além disso, as escolas poderiam estabelecer parcerias com universidades que ofereçam cursos na área de Educação e TDIC, desenvolvendo ações voluntárias para apresentar a segurança da informação como um elemento crucial na construção de uma comunidade escolar conectada, impactando diretamente o aprendizado e as práticas sociais no mundo digital.

Portanto, para garantir os princípios da segurança da informação, é essencial capacitar os professores a promover a conscientização no ambiente virtual. Além disso, os estudantes devem aprender mais sobre os cuidados necessários ao expor dados pessoais, os riscos da engenharia social (*phishing* e *pharming*) e as formas de navegação e pesquisa seguras.

Este estudo não busca esgotar os debates e desafios relacionados ao tema, mas os objetivos propostos foram devidamente atingidos, assim como a problemática de pesquisa foi abordada ao longo do trabalho. Espera-se que investigações futuras explorem mais profundamente este tema tão relevante para a segurança da informação aplicada à educação.

REFERÊNCIAS

ABNT. NBR ISO/IEC 27002: 2005. Tecnologia da informação: Técnicas de segurança e código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2006.

BRASIL. Ministério da Educação e Cultura - MEC. Base Nacional Comum Curricular (BNCC). Disponível em 2018, em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em: 26 de mai. 2024.

CERT.BR. Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, 2024. Disponível em: https://cert.br/. Acesso em: 02 abr. 2024.

DEMO, P. Aprendizagens e novas tecnologias. Roteiro, [S. l.], v. 36, n. 1, p. 9–32, 2011. Disponível em: https://periodicos.unoesc.edu.br/roteiro/article/view/860. Acesso em: 24 de mai. 2024.

ISO. ISO/IEC 27001: Information security management systems. Disponível em: https://www.iso.org/standard/27001. Acesso em: 27 mai 2024.

MORAN, J. M.; MASETTO, M. T.; BEHRENS, M. Novas tecnologias e mediação pedagógica. Campinas: Papirus, 2010.

RIBBLE, M. Digital citizenship in schools: Nine elements all students should know. International Society for Technology in Education, 2015.

SANTOS, C. P. Educação, Práticas Digitais e Novos Riscos em Rede. Em XI Congresso Brasileiro de Informática na Educação (CBIE 2022), Anais do XXVIII Workshop de Informática na Escola (WIE 2022). DOI: 10.5753/wie.2022.225607. Disponível em: https://sol.sbc.org.br/index.php/wie/article/view/22363/22187. Acesso em: 27 mai. 2024.

ZIMMER, K. Como as escolas podem melhorar a segurança online: um guia para educadores. Disponível em: https://www.lumiun.com/blog/como-as-escolas-podem-melhorar-a-seguranca-online-um-guia-para-educadores/. Acesso em: 21 mai. 2024.