Educação, Práticas Digitais e Novos Riscos em Rede

Cristina Paludo Santos

Instituto Federal Farroupilha – Santo Ângelo/RS

cristina.paludo@iffarroupilha.edu.br

Abstract. *This paper describes efforts to disseminate and popularize new attitudes and good practices in the digital world, promoting reflections on the topic of Information Security in the school environment. The target audience includes high school students and teachers, both from public schools. The strategies developed aim to strengthen digital education through the formation of citizens who are connected and aware of the risks and vulnerabilities that the network society offers, favoring the development of skills provided for in the BNCC and reaffirmed by the Brazilian Computer Society and the Center for Innovation in Brazilian Education through guidelines for teaching computing in Basic Education. The practices were initially developed with a restricted group of students from the 3rd year of high school and, later, were disseminated to other actors in the school community in order to foster a culture of information security in this environment, as well as encourage students to use technology in a more conscious way, in which it is possible to stimulate reflection and other ethical concepts in society. An overview of such strategies, as well as the results obtained, are presented so that the experience can be replicated and/or improved by other institutions.*

Resumo. *Este artigo descreve os esforços direcionados para disseminação e popularização de novas posturas e boas práticas no mundo digital, fomentando no âmbito escolar reflexões acerca do tema Segurança da Informação. O público-alvo das ações inclui estudantes do ensino médio e docentes, ambos de escolas públicas. As estratégias desenvolvidas visam fortalecer a educação digital por meio da formação de cidadãos conectados e cientes dos riscos e vulnerabilidades que a sociedade em rede oferece, favorecendo o desenvolvimento de competências previstas na BNCC e reafirmadas pela Sociedade Brasileira de Computação e pelo Centro de Inovação da Educação Brasileira. As práticas foram desenvolvidas inicialmente com um grupo restrito de alunos do 3º ano do ensino médio e, posteriormente, foram difundidas para os demais atores da comunidade escolar a fim de fomentar uma cultura de segurança de informação neste ambiente, bem como incentivar os estudantes a utilizar a tecnologia de forma mais consciente, em que seja possível estimular a reflexão e os demais conceitos éticos da sociedade. Uma visão geral de tais estratégias, bem como dos resultados obtidos são apresentadas de modo que a experiência possa ser replicada e/ou aprimorada por outras instituições.*

DOI: 10.5753/wie.2022.225607

1. Introdução

Vivemos em uma sociedade em rede onde o novo paradigma conferido para essa nova cultura se entrelaça com a produção e disseminação da informação. Essa onda de disseminação da informação em um mundo cada vez mais conectado tem seus prós, pois gera oportunidades e facilidades para organizações e indivíduos, mas tem um efeito oculto.

Se por um lado a cultura digital potencializa novas formas de interação, novos tipos de sociabilidade, novas possibilidades e oportunidades, por outro viabiliza também novos riscos. É um palco onde diariamente se experimentam "oportunidades arriscadas" (Livingstone, 2013). Este fato é extraordinariamente evidente no mundo juvenil. Evidências empíricas, obtidas por meio de alguns estudos, nacionais e internacionais, revelam que para a *net generation*, os *digital natives, millennials* ou a *thumb tribe* o digital é a vida em tempo real (Eisenstein e Da Silva, 2016; Livingstone *et al*, 2014; Madden *et al*, 2015). Em um nível global, registram-se padrões comuns no mundo digital: a massificação do acesso é impressionante e a intensidade do uso da internet é surpreendente. É um dado incontestável: a vida dos jovens é/está profundamente midiatizada e essa midiatização passa, em larga escala, pelo digital.

Apesar do uso das Tecnologias da Informação e Comunicação (TICs) proporcionar indiretamente o desenvolvimento social e cultural, paralelamente a esta evolução, vê-se surgir pessoas que têm usado esse avanço para a prática de atos danosos. Roubo de dados, perseguições, uso indevido de imagem, *cyberbullying*, são apenas alguns dos riscos aos quais os internautas estão expostos todos os dias. Esses crimes têm como principal elemento a falta de conhecimento dos usuários das redes. Sem o conhecimento necessário para aferir sobre quais atitudes tomar diante dessa nova realidade, o usuário torna-se facilmente manipulável.

Consoante a esta realidade, percebe-se oportuno fomentar no âmbito escolar reflexões envolvendo o tema Segurança da Informação, disseminando e popularizando novas posturas e boas práticas no mundo digital entre os jovens. E é nesse cenário que se insere este artigo, que apresenta o relato de uma experiência realizada com alunos do ensino médio de uma escola pública com vistas à educação em prol da formação de um cidadão conectado e ciente dos riscos e vulnerabilidades que a sociedade em rede oferece.

Tal trabalho insere-se no rol de estratégias existentes que visam fortalecer a educação digital. Entre os trabalhos relacionados pode-se citar o jogo para auxílio no ensino de conceitos relacionados a Segurança na Internet para Crianças e Adolescentes proposto por Farias (2019), bem como a história em quadrinhos elaborada por Cruz (2017) em que é abordado o enfoque social da segurança da informação. Carvalho et al (2017) propõem uma reflexão sobre a necessidade de um melhor embasamento sobre a Segurança da Informação pela comunidade escolar, bem como fundamenta a necessidade de debates, capacitações e até mesmo a criação de disciplinas para tratar adequadamente o assunto.

Cabe destacar, por oportuno, que a abordagem adotada neste trabalho se difere das propostas por Farias (2019) e Cruz (2017), mas convergem com as ideias apresentadas por Carvalho *et al* (2017), uma vez que promove uma Campanha de Conscientização junto à comunidade escolar com estratégias que compreendem a produção de material

informativo, entrevistas em rádio, divulgação em redes sociais, dentre outros. Além disso, às ações alinham-se às competências e premissas específicas da Computação na Base Nacional Comum Curricular (BNCC) em que a exposição de conceitos inerentes à Segurança Digital perpassa pelos diversos níveis da Educação Básica a fim de desenvolver as habilidades necessárias do século XXI.

Uma descrição mais detalhada das práticas desenvolvidas é apresentada nas seções subsequentes. A seção 2 descreve os procedimentos metodológicos adotados. A seção 3 apresenta os resultados do diagnóstico realizado e o plano de ação proposto, enfatizando as práticas sendo desenvolvidas e/ou em desenvolvimento. Por fim, a seção 5 apresenta as considerações finais.

2. Procedimentos Metodológicos

A inspiração para o desenvolvimento do presente trabalho surgiu a partir da aplicação de uma atividade diagnóstica no escopo da disciplina Segurança em Sistemas de Informação, ofertada para uma turma do 3º ano de um Curso Técnico Integrado em Manutenção e Suporte em Informática. Ao analisar os resultados da atividade constatou-se que, em uma turma com 24 alunos, apenas 5 deles possuíam conhecimentos básicos em relação às medidas de segurança da informação.

Este fato incitou reflexões sob diversos aspectos que podem ser expressos por meio das seguintes questões: (a) quais são os conhecimentos dos jovens a respeito do uso seguro da Internet e seus recursos? (b) como se estabelece a articulação dos professores para a promoção de práticas pedagógicas, independente da área e/ou curso, que envolvem o tema segurança da informação?

Tais indagações e reflexões impulsionaram o desenvolvimento de um projeto que abarcou uma equipe composta por 24 alunos do 3º ano e a docente e que repercutiu em toda a comunidade escolar. O tema foi inicialmente abordado junto aos integrantes da equipe para que pudessem compreender a importância da Segurança da Informação, seus principais conceitos e exemplos de riscos e vulnerabilidades. Além das aulas expositivas, diversos recursos multimodais foram explorados com o intuito de ampliar o horizonte de conhecimento dos alunos, a citar, vídeos, documentários, depoimentos de casos reais, notícias, palestra com especialista e cine-debate envolvendo o filme “Privacidade hackeada”.

Após a exploração dos conceitos fundamentais que permeiam o contexto da Segurança da Informação, a equipe foi desafiada a realizar um diagnóstico envolvendo a comunidade escolar com o objetivo de estimar o nível de maturidade dos alunos em suas práticas de segurança da informação e, principalmente, fundamentar a necessidade de um tratamento mais adequado ao tema nessa instituição de ensino.

Nesta etapa, o projeto fundamentou-se numa pesquisa aplicada, objetivando gerar conhecimentos para tomada de ações relacionadas ao uso seguro de dispositivos computacionais conectados em rede. Utilizou-se uma abordagem social empírica participativa estabelecendo relações comunicativas com discentes e docentes do 1º, 2º e 3º anos do ensino médio, que formaram o espaço amostral.

A fim de inferir sobre as medidas de segurança adotadas pelos participantes, bem como seus conhecimentos e experiências em relação ao uso e disseminação de

informação na Internet, foi elaborado um questionário baseado nas competências e habilidades previstas na BNCC. Diante do número significante de assuntos que podem ser abordados e facilmente discutidos envolvendo o tema optou-se por questões envolvendo o uso e gerenciamento de senha, incluindo criação, frequência de troca e proteção; proteção contra vírus e outros códigos maliciosos; e-mails e anexos desconhecidos; engenharia social; clonagem de *whatsapp* e redes sociais; questões de segurança em dispositivos móveis; uso de declarações de confirmação (senhas, acesso a sistemas e dados); dentre outros.

O questionário contempla 20 questões e dentre elas alguns exemplos incluem: Você usa a mesma senha em contas diferentes? Você salva senhas no seu navegador ou computador? Você sabe identificar uma *fake news*? Você já recebeu algum email malicioso dizendo, por exemplo, que você foi contemplado com um prêmio ou um anúncio falando que uma quantia em dinheiro esperava por você? Você sabe o que é uma senha segura? Você sabe verificar se um link é verdadeiro ou falso?

No questionário dos docentes foram acrescidas outras questões com vistas a identificar a atuação dos mesmos em relação ao tema "Segurança da informação". São elas:

1) Considera importante tratar o tema "Segurança da Informação" em disciplinas do Ensino Médio?
2) Em algum momento nas suas práticas pedagógicas você abordou com seus alunos assuntos relacionados ao uso seguro da Internet e seus recursos?
3) Você se sente preparado para abordar o tema com seus alunos?

Os dados coletados por meio dos questionários foram analisados de forma a estimar o conhecimento do público em relação a assuntos menos conhecidos e, principalmente, fundamentar a necessidade de um tratamento mais adequado ao tema em na instituição de ensino em que a pesquisa foi realizada.

3. Resultados e Plano de Ação

Participaram da pesquisa 254 pessoas, sendo 77 alunos do 3º ano, 78 do 2º ano, 85 do 1º ano e 14 docentes. Os resultados revelam a carência do público em relação a conhecimentos que são essenciais para quem utiliza celulares, *tablets* e computadores.

Dentre os vários aspectos analisados, alguns se destacaram por apresentar índices bem expressivos, tais como: 75% dos participantes afirmam não saber identificar sites falsos; 80% desconhecem o método de autenticação de 2 fatores; 70% afirmam salvar as senhas no navegador ou no computador; 85% declararam não saber identificar links falsos; 90% dos participantes revelam que não sabem quais são as providências a serem tomadas caso seu whatsapp ou perfil em redes sociais seja clonado; 45% afirmam não reconhecer ataques/fraudes que ocorrem através da falsificação de e-mails; 85% afirmam já ter compartilhado informações pessoais em plataformas ou aplicativos online; aproximadamente 40% das pessoas avaliadas não mostraram domínio sobre como criar uma senha segura; 80% afirmam que sabem identificar *fake news* apenas em alguns casos; 95% afirmam desconhecer os termos *phishing* e engenharia social e aproximadamente 75% do público não associaram o protocolo https à criptografia das

informações que trafegam pela rede. Este último índice merece atenção se considerarmos que o não uso do mecanismo pode expor dados sensíveis do usuário, tais como número de cartões de créditos, senhas de acesso, número de documentos, dentre outros.

O funcionamento dos cookies, utilizados, geralmente, para rastrear a navegação do usuário, não foi identificado por 65% das pessoas pesquisadas, com esse percentual chegando a 52% entre os alunos do Ensino Médio. Considerando que nem todo tipo de cookie é seguro, essa é uma estatística perigosa. Tais índices são preocupantes e evidenciam a necessidade de direcionamentos mais específicos para amenizar a falta de informação.

A análise dos dados foi realizada considerando o público como um todo, com ressalvas relacionadas ao perfil específico de docente que levou em consideração as questões acrescidas ao questionário com vistas a averiguar a atuação docente em relação à Segurança da Informação. A pesquisa mostra que apesar de 100% dos professores considerem importante a discussão sobre o tema com o público jovem, apenas 35% deles afirma ter abordado sobre o tema com seus alunos. Os demais justificam o fato de não se sentirem preparados para debater o assunto (53%) ou julgar que o assunto foi tratado em alguma outra disciplina (3%). Além de aproximadamente 9% alegar que nunca havia pensado sobre essa questão.

A partir dos resultados do processo de análise foi possível definir um conjunto de ações embasado no diagnóstico sobre as carências de conhecimento ou habilidades do público-alvo em relação ao tema abordado, o que nos permite produzir uma abordagem de conscientização dos problemas existentes relacionados ao mundo digital. Assim o plano de ação proposto abarca práticas que se complementam com a intencionalidade de produzir conhecimento crítico necessário para gerar medidas de amadurecimento que viabilizem dirimir os problemas diagnosticados.

A proposta de tais práticas se respalda nas competências e habilidades previstas pela BNCC e incluem atividades que buscam estimular o desenvolvimento das seguintes habilidades:

- Analisar criticamente artefatos computacionais, sendo capaz de identificar as vulnerabilidades dos ambientes e das soluções computacionais buscando garantir a integridade, privacidade, sigilo e segurança das informações;
- Acessar as informações na Internet de forma crítica para distinguir os conteúdos confiáveis de não confiáveis;
- Entender como mudanças na tecnologia afetam a segurança, incluindo novas maneiras de preservar sua privacidade e dados pessoais online, reportando suspeitas e buscando ajuda em situações de risco;
- Reconhecer o potencial impacto do compartilhamento de informações pessoais ou de seus pares em meio digital;
- Conhecer as possibilidades de uso seguro das tecnologias computacionais para proteção dos dados pessoais e para garantir a própria segurança e,
- Reconhecer a importância de verificar a confiabilidade das fontes de informações obtidas na Internet.

A partir disso, temos a perspectiva de trazer um panorama sobre os cuidados com a segurança ao usar dispositivos como celular, *tablets*, computadores dentre outros (roubo de dados em dispositivos físicos, rastro de dados online quando da utilização de jogos por exemplo etc.) e promover reflexões sobre aspectos de segurança e privacidade que são importantes quando utilizamos ambientes virtuais, como jogos online, compras online, interação em salas de conversa online, interação em redes sociais, destacando o compartilhamento de informações e acesso a sites da internet que não são seguros e desconhecidos.

A seguir são descritas as estratégias definidas no escopo do projeto. É importante salientar que algumas já foram implementadas, enquanto outras estão em fase de produção e/ou planejamento. Tais estratégias incluem:

(a) Produção de materiais informativos como cartazes e *folders* para serem distribuídos no ambiente escolar. Alguns exemplos de materiais produzidos pelos alunos para alertar os usuários sobre possíveis riscos e para disseminar boas práticas em Segurança da Informação são apresentados na Figura 1.

Os materiais foram produzidos pelos alunos do 3º ano do ensino médio e é resultado de um compilado de estudos e informações. Acredita-se que estes materiais sejam interessantes não só para popularizar o conhecimento, mas também para criar uma cultura de segurança na instituição, pois a jornada de aprendizagem em segurança é um processo constante e se mostra mais eficiente quando compartilhado coletivamente. Os materiais já estão disponíveis no ambiente escolar.

Figura 1. Materiais informativos produzidos

(b) Realização de entrevistas na rádio escolar. O projeto utiliza diversos meios de comunicação, dentre eles o rádio. Isso oportuniza aos alunos, principalmente aos que integram a equipe executora, vivenciar experiências diferenciadas e apoderar-se dos equipamentos midiáticos para elaborar atividades que desenvolvam a cidadania, desenvolvendo novas práticas enriquecedoras para sua formação. Além disso, demonstra que a rádio escolar é uma ferramenta apta a contribuir para o aprendizado, favorecendo a troca, cooperação e diálogo entre os membros envolvidos. Tudo isso decorrente da valorização dos diferentes conhecimentos e fortalecimento da autoestima do educando com oportunidade de vivenciar habilidades e competências para uma proposta relacionada à referida mídia.

(c) Elaboração de cursos específicos para professores. Os resultados obtidos durante a etapa de investigação demonstram a necessidade de prover meios para que os próprios professores se apropriem dos conceitos básicos relacionados à Segurança Digital. Independente da área do professor, estes conhecimentos constituem-se atualmente como essenciais tanto como conteúdo de ensino, para que os professores estejam preparados para apoiar os alunos na compreensão e na apropriação de tais conceitos, quanto para a segurança de suas próprias informações.

Como forma de suprir essa lacuna está em andamento a elaboração de cursos de curta duração que têm como objetivo a inclusão digital de professores no contexto de Segurança da Informação. Esses cursos devem ser ministrados inicialmente para os professores da escola e, a partir da experiência vivenciada, os mesmos poderão ser abertos para participação de professores que atuam em outras escolas, públicas ou privadas.

(d) Desenvolvimento de um *chatbot* para esclarecer dúvidas relacionadas às questões de segurança abordadas no escopo do projeto. Os *chatbots* são tecnologias emergentes que têm aplicação em diversos contextos, incluindo o contexto educacional. No escopo deste projeto, o *chatbot* apresenta-se como um recurso interativo viável uma vez que possibilita uma comunicação dinâmica instantânea; possui uma interface amigável; está disponível 24 horas por dia, 7 dias por semana e, sobretudo, pode aumentar o engajamento dos jovens quando bem projetado.

Dentre os princípios que regem o desenvolvimento do *chatbot* proposto está a utilização de uma linguagem conversacional com a qual o público jovem está acostumado. Acredita-se que o uso de recursos multimídia, *emojis*, *gifs* e afins pode ser um aliado na busca de um maior engajamento. Além disso, o *bot* deverá adotar um tom mais leve e divertido para se comunicar, buscando atrair a atenção dos utilizadores aos conteúdos por ele abordados. Cabe destacar que o *chatbot* está sendo desenvolvido no escopo de um projeto de Iniciação Científica.

(e) Publicações de materiais informativos nas redes sociais da instituição. Com isso, busca-se disseminar o programa através de múltiplos canais, permitindo que tanto o público interno quanto externo tenha acesso às informações.

(f) Produção e realização de oficinas. As oficinas diferem dos cursos, visto que não têm como objetivo abordar conceitos teóricos, mas sim permitir um compartilhamento de experiências e realidades entre as pessoas participantes. Acredita-se que a adoção de modelos de oficinas neste contexto possa criar um ambiente em que

todos aprendem com todos e fazer emergir boas possibilidades de uso da Segurança da Informação pelo grupo.

Ainda, dentro das estratégias presentes no plano de ação do projeto em desenvolvimento, está a produção de uma peça teatral. A peça é uma adaptação da história do chapeuzinho vermelho e tem por objetivo explorar os conceitos básicos sobre cibersegurança junto ao público infanto-juvenil. O roteiro da história está sendo escrito com apoio com a professora de Artes da escola, com a participação de 10 alunos do 3º ano que integram a equipe do projeto.

4. Considerações Finais

Na BNCC, define-se competência como a mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas, cognitivas e socioemocionais), atitudes e valores para resolver demandas complexas da vida cotidiana (Brasil, 2018). Entre as dez competências gerais relacionadas no documento, destaca-se, na discussão deste artigo, as seguintes competências:

Competência 5. Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva;

Competência 7. Argumentar com base em fatos, dados e informações confiáveis, para formular, negociar e defender ideias, pontos de vista e decisões comuns que respeitem e promovam os direitos humanos, a consciência socioambiental e o consumo responsável em âmbito local, regional e global, com posicionamento ético em relação ao cuidado de si mesmo, dos outros e do planeta.

Ambas as competências reforçam o papel da escola no desenvolvimento da competência informacional e evidenciam a importância de compreender a abrangência que a temática "segurança da informação" alcança. Neste sentido, este artigo apresenta um plano de ação que, apesar de denominado "Campanha de Conscientização", abarca práticas que abordam o tema utilizando-se de variadas estratégias a fim de explorar a diversidade de assuntos que envolvem a temática.

Os dados apresentados apontam o caminho: a educação como estratégia para minimizar riscos e maximizar capacidades e competências digitais colocando em evidência a necessidade urgente de alertar os indivíduos para reconhecer situações de segurança da informação e agir corretamente, garantindo a sua inclusão digital de forma competente, responsável e segura.

Sob essa perspectiva, além da campanha em si, realizada a partir da elaboração de produtos educacionais como cartazes, folders, publicações e entrevistas, são propostas ações de formação de professores por meio de cursos e oficinas, desenvolvimento de solução computacional por meio dos chatbots e, também atividades culturais de cunho educativo na forma de peça teatral. Com esse arsenal de possibilidades busca-se preparar alunos e professores para fazerem análises críticas sobre as tecnologias a que têm acesso, sendo capazes de identificar os riscos a que estão expostos, seja por meio do

compartilhamento de informações pessoais desnecessárias ou sensíveis ou na interação com pessoas ou grupos desconhecidos e saber como se proteger e denunciar situações suspeitas, além do desenvolvimento de muitas outras habilidades relacionadas ao uso e compartilhamento seguro e confiável de informações.

Algumas das ações já foram implementadas como, por exemplo, a produção e divulgação de materiais informacionais e entrevistas na rádio. Tais ações já tiveram grande repercussão no ambiente escolar, com convites para que a equipe desenvolvesse novos trabalhos com turmas específicas de alunos do ensino médio. A partir dessa demanda que se apresentou se instituiu a oferta de oficinas como estratégia para abordar o tema de segurança junto a essas turmas de alunos. As oficinas devem ocorrer no início do segundo semestre envolvendo, inicialmente, alunos dos 1^0 e 2^0 anos do ensino médio. Professores e funcionários da instituição também demonstraram interesse em "aprender mais" sobre o assunto. Para este público estão programadas, também para o 2^0 semestre do ano corrente, a oferta de cursos de curta duração.

Cabe destacar, por oportuno, que por muito tempo a segurança da informação era tratada apenas tecnicamente, com proteção por meio de uso de antivírus, firewall e outras ferramentas similares. Porém, ultimamente, muito se fala em espionagem, privacidade, *phishing* e engenharia social, que são temas que nos faz repensar a grande dificuldade que ainda persiste por parte das pessoas em entender a importância da segurança da informação, por isso o usuário é considerado o elo mais fraco, já que nos incidentes de segurança sempre há pessoas envolvidas, tanto no lado das vulnerabilidades exploradas, quanto no lado das ameaças.

Isso reforça ainda mais a importância de estabelecer uma cultura de segurança da informação no âmbito escolar. Atitudes em relação à segurança e privacidade no ambiente digital devem fazer parte dos requisitos necessários para o pleno uso dos recursos disponibilizados em rede, já que os cuidados que se tem no dia a dia não podem ser esquecidos no ambiente digital, onde também se está exposto a normas e riscos semelhantes.

É nesse sentido que se insere esse projeto cujo as estratégias adotadas são ferramentas apropriadas para engajar as pessoas e garantir que estas recebam treinamento, educação e conscientização adequadas para formação de cidadãos com consciência crítica no mundo virtualizado em que vivemos. Além disso, acredita-se que compartilhar boas práticas por meio da divulgação dos trabalhos realizados também seja uma iniciativa importante que permite a replicação das ações em outras instituições de ensino e, por isso, fica aqui registrada nossas contribuições.

Referências Bibliográficas

BRASIL. **Ministério da Educação**. Base Nacional Comum Curricular. Brasília, **2018**.

Castells, M. (2006). A Sociedade em Rede: do Conhecimento à Política. In Castells, M., & Cardoso, G. (orgs.). A Sociedade em Rede: do Conhecimento à Acção Política (pp.17-30). Lisboa: Debates, Presidência da República.

CRESPO, Marcelo Xavier de Freitas. Crimes digitais. Rio de Janeiro: Saraiva. 2011. 242p.

Cert.br. (2022). Centro de estudos, resposta e tratamento de incidentes de segurança no brasil. [Online. Acesso em 21 de março de 2022].

Carvalho, Emerson A.; Reis, Thales; Alves, Fábio J.. Ensino de Noções Básicas de Segurança da Informação nas Escolas Brasileiras. *In*: ***Anais do Workshop de Informática na Escola***, Vol. 23, 2017, Recife. Porto Alegre: Sociedade Brasileira de Computação, 2017 . p. 765-774.

Cruz, Efraim Silveira. **O enfoque social da segurança da informação** [recurso eletrônico] / Efraim Silveira Cruz, Albert Santos Barbosa, Maria Augusta Silveira Netto Nunes. – 2. ed. --Porto Alegre : SBC, 2017. 16 p. : il. – (Almanaque para popularização de ciência da computação. Série 1, Informática, ética e sociedade ; v. 3).

Farias, Fernando Lucas de Oliveira, et al. "Self Protect: Um jogo para auxílio no ensino de conceitos relacionados a Segurança na Internet para Crianças e Adolescentes." In: ***Anais do Workshop de Informática na Escola***. Vol. 25. No. 1. 2019.

Eisenstein, Evelyn; Da Silva, Eduardo Jorge Custódio. Crianças, adolescentes e o uso intensivo das tecnologias de informação e comunicação: desafios para a saúde. **KIDS ONLINE BRASIL**, p. 117, 2016.

Livingstone, S. (2013), **Children's internet culture: power, change and vulnerability in twenty-first century childhood** In Lemish, D. (org.), The Routledge International Handook of children, adolescents and media, Nova Iorque, Routledge

Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G., & Ólafsson, K. (2014). **Net Children Go Mobile**. *The UK*.

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2015). **Teens, social media, and privacy**. *Pew Research Center*, *21*(1055), 2-86.