



UNIVERSIDADE ESTADUAL PAULISTA
Faculdade de Filosofia e Ciências de Marília
Departamento de Ciência da Informação
Curso de Biblioteconomia

Anis Costa dos Santos

Segurança e privacidade digital no contexto da Unesp:

Orientações para o trabalho remoto

Marília

2024

Anis Costa dos Santos

Segurança e privacidade digital no contexto da Unesp:
Orientações para o trabalho remoto

Trabalho de Conclusão de Curso
apresentado ao Conselho de Curso de
Biblioteconomia da Faculdade de Filosofia
e Ciências, da Universidade Estadual
Paulista – UNESP – Campus de Marília,
como requisito parcial para obtenção do
título de Bacharel em Biblioteconomia.

Linha de Pesquisa: Informação e
Sociedade

Orientador(a): Prof. (a) Dr. (a) Helen de
Castro Silva Casarin

Marília

2024

S237s	Santos, Anis Costa dos Segurança e privacidade digital no contexto da Unesp : Orientações para o trabalho remoto / Anis Costa dos Santos. -- Marília, 2024 64 p. : tabs. Trabalho de conclusão de curso (Bacharelado - Biblioteconomia) - Universidade Estadual Paulista (UNESP), Faculdade de Filosofia e Ciências, Marília Orientadora: Helen de Castro Silva Casarin 1. Competência Digital. 2. Segurança Digital. 3. Formação de usuários. 4. DigComp. 5. DigCompEdu. I. Título.
-------	--

Anis Costa dos Santos

Segurança e privacidade digital no contexto da Unesp:

Orientações para o trabalho remoto

Trabalho de Conclusão de Curso apresentado Conselho de Curso de Biblioteconomia da Faculdade de Filosofia e Ciências, da Universidade Estadual Paulista – UNESP – Campus de Marília, como requisito parcial para obtenção do título Bacharel em Biblioteconomia

Financiadora: CNPQ – N° do Projeto 5520

BANCA EXAMINADORA

Orientadora: Profa. Dra. Helen de Castro Silva Casarin - Universidade Estadual Paulista – UNESP/ Marília.

2º Examinador: Profa. Dra. Franciele Marques Redigolo - Universidade Estadual Paulista – UNESP/ Marília

3º Examinador: Prof. Dr. Jean Fernandes Brito - Universidade Estadual Paulista – UNESP/ Marília

Marília, 5 de dezembro de 2024

Dedico este trabalho a todos os professores, alunos e profissionais da educação pública, cuja dedicação transforma vidas e constrói futuros. Que este esforço seja um tributo à importância da educação como alicerce de uma sociedade mais justa e igualitária. Aos educadores, meu profundo respeito e gratidão.

AGRADECIMENTOS

O ano de 2024 foi marcado por muitas conquistas, mas também por perdas preciosas. Por isso, inicio meus agradecimentos dedicando este trabalho à memória da minha querida avó, Jurema de Almeida Rodrigues. Uma mulher forte e generosa, que sempre me ofereceu amor incondicional e dedicação. Sua força e seu carinho me inspiraram a seguir meus sonhos e enfrentar novos desafios sem medo. Tenho certeza de que, agora, ela está em um lugar maravilhoso, guiando meus passos e me abençoando com sua presença eterna em meu coração.

Agradeço profundamente aos meus pais: Jusseli de Almeida Rodrigues, a mãe mais carinhosa, empática e bondosa que existe, cujo amor e apoio foram fundamentais para que eu chegasse até aqui; e Valdir Costa dos Santos, o pai mais trabalhador, honesto e generoso que conheço, cuja dedicação incansável sempre será um exemplo.

Sou igualmente grato aos meus irmãos, Micheli Costa dos Santos e Cleiton Costa dos Santos, pelo apoio e amor ao longo desta jornada. E um agradecimento especial vai para o maior amor que tenho, minha irmã caçula, Raissa Costa dos Santos, um presente divino em minha vida. Sou extremamente grato por tê-la como a irmã mais carinhosa, amorosa e inteligente, cuja presença iluminou muitos momentos difíceis e me deu forças para continuar.

Agradeço de coração à minha orientadora e professora, Helen de Castro Silva Casarin, um verdadeiro exemplo de ser humano e profissional, em quem me espelho. Suas orientações, apoio e parceria em diversos trabalhos e eventos foram fundamentais para meu crescimento acadêmico e pessoal.

Minha gratidão também se estende à minha amiga, Caroline de Oliveira, cujo apoio incondicional foi uma fonte constante de motivação, carinho e companheirismo.

Meu reconhecimento vai ainda à banca examinadora, composta pela Profa. Dra. Franciele Marques Redigolo e pelo Dr. Jean Fernandes Brito, ambos da UNESP Marília, por suas valiosas contribuições.

Sou imensamente grato ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo financiamento do projeto número 5520, referente ao edital 4/2022 - PIBIC, que foi fundamental para o desenvolvimento deste trabalho de conclusão de curso, permitindo-me aprofundar ideias inovadoras e contribuir significativamente para a pesquisa na área.

À Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), expresso minha mais sincera gratidão por todo o suporte oferecido para minha permanência estudantil, desde o acesso a recursos até a excelência de seu

corpo docente. Esta instituição me proporcionou não apenas uma formação acadêmica de qualidade, mas também experiências transformadoras. Espero que este seja apenas o início de uma longa jornada nesta universidade que tanto admiro.

Não posso deixar de mencionar minha escola de ensino fundamental, a EMEIEF Martin Lutero, e minha escola de ensino médio, a Escola Estadual Professor Dorivaldo Damm, locais fundamentais na minha formação acadêmica e pessoal. Foi na Martin Lutero que construí as bases para o meu aprendizado, e na Dorivaldo Damm que fortaleci minha confiança e fiz amizades que levarei para a vida inteira. Ambas acreditaram no meu potencial e foram essenciais para que eu trilhasse este caminho.

Por fim, a todas as pessoas que, direta ou indiretamente, contribuíram para minha formação e caminhada, meu mais profundo obrigado. Este trabalho é o reflexo de uma jornada que só foi possível graças a cada um de vocês.

"A vida, senhor Visconde, é um pisca-pisca. A gente nasce, isto é, começa a piscar. Quem para de piscar chegou ao fim, morreu. Piscar é abrir e fechar os olhos – viver é isso."

Lobato, M. 2009, p. 16

Resumo

O aumento significativo de ataques cibernéticos e violações de dados durante a pandemia de Covid-19 evidenciou a necessidade de governança mais eficaz em segurança digital, especialmente em ambientes educacionais, onde controles formais são mais difíceis de implementar fora do espaço físico. Fatores humanos, como o domínio de competências digitais, desempenham papel crucial na proteção de privacidade e segurança. Nesse contexto, esta pesquisa tem como objetivo geral analisar como a Unesp aborda a proteção de privacidade e segurança digital de docentes e alunos em ambientes digitais. Os objetivos específicos incluem: (1) revisar e sistematizar a literatura científica sobre competências digitais, segurança e privacidade no trabalho remoto; (2) analisar as recomendações dos documentos DigComp 2.2 e DigCompEdu para segurança digital em contextos educacionais; (3) identificar materiais de autoformação nas páginas das Diretorias Técnicas de Informática (DTIs) dos campi da Unesp; e (4) analisar as portarias institucionais relacionadas à privacidade e segurança no trabalho remoto. A metodologia, de natureza quali-quantitativa, foi desenvolvida em três etapas. O levantamento dos materiais de autoformação relacionados à segurança digital foi realizado por meio das páginas web das DTIs dos 24 campi da Unesp, distribuídos no estado de São Paulo. O segundo levantamento ocorreu no site da Reitoria, analisando portarias publicadas entre 2020 e 2023. A última etapa envolveu a análise quali-quantitativa dos dados para propor ações formativas mais eficazes e recomendações para o fortalecimento da segurança digital. Os resultados revelaram que 7 das 37 DTIs não oferecem materiais de autoformação sobre segurança digital. Entre as 30 unidades restantes, apenas 2 (6,7%) contemplam todas as competências da Área 4 do DigComp, enquanto 22 (79,9%) abordam apenas uma competência. As DTIs analisadas também apresentaram documentos que abrangem nove das dez capacidades da Competência 6.4 do DigCompEdu. Em relação às portarias, foram analisados 491 documentos publicados entre 2020 e 2023. Apenas 8 mencionam "trabalho remoto" ou "híbrido", mas nenhuma delas aborda diretamente a proteção de dados ou riscos cibernéticos. Esse resultado evidencia a ausência de orientações específicas sobre segurança digital e privacidade para a comunidade acadêmica, mesmo em um período crítico como a pandemia. Conclui-se que é necessário ampliar as ações formativas e revisar as políticas institucionais, promovendo diretrizes específicas que integrem competências digitais e governança de segurança para fortalecer a proteção da comunidade acadêmica frente aos desafios da transformação digital.

Palavras-chave: Competência Digital; Segurança Digital; Formação de usuários; DigComp; DigCompEdu.

ABSTRACT

The significant increase in cyberattacks and data breaches during the Covid-19 pandemic highlighted the need for more effective digital security governance, especially in educational environments where formal controls are more difficult to implement outside of physical spaces. Human factors, such as the mastery of digital competencies, play a crucial role in protecting privacy and security. In this context, the general objective of this research is to analyze how Unesp addresses the protection of privacy and digital security for faculty and students in digital environments. The specific objectives include: (1) reviewing and systematizing the scientific literature on digital competencies, security, and privacy in remote work; (2) analyzing the recommendations from the DigComp 2.2 and DigCompEdu documents for digital security in educational contexts; (3) identifying self-training materials on the pages of the Information Technology Departments (DTIs) at Unesp's campuses; and (4) analyzing institutional regulations related to privacy and security in remote work. The methodology, of a qualitative-quantitative nature, was developed in three stages. The survey of self-training materials related to digital security was conducted through the web pages of the DTIs at 24 Unesp campuses located across the state of São Paulo. The second survey took place on the Rectorate's website, analyzing regulations published between 2020 and 2023. The final stage involved qualitative-quantitative analysis of the data to propose more effective training actions and recommendations for strengthening digital security. The results revealed that 7 out of 37 DTIs do not offer self-training materials on digital security. Among the remaining 30 units, only 2 (6.7%) address all the competencies of DigComp's Area 4, while 22 (79.9%) address only one competency. The DTIs analyzed also presented documents that cover nine of the ten capabilities of DigCompEdu's Competency 6.4. Regarding the regulations, 491 documents published between 2020 and 2023 were analyzed. Only 8 mention "remote" or "hybrid" work, but none address data protection or cybersecurity risks directly. These results highlight the lack of specific guidelines on digital security and privacy for the academic community, even during a critical period such as the pandemic. It is concluded that it is necessary to expand training actions and review institutional policies, promoting specific guidelines that integrate digital competencies and security governance to strengthen the protection of the academic community against the challenges of digital transformation.

Keywords: Digital Competence; Digital Security; User Training; DigComp; DigCompEdu.

LISTA DE QUADROS

Quadro 1 - Modelo conceitual do DigComp 2.2.....	22
Quadro 2 - Níveis de proficiência e seus respectivos estágios DigComp.....	26
Quadro 3 - Proteção de dispositivos.....	31
Quadro 4 - Proteção de dados pessoais e privacidade	33
Quadro 5 - Proteção da saúde e do bem-estar	34
Quadro 6 - Proteção do meio ambiente.....	35
Quadro 7 - Área 4 do DigComp 2.2 e Materiais de Formação Oferecidos pelas DTIs da Unesp	50
Quadro 8 - Competência 6.4: Uso responsável do DigCompEdu e Materiais de Formação Oferecidos pelas DTIs da Unesp.....	51
Quadro 9 - Portarias Unesp de 2020 relacionadas a atividades remotas.....	53
Quadro 10 - Portarias Unesp de 2021 relacionadas a atividades remotas.....	54
Quadro 11 - Portarias Unesp de 2023 relacionadas a atividades remotas.....	54

LISTA DE ABREVIATURAS E SIGLAS

Agetic	Agência de Tecnologia da Informação e Comunicação
BRAPCI	Base de Dados em Ciência da Informação
CAIS	Centro de Atendimento a Incidentes de Segurança
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.BR	Comitê Gestor da Internet no Brasil
CLP	Campus do Litoral Paulista/Instituto de Biociências
COVID-19	<i>Corona Vírus Disease 2019</i>
CP/M	<i>Control Program for Microcomputers</i>
DigComp	<i>DigitalCompetence Framework for Citizens</i>
DigCompEdu	<i>Digital Competence Framework for Educators</i>
DPC	Desenvolvimento Profissional Contínuo Digital
DTI	Diretoria Técnica de Informática
FAAC	Faculdade de Arquitetura, Artes, Comunicação e Design
FC	Faculdade de Ciências
FCA	Faculdade de Ciências Agrônômicas
FCAT	Faculdade de Ciências Agrárias e Tecnológicas
FCAV	Faculdade de Ciências Agrárias e Veterinárias
FCAVR	Faculdade de Ciências Agrárias do Vale do Ribeira
FCE	Faculdade de Ciências e Engenharia
FCFAR	Faculdade de Ciências Farmacêuticas
FCHS	Faculdade de Ciências Humanas e Sociais

FCLAR	Faculdade de Ciências e Letras
FCLAs	Faculdade de Ciências e Letras
FCT	Faculdade de Ciências e Tecnologia
FCTE	Faculdade de Ciências, Tecnologia e Educação
FEB	Faculdade de Engenharia
FEC	Faculdade de Engenharia e Ciências
FEG	Faculdade de Engenharia
FEIS	Faculdade de Engenharia
FESJ	Faculdade de Engenharia São João
FFC	Faculdade de Filosofia e Ciências
FMB	Faculdade de Medicina
FMVA	Faculdade de Medicina Veterinária
FMVZ	Faculdade de Medicina Veterinária e Zootecnia
FOA	Faculdade de Odontologia
FOAr	Faculdade de Odontologia
GTID	Grupo Técnico de Informação e Documentação
IA	Instituto de Artes
IB	Instituto de Biociências
IBB	Instituto de Biociências
IBGE	Instituto Brasileiro de Geografia e Estatística
IBILCE	Instituto de Biociências, Letras e Ciências Exatas
IBM	<i>International Business Machines Corporation</i>
ICE	Instituto de Ciências e Engenharia
ICT	Instituto de Ciência e Tecnologia

ICTS	Instituto de Ciência e Tecnologia de Sorocaba
IES	Instituições de Ensino Superior
IFT	Instituto de Física Teórica
IGCE	Instituto de Geociências e Ciências Exatas
IPPRI	Instituto de Políticas Públicas e Relações Internacionais
IQ	Instituto de Química
LGPD	Lei Geral de Proteção de Dados Pessoais
Nic.br	Núcleo de Informação e Coordenação do Ponto BR
NUMIS	Núcleo de Movimento Inclusão e Saúde
OMS	Organização Mundial da Saúde
PNED	Política Nacional de Educação Digital
RAMAC 350	<i>Random Access Method of Accounting and Control</i>
SciELO	<i>Scientific Electronic Library Online</i>
TDIC	Tecnologias Digitais da Informação e Comunicação
TIC	Tecnologias da Informação e Comunicação
UNESCO	<i>United Nations Educational, Scientific and Cultural Organization</i>
Unesp	Universidade Estadual Paulista “Júlio de Mesquita Filho”

Sumário

1 INTRODUÇÃO	14
1.1 Objetivo Geral	19
1.2 Objetivos específicos	19
2 Quadro Europeu de Referência de Competência Digital para os Cidadãos (DigComp).....	20
2.1 Segurança Digital.....	28
2.2 Segurança Digital e o DigComp.....	31
3 Quadro Europeu de Competência Digital para Educadores (DigCompEdu).....	38
4 CONTEXTUALIZAÇÃO DA PESQUISA.....	45
5 METODOLOGIA	46
6 RESULTADOS	49
7 CONCLUSÃO	56
REFERÊNCIAS	59

1 INTRODUÇÃO

As Tecnologias Digitais da Informação e Comunicação (TDIC) surgiram com o propósito de servir como ferramentas de desenvolvimento social e econômico em um panorama global de intenso avanço e demanda por conhecimento. Os serviços de telecomunicação se tornaram instrumentos poderosos para impulsionar o desenvolvimento social, atraindo grandes investimentos nacionais e internacionais e gerando inúmeros empregos em diversos setores (Brasil, 2018).

As TDIC permeiam todas as esferas e setores governamentais voltados a regular ou gerenciar as necessidades da sociedade. Uma das áreas em que as TDIC estão mais presentes é a educação. Nessa esfera, as ferramentas tecnológicas digitais atuam não apenas como instrumentos de apoio à comunidade acadêmica no processo de ensino, mas também como importantes meios de acesso à comunicação e cultura, e frequentemente relacionam-se com o Projeto Político-Pedagógico escolar (Anjos e Silva, 2018).

No primeiro semestre de 2020, as ferramentas digitais e tecnológicas tornaram-se extremamente necessárias, mais do que o normal, visto que, em 2020, o mundo adotou o modelo de trabalho remoto¹ devido à quarentena causada pelo *Corona Vírus Disease 2019* (COVID-19), uma doença infecciosa respiratória que afetou o modo de trabalho em todos os setores, tanto públicos quanto privados.

A comunidade acadêmica, assim como outros grupos, teve que adaptar suas atividades para o formato online, uma modalidade pouco difundida no país devido à fraca cultura de trabalho *home office*. Inicialmente, houve resistência tanto no setor público quanto no privado, agravada pela limitada qualificação oferecida por empresas e instituições de ensino a seus profissionais acerca da temática competência digital. Essa falta de preparo incluiu a formação

¹ O trabalho remoto é todo o trabalho que pode ser feito à distância, através da internet e dos nossos dispositivos (Remote Portugal, 2021).

insuficiente sobre o uso das TDIC, além da ausência de diretrizes claras sobre comportamento, proteção de imagem e segurança de dados de clientes e alunos.

As mudanças emergentes que ocorreram no processo de ensino frente o atual contexto da pandemia causada pelo novo coronavírus, levaram a adoção de metodologias, até então, não adotadas por muitos professores em seus ambientes de ensino. O que fez urgir a necessidade de inovação perante o ato de lecionar, buscando alternativas inovadoras para levar conhecimento aos seus alunos, com o intuito, sobretudo, de prover autonomia aos estudantes no seu processo de aprendizagem (Marques, 2020, p. 5).

Durante a pandemia de COVID-19, as Tecnologias da Informação e Comunicação (TIC) deixaram de ser apenas ferramentas para a busca de informação e se tornaram importantes instrumentos de comunicação entre professores e alunos, uma vez que o mundo entrou em isolamento social.

Para que as atividades educacionais prosseguissem, as instituições de ensino adotaram o ensino remoto como alternativa para ministrar aulas. No entanto, a capacitação em competência digital, abrangendo áreas como alfabetização em informação e dados, comunicação e colaboração, criação de conteúdo digital, resolução de problemas e principalmente o aspecto segurança, foi trabalhada de forma superficial e sem aprofundamento teórico e prático.

O Núcleo de Informação e Coordenação do Ponto BR (Nic.br) (2020) aponta que, durante a pandemia no Brasil, o apoio fornecido pelas empresas aos funcionários para o trabalho remoto foi desigual. Os participantes das classes A e B foram os que mais receberam suporte, ainda que apenas em torno de 50%. Nas demais classes, esse percentual ficou abaixo de 30%. Além disso, verificou-se um alto índice de uso de equipamentos pessoais, e apenas 20% dos participantes indicaram ter recebido acesso a aplicações de segurança digital, como antivírus. Diante disso, evidencia-se a preocupação restrita a equipamentos e não a fatores e qualificações humanas, como a competência digital, visto que elas desempenham um papel crucial na proteção da privacidade e da segurança dos indivíduos.

De acordo com o *Security Leaders* (2023), em 24 de setembro de 2023, a Universidade Federal do Mato Grosso do Sul sofreu um ataque cibernético em um de seus servidores que armazena dados pessoais, senhas e e-mails

institucionais de sua comunidade. O crime foi identificado pela Agência de Tecnologia da Informação e Comunicação (Agetic) da instituição. O incidente evidencia a fragilidade do sistema e a falta de habilidades relacionadas à competência em segurança digital para prevenir ameaças cibernéticas na comunidade acadêmica.

Segundo Lallie *et al.* (2021), os ciberataques tornam-se mais frequentes em momentos de estresse social, como desastres naturais, catástrofes, eventos de grande impacto envolvendo celebridades ou campanhas de saúde, a exemplo da pandemia. Os criminosos aproveitam a sensibilização das vítimas nesses períodos para enganá-las. Para testar essa hipótese, os pesquisadores elaboraram uma linha do tempo que abrange desde o alerta da China à Organização Mundial da Saúde (OMS) sobre os primeiros casos da doença até a incidência de ataques cibernéticos em meados de maio de 2020. Os resultados mostraram uma intensificação global desses ataques ao longo do período estudado, as consequências incluíram grandes prejuízos financeiros para pessoas e empresas, além de crimes como roubo de identidade, sequestro de dados e imagens.

Segundo o estudo realizado pela MetaRede, que contou com a participação de 3.100 docentes de Instituições de Ensino Superior (IES) públicas e privadas em diversas regiões do país, 80% dos professores passaram a utilizar ferramentas digitais e outros recursos em suas aulas. Conforme os dados da pesquisa, "mais de 60% [dos participantes] possui entre 1 e 9 anos de uso de TIC em suas atividades de ensino, e as tecnologias mais citadas ainda se restringiam a: apresentações em *PowerPoint* e uso de recursos de áudio e vídeo", o que revela o distanciamento de boa parte dos docentes em relação às ferramentas disponíveis para o ensino remoto. No entanto, o estudo não incluiu questões específicas sobre os cuidados dos professores com segurança e privacidade, tanto para si mesmos quanto para seus alunos (Carvalho; Marroni; Tavares, 2020).

Conforme o levantamento de Haynes (2019), o trabalho remoto expõe o indivíduo a diversos riscos, como divulgação de circunstâncias domésticas, identificação de outros membros da família, cruzamento de documentos

peçoais em sistemas dos empregadores e divulgação de localização e movimentos.

Para mitigar os riscos relacionados à segurança e privacidade das pessoas no uso de recursos digitais, são necessárias soluções técnicas e regulamentações sobre o tema; entretanto, elas ainda são insuficientes e, no caso das regulamentações, geram bastante controvérsia. No Brasil, a legislação sobre essa temática ainda está em fase de estruturação. Em 2014, foi aprovado o 'Marco Civil da Internet', que estabelece princípios, garantias, direitos e deveres para o uso da internet no país. Mais recentemente, em 2020, entrou em vigor a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), que passou a ser exigida das empresas e organizações. Como afirma o relatório do Science Hub:

[...] devemos enxergar a cibersegurança como um desafio societal, e não apenas tecnológico. Ela exige mudanças comportamentais em todas as partes da sociedade. Trata-se de uma questão de educação, cultura, política e políticas públicas (Flavino, *et al.*, 2020, p. 7, tradução nossa).²

Diversos autores e instituições destacam que, além das soluções técnicas e regulamentações, é fundamental criar uma cultura de segurança no uso de recursos tecnológicos, o que envolve a educação das pessoas sobre essa temática (Furnell; Shah, 2020). No entanto, no contexto brasileiro, ainda há muito a ser feito nesse sentido.

Segundo estudos de Soares, Araujo e Souza (2020), revela-se que, mesmo entre estudantes da área de computação, que possuem maior conhecimento técnico sobre a temática segurança digital, são comuns comportamentos de risco no uso de dispositivos digitais, isso evidencia a necessidade de uma formação que promova hábitos mais seguros no uso de tecnologias digitais.

A Universidade Estadual Paulista “Júlio de Mesquita Filho” (Unesp) é uma das maiores e mais renomadas instituições públicas de ensino superior do Brasil. Com presença em 24 cidades do estado de São Paulo, a universidade

² [...] we must see cybersecurity as a societal, not just a technological, challenge. It requires behavioral change in all parts of society. It is a matter of education, culture, politics and policies (Flavino, *et al.*, 2020, p. 7)

desempenha um papel fundamental na formação de profissionais altamente qualificados, além de se destacar por sua produção científica e iniciativas de internacionalização.

No contexto da pandemia de COVID-19, a Unesp enfrentou o desafio de implementar o ensino remoto de forma ampla e ágil, exigindo a adaptação de sua estrutura tecnológica e a capacitação de seu corpo docente e discente. Essa transição trouxe à tona questões cruciais relacionadas à segurança digital, especialmente no que tange à proteção de dados, privacidade e boas práticas no digital.

Este trabalho analisa as portarias institucionais emitidas entre 2020 e 2023, que abordam competências em segurança digital para o trabalho remoto, bem como os materiais de autoformação disponibilizados pelas Diretorias Técnicas de Informática (DTIs) em diferentes unidades de ensino. A investigação busca compreender como essas ações refletem as estratégias da Unesp para enfrentar os desafios impostos pela transformação digital no ambiente acadêmico.

O início das investigações da presente comunicação, que aborda a temática “proteção de dados pessoais, privacidade e segurança digital”, ocorreu em setembro de 2022, período em que a pandemia de COVID-19 ainda estava em curso. Esse contexto destacou a importância e a crescente dependência da sociedade em relação à tecnologia para garantir a continuidade das atividades educacionais.

Ao mesmo tempo, evidenciou inúmeras lacunas, como a vulnerabilidade das instituições e a falta de competências digitais de professores e alunos, especialmente no que se tange à proteção, segurança e privacidade em ambientes online. Esse cenário reforça a relevância de desenvolver e aprimorar competências digitais que capacitem os indivíduos para atuar com segurança nos ambientes online, minimizando os riscos e fortalecendo práticas educacionais em ambientes digitais.

A presente comunicação justifica-se pela necessidade e importância de investigar e propor reflexões que minimizem fragilidades e promovam competências digitais relacionadas à segurança, viabilizando o uso seguro das

TDIC. Paralelamente, busca-se fortalecer a privacidade e a proteção de dados nos contextos educacionais de nível superior, além de estimular a autoformação da comunidade acadêmica acerca da temática.

O estudo busca contribuir para o aprimoramento de práticas seguras em ambientes digitais, alinhando-se de forma concisa às demandas da sociedade contemporânea e ao fortalecimento da educação em um cenário cada vez mais mediado pela tecnologia.

Questão de pesquisa: Quais são as orientações institucionais da Universidade Estadual Paulista “Júlio de Mesquita Filho” (UNESP) em relação à proteção de dados pessoais, privacidade e segurança digital para discentes e docentes no contexto do trabalho remoto?

1.1 Objetivo Geral

- Verificar como a UNESP tem lidado com a proteção da privacidade e segurança digital de docentes e alunos no ambiente digital³.

1.2 Objetivos específicos:

- A) Revisar e sistematizar a literatura sobre os temas competência digital, segurança e privacidade no trabalho remoto.
- B) Identificar materiais de autoformação disponíveis nas webpages das Diretorias Técnicas de Informática (DTI) dos 24 campi da UNESP, com foco na segurança digital e privacidade.
- C) Analisar as recomendações dos documentos *DigComp 2.2* e *DigCompEdu* relacionadas à segurança digital e privacidade em contextos educacionais, alinhando-as às orientações das portarias da UNESP voltadas à comunidade acadêmica no trabalho remoto.

³ Ambiente digital é um espaço virtual que pode ser acessado pela Internet, permitindo que os usuários interajam com outros e se envolvam em várias atividades usando diferentes dispositivos, plataformas de mídia social ou tecnologia de realidade virtual (Floresta; Wexler, 2023).

2 Quadro Europeu de Referência de Competência Digital para os Cidadãos (DigComp)

O acesso da população brasileira a serviços e dispositivos digitais vem crescendo expressivamente nos últimos anos. De acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE, 2022), o acesso à internet no Brasil chegou a 90,0% na área urbana e 84,0% na área rural. Observa-se que as Tecnologias da Informação e Comunicação (TIC) mais utilizadas para acesso à internet são: 99,5% utilizam *smartphones*, 44,4% televisores, 42,2% computadores e 9,9% *tablets*.

As TIC são ferramentas digitais necessárias e utilizadas em todo o mundo. Elas têm por finalidade armazenar e processar informações, além de servirem como instrumentos de comunicação entre diversos dispositivos, facilitando a disseminação e o compartilhamento de informações.

O desenvolvimento e aprimoramento das TIC trouxeram inúmeros benefícios para a sociedade e, conseqüentemente, uma das áreas mais impactadas por essas ferramentas foi a educação. Um fato histórico marcante sobre as TIC na educação foi a inserção de computadores nas escolas brasileiras. A partir da introdução dessas máquinas nas instituições de ensino, a educação avançou significativamente na busca e utilização da informação. Atualmente, outros dispositivos com conexão à internet, como *smartphones*, *notebooks* e *tablets*, predominam no ambiente educacional, tornando o acesso às TIC acessível a uma parcela notável da sociedade. Esses dispositivos vêm crescendo exponencialmente em diversas áreas, como comunicação social, segurança, indústria e educação (Rodrigues, 2016).

As TIC desempenham um papel fundamental no mundo contemporâneo, impactando diretamente o papel desempenhado por docentes, fazendo dos professores não apenas transmissores de conhecimento, mas também guias do aprendizado e do processo de construção do conhecimento (Cantabrana; Cervera; Queiroz, 2020).

Para Barros *et al.* (2011), a utilização das TIC nos ambientes escolares está cada vez mais presente, trazendo novos desafios pedagógicos e exigindo a redefinição das funções dos diversos profissionais envolvidos no processo

educativo. Nesse contexto, as TIC podem ser compreendidas tanto como ferramentas que reforçam os métodos tradicionais quanto como oportunidades para atualizar práticas mais antigas de ensino. Com o auxílio das TIC, os alunos deixam de ocupar apenas a posição de receptores de conhecimento, tornando-se agentes ativos na construção e na partilha do saber.

Para que as competências digitais, relacionadas ao uso das TIC, sejam plenamente desenvolvidas, o corpo docente necessita estar preparado para ensinar seus alunos a utilizarem essas tecnologias em seu potencial, com responsabilidade e segurança. Ou seja, o ensino da competência digital, que abarque: literacia da informação e de dados, comunicação e colaboração, criação de conteúdo digital, segurança e resolução de problemas.

Durante a pandemia de COVID-19, a utilização das TIC se intensificou em todos os setores, tanto público quanto privado. Esse uso intenso dos dispositivos eletrônicos e plataformas virtuais foi resultado da suspensão das atividades presenciais em resposta ao isolamento social causado pelo coronavírus. Diante deste cenário, as escolas tiveram de se preparar de forma instantânea, com o intuito de suprir as necessidades educacionais de seus alunos, e trabalhando aspectos relacionados à competência digital.

O termo *Digital Competence* (Competência Digital) surge em meados de 2006, no relatório *Recommendation Of The European Parliament and of the Council: On Key Competences for Lifelong Learning* ⁴realizado pela Comissão Europeia de cultura e educação, o objetivo da conferência foi discutir e identificar as abordagens e direcionamentos resultantes na Europa sobre a temática *Media Literacy* (Letramento em Mídias), na reunião foi apresentado um modelo contendo 8 competências essenciais para o aprendizado ao longo da vida, incluindo a competência digital, que tem como base a utilização das Tecnologias Digitais da Informação e Comunicação (TDIC) de forma efetiva, crítica e segura, no trabalho, lazer e comunicação. A partir dessa conferência, a União Europeia inicia um movimento focado no desenvolvimento de estudos destacando o termo

⁴ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:394:0010:0018:en:PDF>

frameworks de competências digitais para a comunidade europeia (Silva; Behar, 2019).

Com o surgimento de inúmeros dispositivos tecnológicos, que atuam como mediadores no processo de comunicação e busca de informação, surgiram algumas dificuldades e desafios relacionados à alfabetização digital, comunicação, resolução de problemas e, não menos importante, à segurança informacional dos usuários. Todos esses tópicos são abordados pelo DigComp (Quadro Europeu de Referência para o Desenvolvimento e Compreensão da Competência Digital), referencial cuja primeira versão surgiu em 2013, por meio de reuniões realizadas pelo Parlamento Europeu e pela Comissão Europeia de Cultura e Educação. A partir dessas conferências e dos relatórios elaborados por ambas as organizações, nasceu o DigComp.

As competências digitais presentes no documento DigComp são combinações de conhecimentos, habilidades e atitudes desenvolvidas ao longo da vida. O documento, criado pelo Parlamento Europeu, recebeu algumas atualizações desde sua primeira edição; as alterações são decorrentes das evoluções tecnológicas que ocorreram ao longo dos anos. O mais recente “DigComp 2.2” abrange temáticas como inteligência artificial, internet das coisas, realidade aumentada e virtual, dataficação, desinformação, aspectos tecnológicos e sustentabilidade. Essas habilidades são necessárias para serem desenvolvidas pelos cidadãos, visto que essas temáticas permeiam a sociedade, impactando diretamente as atividades do cotidiano. Essas e outras questões são abordadas em cinco áreas pré-estabelecidas no DigComp 2.2:

Quadro 1 - Modelo conceitual do DigComp 2.2

Áreas	Competências
Literacia de informação e de dados	1.1 Navegação, procura e filtragem de dados, informação e conteúdo digital. 1.2 Avaliação de dados, informação e conteúdo digital. 1.3 Gestão de dados, informação e conteúdo digital.
Comunicação e Colaboração	2.1 Interpretação através de tecnologias digitais. 2.2 Partilha através de tecnologias digitais 2.3 Envolvimento na cidadania através de tecnologias digitais. 2.4 Colaboração através de tecnologias digitais 2.5 Netiqueta 2.6 Gestão da Identidade Digital

Criação de Conteúdo Digital	3.1 Desenvolvimento de conteúdo digital. 3.2 Integração e reelaboração de conteúdo digital. 3.3 Direitos de autor e licença. 3.4 Programação.
Segurança	4.1 Proteção de dispositivos 4.2 Proteção de dados pessoais e privacidade 4.3 Proteção da saúde e do bem-estar. 4.4 Proteção do meio ambiente.
Resolução de Problemas	5.1 Resolução de problemas técnicos. 5.2 Identificação de necessidades e respostas tecnológicas. 5.3 Utilização criativa das tecnologias digitais. 5.4 Identificação de lacunas nas competências digitais.

Fonte: Lucas; Moreira e Trindade, 2022.

A primeira área do DigComp 2.2 trabalha com dimensões voltadas à navegação, busca de dados e conteúdos digitais, abrangendo a gestão e avaliação de fontes informacionais. Quanto às competências e habilidades desenvolvidas nesta área, pode-se apontar a articulação das necessidades de informação, a localização e recuperação de informações e conteúdos digitais, a análise, comparação e avaliação crítica da confiabilidade e credibilidade das fontes informacionais digitais utilizadas para as buscas, além da organização, armazenamento, recuperação de dados e informações, incluindo seu processamento em um ambiente digital estruturado.

A segunda área volta-se a comunicação e colaboração, desenvolvendo habilidades e competências digitais relacionadas à interação do usuário com as diversas TDIC, abordando questões voltadas aos modos mais apropriados de comunicação digital para diferentes contextos. Outro ponto trabalhado é a partilha de dados e informações através de tecnologias digitais. Ao realizar o compartilhamento de dados e informações, é necessário analisar qual tecnologia digital é apropriada, conhecer práticas de referência e atribuição de autoria, habilidades desenvolvidas nesta área.

O envolvimento na cidadania através de tecnologias digitais é abordado, com ênfase na participação da sociedade através da utilização dos serviços digitais públicos e privados, além da busca por oportunidades de autocapacitação para uma participação cidadã mais intensa através das tecnologias digitais. As colaborações são um ponto importante destacado pelo DigComp 2.2, visto que as ferramentas digitais servem como parte do processo

colaborativo e de construção e co-criação de recursos e conhecimentos adequados entre cidadãos. Além disso, trabalha-se a habilidade do cidadão em criar ou gerenciar uma ou diversas identidades digitais, seja para fins pessoais ou profissionais, desenvolvendo a competência de proteger sua reputação e lidar com os dados produzidos através das diversas ferramentas e ambientes digitais.

A terceira área aborda a criação de conteúdo digital, trabalhando habilidades de desenvolvimento de tópicos centrados em competências voltadas à criação e edição de conteúdos digitais em diferentes formatos, como vídeos, fotografias, áudio etc. De modo que o usuário consiga expressar-se através dos meios digitais. Outro aspecto é a integração e reelaboração de conteúdos digitais, ou seja, a modificação e aperfeiçoamento através da inserção de informações em uma estrutura já existente de conhecimento, elaborando novos conhecimentos de cunho original e relevante.

Outro aspecto importante trabalhado na área 3 direciona-se aos direitos de autor e licença. É de extrema importância que os usuários compreendam os direitos dos autores e as licenças aplicadas aos dados, à informação e aos conteúdos digitais utilizados. A programação também é abordada no documento, com destaque no planejamento e desenvolvimento de instruções ou procedimentos acessíveis, de fácil compreensão, para que um sistema computacional resolva determinados problemas ou até mesmo realize uma tarefa complexa ou específica.

A quarta área do DigComp 2.2 aborda como tópico central a segurança digital. Os aspectos tratados incluem a proteção de dispositivos, desenvolvendo habilidades e competências voltadas para a percepção de riscos e ameaças presentes em ambientes digitais. Além disso, são desenvolvidos conhecimentos sobre medidas de segurança, levando em consideração a privacidade e confiabilidade. A proteção de dados pessoais envolve competências relacionadas à privacidade e confiabilidade de informações privadas, compreendendo como utilizar e compartilhar essas informações de forma segura, protegendo tanto os próprios dados quanto os de terceiros. É fundamental compreender que os serviços digitais possuem políticas de privacidade, nas quais é informado como serão utilizados os dados dos usuários.

O aspecto da proteção da saúde e do bem-estar aborda o desenvolvimento da capacidade de evitar riscos, tanto psicológicos quanto físicos. As competências trabalhadas têm como objetivo tornar o usuário capaz de se proteger de perigos nos ambientes digitais. Um exemplo é o *cyberbullying*⁵; quando se sentir ameaçado, o usuário conseguirá identificar os ataques e realizar os processos necessários de denúncia aos órgãos responsáveis.

A temática percorrida acima adquiriu maior relevância em tempos de pandemia, uma vez que, durante esse período, inúmeras instituições públicas e privadas foram amplamente alvo de ataques virtuais. A quarta área do Quadro Europeu de Competência Digital para Cidadãos, que era escassamente discutida, ganhou destaque durante o momento pandêmico, evidenciando as significativas lacunas no que diz respeito à segurança da informação, aspecto esse que era pouco considerado nas instituições de diversas esferas. Os tópicos destacados na seção de segurança do DigComp 2.2 referem-se à proteção de dispositivos fixos ou móveis e à preservação de dados pessoais, tais como endereço, telefone, número do documento de identidade ou cartões de crédito, além do resguardo de contra-ataques cibernéticos.

A quinta e última área do DigComp 2.2 aborda a resolução de problemas como ponto central. As competências e habilidades desenvolvidas são direcionadas para a identificação de problemas técnicos em dispositivos e sua resolução utilizando ambientes digitais. Essas competências envolvem a resolução de problemas, desde os mais simples até os mais complexos. A identificação de necessidades e respostas tecnológicas aborda a identificação e avaliação das necessidades, seguida pela utilização de ferramentas digitais para corrigi-las. A personalização e ajustes de acordo com as necessidades do usuário desses ambientes digitais também são tratados no desenvolvimento dessas competências.

Além disso, também se explora na quinta área a utilização criativa das tecnologias, com ênfase na utilização de ferramentas e tecnologias digitais para

⁵ Cyberbullying é o bullying realizado por meio das tecnologias digitais. Pode ocorrer nas mídias sociais, plataformas de mensagens, plataformas de jogos e celulares. É o comportamento repetido, com intuito de assustar, enfurecer ou envergonhar aqueles que são vítimas (Unicef, 2020).

criar conhecimentos e inovar nos processos e produtos concebidos. Por último, mas não menos importante, é abordada a identificação de lacunas na competência digital, onde o usuário compreende em quais áreas sua competência digital precisa ser aperfeiçoada ou atualizada. Além disso, desenvolvem-se aspectos relacionados à capacidade de apoiar outros usuários no desenvolvimento de sua competência digital, procurando sempre oportunidades para o autodesenvolvimento e mantendo-se atualizado com a evolução digital.

Adicionalmente, pode-se apontar que, além das áreas trabalhadas acima, há um sistema de nivelamento para cada uma delas e para as competências desenvolvidas, são quatro níveis de proficiência e oito estágios:

Quadro 2 - Níveis de proficiência e seus respectivos estágios DigComp

Nível 1		Nível 2		Nível 3		Nível 4	
1	2	3	4	5	6	7	8
Básico		Intermédio		Avançado		Especializado	

Fonte: Luca; Moreira e Trindade, 2022.

O sistema de nivelamento idealizado por Lucas e Moreira (2022), possui quatro modos; básico, intermediário, avançado e especializado, o modo básico abrange o primeiro nível de proficiência, e concomitantemente os estágios 1 e 2, neles são desenvolvidos habilidades e competências para a realização de tarefas e processos digitais tidos como básicos, no primeiro estágio é necessário a orientação de um profissional especializado, no segundo o usuário possui uma determinada autonomia, entretanto quando houver uma necessidade específica é fundamental a orientação de um profissional competente digitalmente, quanto os domínios cognitivos, os autores apontam o “lembrar”, ou seja, recordar como realizar determinadas atividades ou tarefas.

O modo intermediário compreende o segundo nível e os estágios 3 e 4. A complexidade das operações é definida pelos autores como sendo: tarefas bem definidas e rotineiras, problemas simples; tarefas e problemas bem definidos não rotineiros e problemas simples. Quanto à autonomia dos usuários no estágio 3, estes conseguem utilizar as tecnologias de forma independente. No estágio 4, eles se tornam independentes do ponto de vista informacional, utilizando as tecnologias de acordo com suas necessidades.

O modo avançado abrange o terceiro nível e os estágios 5 e 6. As complexidades apontadas pelos autores são bem definidas como tarefas e problemas distintos, além de tarefas mais apropriadas. Quanto à autonomia, os usuários nesse nível conseguem orientar outras pessoas, além de se adaptarem a outros em um contexto complexo. No que diz respeito aos seus domínios cognitivos, Lucas e Moraes (2017) apontam que os usuários conseguem aplicar as habilidades desenvolvidas, além de realizar avaliações.

O último modo é o avançado, inserido no nível 4, onde estão incluídos os estágios 7 e 8. As complexidades deste modo são definidas como problemas complexos com definição limitada e problemas complexos, com muitos fatores que interagem entre si. Quanto à autonomia do usuário, ele é categorizado como integrado para contribuir para a prática profissional devido ao seu nível de competência digital, além de orientar e propor novas ideias e processos para a área. Quanto ao seu domínio cognitivo, ele é definido pelo termo criar, ou seja, criar conteúdos originais e significativos para a área em que está inserido.

Quanto a guias, cartilhas, manuais, folhetos e diretrizes que abordam a temática competência digital no Brasil, pode-se apontar os documentos elaborados em conjunto com as instituições: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Núcleo de Informação e Coordenação do Ponto BR (NIC.br) e Comitê Gestor da Internet no Brasil (CGI.br), os materiais se direcionam ao desenvolvimento de competências no que diz respeito a; *Acessibilidade na Web* (2023), *Trabalho remoto: Cartilha de Segurança para Internet* (2023), *Backup: Cartilha de Segurança para Internet* (2023), *Banco via Internet: Cartilha de Segurança para Internet* (2023), *Redes Sociais: Cartilha de Segurança para Internet* (2023), *Phishing e Outros Golpes: Segurança para Internet* (2022), *Acessibilidade na Web (Fascículo I)* (2022), *Acessibilidade na Web (Fascículo II)* (2022), *Redes: Cartilha de Segurança para Internet* (2018), *Verificação em Duas Etapas - Cartilha de Segurança para Internet* (2018), *Computadores - Cartilha de Segurança para Internet* (2018), *Internet Banking - Cartilha de Segurança para Internet* (2018), *Internet Banking - Cartilha de Segurança para Internet* (2018), *Dispositivos Móveis - Cartilha de Segurança para Internet* (2018), *Privacidade - Cartilha de Segurança para Internet* (2018), *Comércio Eletrônico - Cartilha de Segurança para Internet*

(2018), Senhas - Cartilha de Segurança para Internet (2018), internet Segura: Divirta-se e aprenda a usar a Internet de forma segura! (2017) e Internet Segura para seus filhos: sua participação é muito importante! (2018). Todas essas cartilhas estão disponíveis de forma gratuita através do site NIC.br.

2.1 Segurança Digital

A primeira máquina considerada precursora do computador moderno foi desenvolvida por uma equipe liderada pelo matemático e criptógrafo inglês Alan Turing durante a Segunda Guerra Mundial (1939–1945). Turing e sua equipe trabalhavam em Bletchley Park, um centro de inteligência britânico dedicado à decifração de códigos nazistas (Alves, 2019).

O sistema utilizado por Turing e sua equipe era denominado *bombe*, sua função principal era decifrar códigos complexos e mensagens secretas trocadas entre os nazistas. Mesmo após a Segunda Guerra Mundial, a preocupação com a proteção de informações continuou sendo extremamente relevante, especialmente durante a Guerra Fria (1947-1991), período em que a segurança da informação se expandiu significativamente. Diversas estratégias, códigos e criptografias foram desenvolvidos, entre elas a chave assimétrica, que é formada por duas chaves: uma pública, destinada a mensagens que podem ser amplamente compartilhadas, e uma privada, que protege mensagens que somente o detentor da chave pode abrir ou editar (Silva *et al.*, 2019).

Dois anos após o final da Segunda Guerra Mundial, iniciou-se a Guerra Fria (1947–1991), um conflito indireto entre os Estados Unidos e a União Soviética (URSS). Nesse confronto, o poder era medido pelo domínio tecnológico, pois o objetivo de ambos os lados incluía a conquista da órbita terrestre. Com isso, houve um expressivo avanço tecnológico, resultando no desenvolvimento de inúmeras tecnologias voltadas à construção e aprimoramento de naves espaciais, que tinham como meta a exploração e conquista do território lunar.

Junto a esses significativos desenvolvimentos tecnológicos, em 1956, a *International Business Machines Corporation* (IBM) desenvolveu o primeiro computador com sistema de armazenamento. A máquina, denominada *Random Access Method of Accounting and Control* (RAMAC 350), foi a primeira a contar

com um sistema de armazenamento em disco rígido, ou seja, um disco com cabeçote de leitura móvel (Costa; Pinto, 2017).

Na década de 80, foi lançado o primeiro computador portátil, chamado *Osborne Portable Computer*. A máquina foi um sucesso instantâneo entre os usuários de tecnologia da época. O computador era relativamente leve e de fácil manuseio para os padrões de então; no entanto, seu tamanho era considerável em comparação com os computadores portáteis atuais. Foi pioneiro no uso de telas LCD, uma grande novidade na época. Seu sistema operacional era o *Control Program for Microcomputers* (CP/M), desenvolvido nas décadas de 70 e 80, e pioneiro na execução de diversos aplicativos em uma mesma máquina (Shallit, 1995).

De acordo com Shallit (1995), o *Osborne Portable Computer* contava com diversos aplicativos pré-instalados, incluindo um editor de texto, banco de dados e planilha eletrônica, o que o tornava popular entre os profissionais que utilizavam essas aplicações. Embora a máquina tenha sido um grande sucesso, não conseguiu acompanhar o mercado e foi descontinuado em 1985. No entanto, deixou um legado de visão e inovação no meio tecnológico.

A partir da popularização dos computadores em empresas e instituições governamentais, a segurança da informação começou a ganhar cada vez mais relevância nos anos 80, visto que, para as instituições, “a informação é um ativo que, como qualquer outro, é essencial para os negócios de uma organização e, conseqüentemente, necessita ser adequadamente protegida” (Nakamura; Geus, 2002, p.9).

O século XXI é conhecido como a era da informação, devido aos grandes avanços tecnológicos que estimulam uma produção exponencial e, ao mesmo tempo, o consumo informacional. A informação assume sua importância em razão da mudança do paradigma da sociedade industrial para a sociedade da informação. A era industrial tinha como princípio fundamental a associação dos recursos terra, trabalho e capital como forma de criar riquezas. Nessa nova era, a informação é o recurso mais importante para agregar valor às organizações, razão pela qual é imprescindível identificar a percepção do seu valor nos ambientes organizacionais (Mascarenhas Neto; Araújo, 2019).

O Ministério Público Federal (2019) aponta que as grandes empresas de tecnologia na internet coletam uma grande quantidade de informações pessoais de seus usuários para, posteriormente, comercializar esses dados. Um exemplo citado pelo Ministério Público Federal é a empresa Google: os dados captados são tratados com o auxílio de técnicas desenvolvidas por inteligência artificial ou métodos estatísticos, visando condensar preferências pessoais, hábitos e outras tipologias de dados. A partir da extração dessas informações, são criados perfis (*profiling*) que permitem direcionar mensagens publicitárias de determinados serviços ou produtos a seus potenciais compradores.

Na cultura ocidental, ter a privacidade resguardada significa possuir autonomia, escolha ou poder sobre o uso de suas informações em um determinado ambiente digital. Navarro e Leonardos (2012) destacam que a definição de privacidade pode variar de acordo com o local, devido a diferenças culturais, bem como a variações no espaço e no tempo, que influenciam a compreensão do corpo social sobre o que é íntimo ou privado. Esses fatores incluem condições econômicas, sociais, religiosas, ambientais e políticas.

Para Gouveia (2016), a segurança e a privacidade da informação têm como objetivo a proteção dos dispositivos e sistemas que utilizam, transmitem ou armazenam informações. No meio corporativo, o objetivo da segurança da informação é proteger a privacidade dos dados, garantindo a continuidade dos negócios e preservando seu valor como ativo.

No Brasil, as preocupações governamentais com a proteção e privacidade de dados pessoais se intensificaram a partir da segunda década do século XXI, quando a Lei nº 12.965, de 23 de abril de 2014, foi sucedida pela Lei nº 13.709, de 14 de agosto de 2018. O Art. 2º da nova lei estabelece os fundamentos que ela disciplina para a proteção de dados pessoais, os quais incluem: respeito à privacidade; autodeterminação informativa; liberdade de informação, expressão, opinião e comunicação; inviolabilidade da intimidade, imagem e honra; desenvolvimento tecnológico e econômico; livre iniciativa; livre desenvolvimento da personalidade; dignidade; e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

[...] a reivindicação de privacidade de uma pessoa geralmente é justificada com base em uma lógica de propriedade e emprego:

uma pessoa possui suas próprias informações (seus fatos intimamente relacionados) e têm o direito de exercer controle total sobre elas, por exemplo, vendê-las, divulgá-las, escondê-las, e assim por diante. Segue-se que o problema moral é normalmente pensado para consistir tanto na aquisição e uso impróprios da propriedade de outra pessoa, quanto no tratamento instrumental de um ser humano, que é reduzido a números e coleções de informações sem vida. (Floridi, 1999, p. 53, tradução nossa)

Além das preocupações voltadas aos dados pessoais, o Estado destaca-se pelos cuidados concentrados na proteção da imagem, como uma das principais características da identidade pessoal. No ano de 2003, antes da grande difusão da internet entre a massa social brasileira, já existiam preocupações relacionadas à proteção da imagem. O artigo 2º e parágrafo único do Decreto Municipal de São Paulo (2003) regulamenta a Lei Municipal nº 13.541, de 24 de março de 2003, que estabelece a obrigação de ambientes localizados em São Paulo, protegidos por câmeras, informar que o local está sendo filmado por questões de segurança. As imagens gravadas devem ser consideradas confidenciais e protegidas por lei, ou seja, não poderão ser divulgadas, compartilhadas ou comercializadas.

2.2 Segurança Digital e o DigComp

Os pontos abordados no DigComp 2.2 (Lucas e Moreira, 2022) na área 4 referentes à segurança dividem-se em quatro subdivisões. Dentro de cada uma das subáreas, o documento apresenta oito níveis de proficiência, do básico ao altamente especializado, os quais são:

Quadro 3 - Proteção de dispositivos

Níveis		Competências
Básico	1	• Identificar formas simples de proteger os meus dispositivos e conteúdo digital; • distinguir riscos e ameaças simples em ambientes digitais; • selecionar medidas de segurança e proteção simples.
	2	• identificar formas simples de respeitar a fiabilidade e a privacidade; • identificar formas simples de proteger os meus dispositivos e conteúdo digital; • distinguir riscos e ameaças simples em ambientes digitais; • seguir medidas de segurança e proteção simples; • identificar formas simples de respeitar a fiabilidade e a privacidade.

Intermediário	3	• Indicar formas bem definidas e rotineiras de proteger os meus dispositivos e conteúdo digital; • distinguir riscos e ameaças bem definidos e rotineiros em ambientes digitais; • selecionar medidas de segurança e proteção bem definidas e rotineiras; • indicar formas bem definidas e rotineiras de respeitar a fiabilidade e a privacidade.
	4	• Organizar formas de proteger os meus dispositivos e conteúdo digital; • distinguir riscos e ameaças em ambientes digitais; • selecionar medidas de segurança e proteção; • explicar formas de respeitar a fiabilidade e a privacidade.
Avançado	5	• Aplicar diferentes formas de proteger dispositivos e conteúdo digital; • distinguir uma variedade de riscos e ameaças em ambientes digitais; • aplicar medidas de segurança e proteção; • empregar diferentes formas de respeitar a fiabilidade e a privacidade.
	6	• Escolher a proteção mais apropriada para dispositivos e conteúdo digital; • discriminar riscos e ameaças em ambientes digitais; • escolher as medidas de segurança e proteção mais apropriadas; • avaliar as formas mais apropriadas de respeitar a fiabilidade e a privacidade.
Altamente especializado	7	• Criar soluções para problemas complexos, com definição limitada, relacionadas com a proteção de dispositivos e conteúdo digital, gestão de riscos e ameaças, aplicação de medidas de segurança e proteção, e fiabilidade e privacidade em ambientes digitais; • integrar o meu conhecimento para contribuir para a prática e conhecimento profissional e orientar outros na proteção de dispositivos.
	8	• Criar soluções para resolver problemas complexos, com muitos fatores que interagem entre si, relacionadas com a proteção de dispositivos e conteúdo digital, gestão de riscos e ameaças, aplicação de medidas de segurança e proteção, e fiabilidade e privacidade em ambientes digitais; • propor novas ideias e processos para a área.

Fonte: Lucas; Moreira e Trindade, 2022, p.35.

O subtópico Competência 4.1 Proteção de dispositivos garante a competência de usuários acerca de formas de proteção de dispositivos e conteúdos digitais, identificação de métodos que respeitem a segurança e a privacidade informacional, conseguir explicar medidas de segurança, criar soluções para ameaças relacionadas à proteção de dispositivos, além de interagir o conhecimento acerca da temática.

Quadro 4 - Proteção de dados pessoais e privacidade

Níveis		Competências
Básico	1	• Selecionar formas simples de proteger os dados pessoais e privacidade em ambientes digitais; • identificar formas simples de usar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; • identificar declarações da política de privacidade simples sobre como os dados pessoais são usados em serviços digitais.
	2	• Selecionar formas simples de proteger os dados pessoais e privacidade em ambientes digitais, • identificar formas simples de usar e partilhar informação pessoalmente identificável, protegendo-se e aos outros de danos; • identificar declarações da política de privacidade simples sobre como os dados pessoais são usados em serviços digitais.
Intermediário	3	• Explicar formas bem definidas e rotineiras de proteger os meus dados pessoais e a privacidade em ambientes digitais; • explicar formas bem definidas e rotineiras de usar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; • indicar declarações da política de privacidade bem definidas e rotineiras de como os dados pessoais são usados em serviços digitais.
	4	• Discutir formas de proteger os meus dados pessoais e privacidade em ambientes digitais; • discutir formas de utilizar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; • indicar declarações da política de privacidade sobre como os dados pessoais são usados em serviços digitais.
Avançado	5	• Aplicar diferentes formas de proteger os meus dados pessoais e privacidade em ambientes digitais; • aplicar diferentes formas específicas de partilhar os meus dados, enquanto me protejo a mim e aos outros contra perigos; • explicar as declarações da política de privacidade que abordam a forma como os dados pessoais são usados em serviços digitais.
	6	• Escolher as formas mais apropriadas de proteger os dados pessoais e privacidade em ambientes digitais; • avaliar as formas mais apropriadas de utilizar e partilhar informação pessoalmente identificável, protegendo-me a mim e aos outros de danos; • avaliar a adequação de declarações da política de privacidade sobre como os dados pessoais são usados.
Altamente especializado	7	• Criar soluções para problemas complexos, com definição limitada, relacionadas com a proteção dos dados pessoais e a privacidade em ambientes digitais, utilizando e

		partilhando informação pessoalmente identificável, protegendo-me e aos outros de danos, e políticas de privacidade para usar os meus dados pessoais; • integrar o meu conhecimento para contribuir para a prática e conhecimento profissional e orientar outros na proteção dos dados pessoais e privacidade.
	8	• Criar soluções para resolver problemas complexos, com muitos fatores que interagem entre si, relacionadas com a proteção de dados pessoais e privacidade em ambientes digitais, utilizando e partilhando informação pessoalmente identificável, protegendo-me e aos outros de danos, e políticas de privacidade para usar os meus dados pessoais; • propor novas ideias e processos para a área.

Fonte: Lucas; Moreira e Trindade, 2022, p.37.

As orientações do subtópico intitulado Proteção de dados pessoais e privacidade do DigComp (2017) abrangem competências voltadas a: seleção e proteção de dados de terceiros, identificação de políticas referentes à coleta e uso de dados pessoais usados em serviços digitais, identificar formas de proteção de dados...

Quadro 5 - Proteção da saúde e do bem-estar

Níveis		Competências
Básico	1	• Distinguir formas simples de evitar riscos para a saúde e ameaças ao bem-estar físico e psicológico ao utilizar tecnologias digitais; • selecionar formas simples de me proteger de possíveis perigos em ambientes digitais; • identificar tecnologias digitais simples para o bem-estar e inclusão social.
	2	
Intermediário	3	• Explicar formas bem definidas e rotineiras de como evitar riscos para a saúde, bem como ameaças ao bem-estar físico e psicológico, ao utilizar tecnologias digitais; • selecionar formas bem definidas e rotineiras de me proteger dos perigos em ambientes digitais; • indicar tecnologias digitais bem definidas e rotineiras para o bem-estar e inclusão social.
	4	• Explicar formas de evitar ameaças à minha saúde física e psicológica relacionadas com a utilização da tecnologia; • selecionar formas de me proteger e aos outros de perigos em ambientes digitais; • discutir tecnologias digitais para o bem-estar e inclusão social.
Avançado	5	• Mostrar diferentes formas de evitar riscos de saúde e ameaças ao bem-estar físico e psicológico ao utilizar tecnologias digitais; • aplicar diferentes formas de me proteger a mim e aos outros de perigos em ambientes digitais;

		• mostrar diferentes tecnologias digitais para o bem-estar e inclusão social.
	6	• Discriminar as formas mais apropriadas para evitar riscos de saúde e ameaças ao bem-estar físico e psicológico ao utilizar tecnologias digitais, • adaptar as formas mais apropriadas de me proteger a mim e aos outros dos perigos em ambientes digitais, • variar a utilização de tecnologias digitais para o bem-estar e inclusão social.
	7	• Criar soluções para problemas complexos, com definição limitada, relacionadas com a prevenção de riscos de saúde e ameaças ao bem-estar, ao utilizar tecnologias digitais, para me proteger e aos outros de perigos em ambientes digitais, e para o uso de tecnologias digitais para o bem-estar e inclusão social; • integrar o meu conhecimento para contribuir para a prática e conhecimento profissional e orientar outros na proteção da saúde.
Altamente especializado	8	• Criar soluções para resolver problemas complexos, com muitos fatores que interagem entre si, relacionadas com o evitar riscos para a saúde e ameaças ao bem-estar, ao utilizar tecnologias digitais, para me proteger e aos outros de perigos em ambientes digitais, e para o uso de tecnologias digitais para o bem-estar e inclusão social; • propor novas ideias e processos para a área.

Fonte: Lucas; Moreira e Trindade, 2022, p.39.

O subtópico Proteção da saúde e do bem-estar trabalha as competências voltadas à segurança física e psicológica. Os usuários digitais conseguem distinguir formas de evitar ataques (*cyberbullying*) ou riscos para sua saúde, selecionando formas de se proteger, identificando tecnologias que o auxiliem em seu bem-estar, inclusão e proteção, além de integração de novos conhecimentos para resolução de possíveis problemas acerca da temática.

Quadro 6 - Proteção do meio ambiente

Níveis		Competências
Básico	1	• Reconhecer os impactos ambientais simples decorrentes das tecnologias digitais e da sua utilização.
	2	
Intermediário	3	• Indicar impactos ambientais bem definidos e rotineiros decorrentes das tecnologias digitais e da sua utilização.
	4	• Discutir formas de proteger o meio ambiente do impacto decorrente das tecnologias digitais e da sua utilização.
Avançado	5	• Mostrar diferentes formas de proteger o ambiente do impacto decorrente das tecnologias digitais e da sua utilização.
	6	• Escolher as soluções mais apropriadas para proteger o meio ambiente do impacto decorrente das tecnologias digitais e da sua utilização.

Altamente especializado	7	• Criar soluções para problemas complexos, com definição limitada, relacionadas com a proteção do meio ambiente do impacto decorrente das tecnologias digitais e da sua utilização; • integrar o meu conhecimento para contribuir para a prática e conhecimento profissional e orientar outros na proteção do ambiente.
	8	• Criar soluções para resolver problemas complexos, com muitos fatores que interagem entre si, relacionadas com a proteção do meio ambiente do impacto decorrente das tecnologias digitais e da sua utilização; • propor novas ideias e processos para a área.

Fonte: Lucas; Moreira e Trindade, 2022, p.41.

O último subtópico é denominado 4.4 Proteção do meio ambiente, ele trabalha com questões voltadas ao reconhecimento dos impactos ambientais causados pelas tecnologias. Através deste reconhecimento, se desenvolvem competências digitais com o intuito de estimular o usuário a discutir formas de proteção, soluções ou propor novas ideias acerca da temática.

No Brasil, não há um modelo padrão que se trabalhe o aspecto da segurança, como o DigComp 2.2, como alternativa em 2021, foi criado a cartilha denominada Cartilha de Segurança para Internet Proteção de Dados, organizada e produzida pelo CERT.br, NIC.br e CGI.br (2021), esse documento aborda métodos de identificação de ataques a dados pessoais e formas de prevenção, os quais são: realização de *backup*, proteção de documentos virtuais que contenham dados pessoais, ter cautela em abrir arquivos enviados por terceiros, criar senhas fortes e seguras que protejam de forma efetiva informações pessoais, orientações referente a habilitação do modo segurança no dispositivo móvel, instalação de aplicativos advindos de lojas oficiais, armazenagem de e-mails confidenciais em formato criptografado.

No mesmo ano, foi desenvolvida a cartilha “Internet Segura: divirta-se e aprenda a usar a *internet* de forma segura” pelas entidades CERT.br, NIC.br e CGI.br (2020), o material empenha-se em trabalhar questões pautadas na proteção quanto ao bem físico e psicológico, tais como: acompanhamento de pais ou responsáveis quanto ao monitoramento das redes sociais de usuários de menores, orientando menores a não compartilhar fotos, dados pessoais ou sua localização, além de orientações quando presenciar ou for vítima de *cyberbullying*.

No início de 2020, foi publicado o Decreto nº 10.222, que estabelece a Estratégia Nacional de Segurança Cibernética do Brasil (E-Ciber). Este decreto é o primeiro documento governamental com o objetivo de fornecer uma perspectiva sobre o papel do Brasil na segurança cibernética, além de definir os propósitos e princípios que guiarão seu desenvolvimento entre os anos de 2020 e 2023. O decreto foi criado em resposta aos crescentes riscos e ataques cibernéticos enfrentados por empresas, órgãos governamentais e instituições de ensino diariamente (Hurel, 2021).

De acordo com o Núcleo de Informação e Coordenação do Ponto BR (NIC.br, 2020), a segurança cibernética é essencial para a proteção dos direitos humanos, como a liberdade de expressão e a privacidade, além de ser fundamental para o bom funcionamento das redes e dos sistemas envolvidos, desde o suporte de acesso até as aplicações nele sustentadas.

A segurança de dados, redes, infraestruturas e sistemas digitais é um dos aspectos mais críticos em uma sociedade cada vez mais conectada. Diariamente, inúmeros ataques são realizados em redes distribuídas globalmente, afetando serviços virtuais, empresas e sistemas, e resultando na exposição de dados pessoais e vulneráveis da população.

Para Hurel (2021), esse fenômeno está relacionado ao grande número de pessoas conectadas à internet, já que mais da metade da população mundial tem ou teve experiências de conectividade concentrada em smartphones. Com o avanço tecnológico, os ataques cibernéticos se tornam cada vez mais eficazes. Segundo a SonicWall (2017), os ataques digitais são disseminados de várias formas, incluindo tráfego na web, *exploits*⁶ automatizados e dispositivos móveis. Para os *hackers*⁷, não importa o porte da empresa; qualquer organização é uma potencial vítima. Quando esses infratores encontram uma brecha na segurança,

⁶ Exploit é um conjunto de passos, muitas vezes materializado em um programa, capaz de tirar proveito de uma vulnerabilidade (Malerba, 2010, p.35).

⁷ Hackers são pessoas com um conhecimento profundo de computação e informática, que trabalham desenvolvendo e modificando softwares e hardwares de computadores, não necessariamente para cometer algum crime (TJSC, s.d).

iniciam um processo de ataque denominado *watering hole*⁸, ativando *exploits*⁹ ou enviando e-mails de *phishing*¹⁰ durante o dia e à noite.

Além das falhas relacionadas à falta de ferramentas adequadas para o combate, há um agravante: a carência de treinamento e orientações sobre como lidar com ataques cibernéticos. Essa deficiência ganhou maior destaque durante a pandemia de COVID-19, quando o número de trabalhadores em regime de *home office* aumentou significativamente. A falta de competências informacionais voltadas à segurança digital fez com que dados pessoais, financeiros, físicos e jurídicos da população se tornassem alvos de ataques, visto que essas informações têm grande valor no cenário atual. Para Hurel (2021), a pandemia acelerou a digitalização das empresas e trouxe consigo novas superfícies de ataques digitais.

Segundo o Correio Braziliense (2020), o número de golpes decorrentes de crimes cibernéticos teve um aumento expressivo em 2020. Esse crescimento vertiginoso reflete os hábitos desenvolvidos durante a pandemia, como compras virtuais em sites desconhecidos e transferências bancárias por aplicativos. Levantamentos realizados pela Polícia Civil do Distrito Federal (PCDF) indicam que os crimes de estelionato pela internet cresceram 198,95%, enquanto os furtos mediante fraude aumentaram 310,97%.

3 Quadro Europeu de Competência Digital para Educadores (*DigCompEdu*)

A partir da necessidade de habilidades relacionadas às competências digitais dos docentes, percebeu-se a importância de criar marcos de referência, tanto no campo teórico quanto no prático. Podem-se apontar dois importantes documentos que são considerados norteadores no desenvolvimento de habilidades digitais de professores: o Quadro Europeu de Competência Digital para Educadores (*DigCompEdu*), desenvolvido pela Comissão Europeia no ano de 2017, e o Quadro de Competências em Tecnologia da Informação e

⁸ *Watering Hole* é um ataque em que criminosos visam sites cujo propósito está alinhado a um certo grupo de interesse.” (El Pescador, 2016, p.24)

⁹ *Exploit* é um software, um bloco de dados ou uma sequência de comandos que se aproveita de um bug ou vulnerabilidade em um aplicativo ou sistema para causar a ocorrência de comportamentos não intencionais ou não antecipados (Bitdefender, s.d).

¹⁰ *Phishing* consiste em tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso (Prodest, s.d).

Comunicação (TIC) para Professores, idealizado pela *United Nations Educational, Scientific and Cultural Organization* (UNESCO) em 2019 (Battle e Pujolà, 2024).

Segundo Lucas e Moreira (2018), os educadores devem estar preparados para lidar e utilizar as tecnologias de forma criativa e consciente, tanto no nível pessoal quanto no profissional. Para os autores, esses profissionais são facilitadores, uma vez que não apenas precisam desenvolver competências digitais para cidadãos, conforme trabalhadas no *DigComp*, mas também necessitam expandir competências e habilidades específicas para utilizar as tecnologias de forma ativa e aproveitar seu potencial na educação.

O DigCompEdu possui um infográfico idealizado por Lucas e Moreira (2018) que delineaia três esferas: competências profissionais para educadores, competências pedagógicas dos educadores e competências dos aprendentes, conforme ilustrado na imagem abaixo:

Figura 1 - Síntese do quadro DigCompEdu



Fonte: Lucas e Moreira, p. 19, 2018.

A esfera "Competências profissionais dos educadores" aborda a área número 1, denominada "envolvimento profissional". Esta área engloba 4 competências.

Na comunicação institucional, as habilidades e competências desenvolvidas referem-se para o uso das tecnologias digitais na comunicação com encarregados, alunos e terceiros. Esta habilidade trabalha questões como contribuir, colaborativamente, desenvolvendo melhorias e estratégias voltadas à

comunicação institucional. A colaboração profissional é responsável pelo desenvolvimento do uso das tecnologias da comunicação e informação, com o intuito de criar redes colaborativas entre profissionais educadores, compartilhando e trocando experiências e conhecimentos, além de realizar colaborações em conjunto para inovar as práticas pedagógicas colaborativas.

Na prática reflexiva, são desenvolvidas competências que se referem à reflexão individual ou coletiva acerca da avaliação crítica, além do desenvolvimento de práticas pedagógicas no âmbito digital voltadas para a comunidade educativa. O Desenvolvimento Profissional Contínuo Digital (DPC) é trabalhado na última competência, ela desenvolve aspectos voltados ao desenvolvimento e aperfeiçoamento constante do profissional da educação, utilizando fontes e recursos digitais para seu desenvolvimento contínuo.

A esfera denominada "Competências pedagógicas dos educadores", aborda quatro áreas: "recursos digitais", "ensino e aprendizagem", "avaliação" e "capacitação dos aprendentes".

A segunda área, denominada recursos digitais, desenvolve habilidades e competências dos educadores acerca da seleção, que consiste na identificação, seleção e avaliação dos recursos digitais que atendam às suas necessidades informacionais para o ensino e aprendizagem, levando em consideração o perfil de seus alunos, analisando seu contexto social e a abordagem pedagógica. A criação e modificação são outras habilidades trabalhadas, visto que focam na competência do desenvolvimento dos recursos tecnológicos existentes com licença aberta, visando à criação de novos recursos tecnológicos voltados para a educação.

À gestão, proteção e partilha, desenvolve competências voltadas à organização de conteúdos digitais e disponibilização a seus alunos, encarregados ou para outros educadores. A proteção dos conteúdos de autoria própria é outro aspecto importante, visando proteger eficazmente todo conteúdo sensível, aplicando corretamente as regras de autoria, além da compreensão, criação e utilização dos recursos educativos que possuem licença aberta.

O ensino e aprendizado é a terceira área, ela desenvolve habilidades e competências acerca da aplicação das ferramentas digitais no processo de ensino de alunos, com o intuito de aprimorar o empenho e o desenvolvimento de aprendizagem, visando melhorar a eficiência das intervenções pedagógicas.

Esta área aborda a importância da utilização das ferramentas tecnológicas para realizar assistências e orientações, tanto por parte do professor quanto do aluno, desenvolvendo formas inovadoras de auxílio pedagógico.

Assim como o professor utiliza as tecnologias como ferramentas de orientação, seus alunos podem as utilizar em atividades colaborativas, visando melhorar a comunicação entre eles e estimular a criação colaborativa de novos conhecimentos. Por fim, e não menos importante, há a competência voltada para a aprendizagem autorregulada, que foca no uso das tecnologias para planejar, refletir e monitorar o desenvolvimento pedagógico, fornecendo informações para que posteriormente o aluno possa encontrar soluções criativas para melhorar seu desempenho em determinadas atividades.

A terceira área é a avaliação, na qual são trabalhadas habilidades e competências, tais como estratégias de avaliação, em que os educadores utilizam as tecnologias para realizar avaliações formativas de seus alunos, diversificando e melhorando as abordagens e formatos avaliativos. A análise de evidências é outro aspecto abordado nesta área, uma vez que o objetivo é produzir, selecionar e analisar criticamente a utilização das tecnologias em atividades, além de observar o progresso do aluno ao utilizar essas ferramentas para desenvolver as atividades solicitadas. Por fim, a competência de *feedback* e planificação, esta habilidade envolve a utilização das TIC para fornecer *feedback* oportuno aos alunos, permitindo que os responsáveis pela educação e os próprios aprendentes compreendam como as evidências fornecidas pelas tecnologias digitais podem ser utilizadas para a tomada de decisões.

O DigCompEdu aborda a avaliação na quarta área do documento, destacando a importância de integrar tecnologias digitais como ferramentas para enriquecer o processo avaliativo. Os educadores devem adotar estratégias que utilizem essas tecnologias para monitorar o desenvolvimento individual dos alunos, fornecer *feedbacks* personalizados e identificar dificuldades, promovendo intervenções pedagógicas eficazes. Além disso, o uso ético e responsável dos dados gerados é essencial, garantindo a privacidade dos estudantes. Assim, a avaliação torna-se um processo dinâmico e centrado no aluno, alinhado às competências de segurança digital e ao uso estratégico das tecnologias no ensino.

A quinta área abordada pelo DigCompEdu trabalha a capacitação dos

aprendentes, considerando habilidades relacionadas à acessibilidade e inclusão. Isso significa analisar as necessidades individuais, contextuais, físicas e cognitivas de cada aluno quanto à utilização das ferramentas digitais, tornando-as acessíveis para todos. A competência envolve também a utilização das tecnologias para atender às diversas necessidades de aprendizado, permitindo que o professor analise a progressão de diferentes estágios e velocidades de seus alunos, com foco em seus objetivos de desenvolvimento pessoal. Além disso, destaca-se o aspecto do envolvimento ativo, em que o educador orienta a utilização das TDIC para promover o envolvimento ativo e criativo dos alunos, utilizando-as para realizar pesquisas científicas e resolver problemas simples e complexos, visando o desenvolvimento ativo de todos.

A sexta e última área abordada no quadro de competências digitais para educadores é a promoção da competência digital dos aprendentes. São trabalhadas habilidades voltadas à literacia da informação e das mídias, onde o educador irá inserir atividades de acordo com o plano pedagógico, fomentando que seus aprendentes se articularam e identificaram as necessidades de encontrarem informações em ambientes digitais, organizando, processando, analisando e interpretando informações.

Lucas e Moreira (2018) apontam outras habilidades e competências na sexta área, uma delas se refere à comunicação e colaboração digital, por meio da inclusão de tarefas, atividades e avaliações nas quais os aprendentes utilizam as ferramentas de maneira eficaz e responsável para a colaboração e participação cívica.

A criação de conteúdo digital também é abordada nesta área, visto que é importante incorporar atividades que permitam aos aprendentes expressarem-se por meio das ferramentas digitais, transformando e criando conteúdo digital original em diversos formatos.

Outro aspecto trabalhado pelos educadores na área seis é a orientação à utilização ética, respeitando os direitos autorais em diversos formatos digitais ou as licenças correspondentes. Quanto à promoção do uso responsável, trata-se de questões relacionadas ao uso consciente das tecnologias digitais, visando garantir o bem-estar psicológico e físico dos aprendentes. Ela capacita os indivíduos a gerir os riscos ao utilizar as tecnologias de forma segura e responsável, tanto para si mesmos quanto para terceiros. A competência

relacionada ao uso responsável é a que mais se aproxima da área 4 do DigComp 2.2 relacionada à segurança. A última competência abordada refere-se à resolução de problemas digitais, na qual o professor desenvolve habilidades voltadas para a identificação de problemas técnicos e em direção à transferência criativa de conhecimentos tecnológicos para novas situações e soluções de problemas.

O DigCompEdu é um marco não somente em contexto europeu, mas serve como guia para outros países, servindo como modelo na elaboração de guias e diretrizes que trabalham essas competências e habilidades nos profissionais da educação.

No contexto nacional, o Brasil não possui um modelo padrão que trabalhe as competências digitais de docentes ou discentes em pedagogia de forma planejada. Entretanto, como mencionado anteriormente, o CERT.br, o NIC.br e o CGI.br auxiliam esses grupos por meio de cartilhas voltadas para temas como proteção de dados, segurança online, ataques cibernéticos e internet segura. As cartilhas são didáticas e podem ser utilizadas por professores em sala de aula, visto que incluem jogos e atividades de colorir, o que pode contribuir para a aprendizagem dos alunos.

Além das cartilhas que servem como material de apoio para o aprimoramento das competências digitais de professores e alunos, em 2023 entrou em vigor a Lei nº 14.533, de 11 de janeiro de 2023¹¹, que institui a Política Nacional de Educação Digital (PNED). O Art. 3º estabelece que o eixo educacional digital escolar tem como objetivo garantir a inclusão do ensino digital nas escolas, abrangendo todos os níveis e modalidades, além de estimular o letramento digital e informacional, bem como a aprendizagem de robótica, computação, programação, entre outras competências.

O inciso IV do Art. 3º destaca que os conteúdos relacionados à competência de segurança devem abordar: direitos autorais, conscientização sobre o uso e o tratamento de dados pessoais nos termos da Lei Geral de Proteção de Dados Pessoais ¹²(LGPD) nº 13.709, conectividade segura e a proteção de dados da população vulnerável, especialmente crianças e

¹¹ https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/l14533.htm

¹² https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

adolescentes.

4 CONTEXTUALIZAÇÃO DA PESQUISA

Universidade Estadual Paulista "Júlio de Mesquita Filho"

A Universidade Estadual Paulista "Júlio Mesquita Filho" (Unesp) foi criada em 1976 com o intuito de incorporar os institutos isolados do Estado de São Paulo que abrangiam diversas áreas do conhecimento. Dois anos após sua criação, a universidade contava com um total de 14 campi, com sede da Reitoria localizada na cidade de São Paulo.

Durante as décadas de 80 e 90, a instituição passou por inúmeras mudanças, reflexos do movimento político Diretas Já. Em seu novo estatuto, assinado em 1989, a Unesp tinha como expectativa se transformar em uma universidade inerentemente democrática. A expansão e a democratização foram pautas defendidas para a construção identitária da Universidade Estadual Paulista (UNESP, s.d).

Atualmente, a Unesp possui um total de 34 unidades (faculdades, institutos e campi experimentais), localizadas em 24 cidades do estado de São Paulo, abrangendo o interior, a capital e o litoral paulista. No interior, destacam-se: em Araçatuba, a Faculdade de Odontologia (FOA) e a Faculdade de Medicina Veterinária (FMVA); em Araraquara, a Faculdade de Ciências Farmacêuticas (FCFAR), a Faculdade de Ciências e Letras (FCLAR), a Faculdade de Odontologia (FOAr) e o Instituto de Química (IQ); em Assis, a Faculdade de Ciências e Letras (FCLAs); em Bauru, a Faculdade de Arquitetura, Artes, Comunicação e Design (FAAC), a Faculdade de Ciências (FC) e a Faculdade de Engenharia (FEB); e em Botucatu, a Faculdade de Medicina (FMB), a Faculdade de Medicina Veterinária e Zootecnia (FMVZ), o Instituto de Biociências (IBB) e a Faculdade de Ciências Agronômicas (FCA).

Outras cidades do interior também contam com unidades da Unesp, como Dracena, com a Faculdade de Ciências Agrárias e Tecnológicas (FCAT); Franca, com a Faculdade de Ciências Humanas e Sociais (FCHS); Guaratinguetá, com a Faculdade de Engenharia (FEG); Ilha Solteira, com a Faculdade de Engenharia (FEIS); Itapeva, com o Instituto de Ciências e Engenharia (ICE); Jaboticabal, com a Faculdade de Ciências Agrárias e Veterinárias (FCAV); Marília, com a Faculdade de Filosofia e Ciências (FFC); Ourinhos, com a Faculdade de

Ciências, Tecnologia e Educação (FCTE); Presidente Prudente, com a Faculdade de Ciências e Tecnologia (FCT); Registro, com a Faculdade de Ciências Agrárias do Vale do Ribeira (FCAVR); Rio Claro, com o Instituto de Geociências e Ciências Exatas (IGCE) e o Instituto de Biociências (IB); Rosana, com a Faculdade de Engenharia e Ciências (FEC); São João da Boa Vista, com a Faculdade de Engenharia (FESJ); São José do Rio Preto, com o Instituto de Biociências, Letras e Ciências Exatas (IBILCE); e Sorocaba, com o Instituto de Ciência e Tecnologia de Sorocaba (ICTS).

Na capital e no litoral, a Unesp também está presente. Em São Paulo, encontram-se o Grupo Técnico de Informação e Documentação (GTID), o Instituto de Artes (IA), o Instituto de Física Teórica (IFT) e o Instituto de Políticas Públicas e Relações Internacionais (IPPRI). Já no litoral paulista, há unidades em São Vicente, com o Campus do Litoral Paulista/Instituto de Biociências (CLP), e em Tupã, com a Faculdade de Ciências e Engenharia (FCE).

Em termos de corpo docente, a instituição conta com cerca de 3 mil professores e oferece mais de 136 cursos de graduação (licenciaturas e bacharelados) nas três grandes áreas do conhecimento: humanas, exatas e biológicas. As vagas dos cursos superiores são destinadas a alunos da rede pública e particular. Hoje, a Unesp conta com um total de 38 mil alunos, dos quais cerca de 52% vieram da rede pública, e 48% de instituições privadas. Assim, a Unesp forma anualmente mais de 5 mil profissionais com alta qualificação científica, técnica e humanística (UNESP, 2024).

De acordo com o ranking elaborado pela revista *Times Higher Education*, que avalia instituições com menos de 50 anos, a Unesp se destaca pela qualidade de seu ensino, que se baseia em três pilares: ensino, educação e pesquisa. No contexto nacional, a universidade paulista ficou em 1.º lugar. No cenário mundial, sua colocação foi a 124.ª posição. O resultado evidencia a qualidade de seus cursos, de seus docentes e de um dos serviços mais importantes da universidade pública: fazer ciência e disseminar para a comunidade.

5 METODOLOGIA

Para alcançar os objetivos desta pesquisa, foi adotada uma abordagem quali-quantitativa (métodos mistos), que envolve a coleta e análise de dados

quantitativos e qualitativos de maneira distinta, seguida pela comparação dos resultados para identificar possíveis convergências ou divergências.

...uma técnica de métodos mistos é aquela em que o pesquisador tende a basear as alegações de conhecimento em elementos pragmáticos (por exemplo, orientado para consequência, centrado no problema e pluralista). Essa técnica emprega estratégias de investigação que envolvem coleta de dados simultânea ou sequencial para melhor entender os problemas de pesquisa. A coleta de dados também envolve a obtenção tanto de informações numéricas (por exemplo, em instrumentos) como de informações de texto (por exemplo, em entrevistas), de forma que o banco de dados final represente tanto informações quantitativas como qualitativas (Creswell, 2007, p. 35).

Para a construção do referencial teórico e sistematização da literatura, utilizou-se uma variedade de documentos. A busca desses arquivos foi realizada em bases de dados nacionais: Base de Dados em Ciência da Informação (Brapci), Portal de Periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), *Scientific Electronic Library Online* (SciELO – Brazil), além de plataformas internacionais, como *Dialnet* e o site institucional português da Direção-Geral da Educação¹³.

Foram realizados dois levantamentos. O primeiro consiste na análise dos materiais informacionais de autoformação sobre segurança digital disponibilizados nas webpages da Diretoria Técnica de Informática (DTI). As páginas analisadas pertencem aos departamentos das 37 faculdades e institutos de ensino superior, bem como ao Grupo Técnico de Informação e Documentação da UNESP, distribuídos em 24 cidades do estado de São Paulo.

A pesquisa nas páginas do DTI foi conduzida por meio do site de cada campus, previamente identificado por meio de buscas no Google pelos sites institucionais de cada unidade. Geralmente, essas páginas estavam localizadas na aba "Informática". Após identificá-las, foi realizado um levantamento de informações dos materiais, como: formato do documento, data da última atualização da página, responsável pela elaboração do material e conteúdo abordado. As informações levantadas foram organizadas de acordo com o campus.

¹³ <https://digital.dge.mec.pt/>

Após o primeiro levantamento realizado nas webpages das DTIs, os materiais foram organizados e relacionados com dois documentos analisados no referencial teórico: o DigComp 2.2 e o DigCompEdu, ambos produzidos pela Universidade de Aveiro, sob a responsabilidade dos autores Margarida Lucas e António Moreira.

A primeira relação do conteúdo encontrado nos documentos de autoformação foi estabelecida com o DigComp, em especial com a Área 4 – Segurança, que abrange cinco competências centrais: Literacia de Informação e de Dados, Comunicação e Colaboração, Criação de Conteúdo Digital, Segurança e Resolução de Problemas. Em seguida, o conteúdo foi relacionado com o DigCompEdu, especificamente com a competência 6.4, que aborda o uso responsável das tecnologias digitais.

O segundo levantamento foi realizado na página institucional da Reitoria da Unesp¹⁴ da seguinte maneira: primeiramente, acessou-se o site da Reitoria. Na seção "Informação", localizada no rodapé do site, foi selecionada a opção "Legislação da Unesp¹⁵" e, em seguida, "Resoluções e Portarias¹⁶". Isso abriu uma nova página contendo as resoluções e portarias publicadas entre 1976 e 2024.

O objetivo do segundo levantamento foi identificar documentos que abordassem a temática de orientações de segurança digital durante a pandemia de COVID-19 para sua comunidade acadêmica. Para isso, delimitou-se o período de análise entre o primeiro semestre de 2020, início da pandemia, e o primeiro bimestre de 2023, considerado o fim da pandemia pela Organização Mundial da Saúde (OMS).

As portarias foram baixadas individualmente e analisadas com o *software* Adobe Reader, a fim de identificar diretrizes, normativas e políticas relacionadas à segurança digital no contexto da universidade.

O processo de análise incluiu a leitura detalhada de cada documento, com o objetivo de extrair informações relevantes sobre as práticas, orientações e

¹⁴ <https://www2.unesp.br/>

¹⁵ <https://www2.unesp.br/portal#!/secgeral/manuais/legislacao-Unesp/>

¹⁶ <https://sistemas.unesp.br/legislacao-web/>

atividades remotas adotadas pela Unesp para garantir a segurança digital no ambiente acadêmico e administrativo.

6 RESULTADOS

Quanto aos resultados do primeiro levantamento, foi identificado que 7 (sete) das 37 Diretorias Técnicas de Informática (DTIs) não oferecem materiais informativos e formativos relacionados à segurança digital para suas respectivas comunidades. Esses materiais são de grande importância para a conscientização e a formação de discentes, docentes, pesquisadores e técnicos administrativos sobre as melhores práticas de segurança no ambiente digital. As unidades que não disponibilizam tais recursos são: FCLAR - Faculdade de Ciências e Letras de Araraquara, FCLAs - Faculdade de Ciências e Letras de Assis, FCTE - Faculdade de Ciências e Tecnologia de Ourinhos, GTID - Grupo Técnico de Informação e Documentação de São Paulo, IFT - Instituto de Física de São Paulo, IPPRI - Instituto de Pesquisa e Planejamento Regional de São Paulo e CLP - Campus de São Vicente.

Foi observado que o Grupo Técnico de Informação e Documentação (GTID)¹⁷, responsável pela execução das atividades relacionadas a atividades documentárias especializadas em áreas administrativas e jurídica tem a função de assegurar o acesso aos instrumentos necessários para a formação, além de manter o acervo de normas da Unesp e providenciar e acompanhar o Diário Oficial do Estado. O GTID não possui uma página digital vinculada à Diretoria Técnica de Informática (DTI) local, contando apenas com uma guia dentro do site da Secretaria Geral da Unesp, o que ocasiona acesso limitado dos seus membros a informações relevantes sobre segurança digital e outros temas relacionados à área de tecnologia.

Esses resultados indicam uma lacuna na oferta de recursos de autoformação em segurança digital em algumas unidades da Unesp, o que pode comprometer a disseminação de boas práticas de segurança entre os membros da comunidade acadêmica.

¹⁷ <https://www2.Unesp.br/portal#!/secgeral/equipes-de-trabalho/grupo-de-informacoes-documentarias/>

Quadro 7 - Área 4 do DigComp 2.2 e Materiais de Formação Oferecidos pelas DTIs da Unesp

Competências	Materiais de Formação em Segurança Digital	
4.1 Proteção de dispositivos	Atualize seu antivírus Atualize seu sistema operacional <i>Backup</i> Cartilha de Segurança Checklist de Segurança Código de Verificação Contas e senhas Crie senhas difíceis Criptografia	Instalação do Antivírus Mecanismos de segurança Remover Vírus de <i>Pen-drive</i> Segurança de computador Segurança em dispositivos móveis Verificação Dois Fatores VPN (<i>Virtual Private Network</i>) Wi-Fi UNESP
4.2 Proteção de dados pessoais e privacidade	Autenticação Cuidado ao fazer cadastros Cuide dos dados pessoais Exposição de filhos <i>Login Social</i> Não revele informações importantes sobre você Privacidade	Proteção de dados Redes públicas Saia usando Logout Vazamento de dados
4.3 Proteção da saúde e bem-estar	Uso de mensageiros instantâneos <i>Cyberbullying</i> <i>DeepFake</i> ¹⁸ Exposição de filhos <i>online</i> Netiqueta Redes Sociais	
4.4 Proteção do meio ambiente	Ataques na <i>Internet</i> Cibersegurança Códigos maliciosos (<i>Malware</i>) Dicas de Segurança Golpes em aplicativos Golpes na Internet <i>Internet Segura</i> <i>Links Desconhecidos</i>	Navegação Anônima Navegadores Portal antispam Segurança de redes Segurança na <i>Internet</i> <i>Spam</i> Uso seguro da <i>Internet</i>

Fonte: Elaborado pelo autor.

Entre as 30 unidades de DTIs analisadas, verifica-se que apenas 2 (6,7%) abordam as quatro competências da Área 4 - Segurança do DigComp 2.2 (4.1 Proteção de dispositivos; 4.2 Proteção de dados pessoais e privacidade; 4.3 Proteção da saúde e bem-estar; e 4.4 Proteção do meio ambiente) de forma abrangente com suas comunidades. Essas unidades são: FAAC - Bauru e ICT - São José dos Campos.

Outras 2 unidades (6,7%) contemplam três competências: A FFC - Marília aborda as competências 4.1 (Proteção de dispositivos), 4.3 (Proteção da saúde e bem-estar) e 4.4 (Proteção do meio ambiente), enquanto a IBB - Botucatu foca

¹⁸ Deepfake consiste em imagens ou vídeos que são gerados por meio de uma técnica de inteligência artificial. Trata-se de uma técnica de "aprendizado de máquina" chamada deep learning (Nacional Geographic Brasil, 2023).

em 4.1 (Proteção de dispositivos), 4.2 (Proteção de dados pessoais e privacidade) e 4.4 (Proteção do meio ambiente). Outras 2 unidades (6,7%) trabalham com duas competências: FEG - Guaratinguetá contempla 4.1 (Proteção de dispositivos) e 4.3 (Proteção da saúde e bem-estar), enquanto a FCT - Presidente Prudente aborda 4.1 (Proteção de dispositivos) e 4.4 (Proteção do meio ambiente).

As 22 unidades restantes (79,9%) abordam apenas uma competência, especificamente 4.1 (Proteção de dispositivos). Essas unidades são: FOA e FMVA - Araçatuba; FCFAR, FOAr e IQ - Araraquara; FC e FEB - Bauru; FMB, FMVZ e FCA - Botucatu; FCAT - Dracena; FCHS - Franca; FEIS - Ilha Solteira; ICE - Itapeva; FCAV - Jaboticabal; FCAVR - Registro; IGCE e IB - Rio Claro; FEC - Rosana; FESJ - São João da Boa Vista; IBILCE - São José do Rio Preto; IA - São Paulo; ICTS - Sorocaba e FCE - Tupã.

Quando comparado o conteúdo dos materiais de formação em segurança digital disponibilizados pelas DTIs com a Área 6 do DigCompEdu, especificamente a competência 6.4 (Uso Responsável), que consiste, pode-se apontar que 12 materiais se correlacionam com as competências 6.4 (Quadro 8).

Quadro 8 - Competência 6.4: Uso responsável do DigCompEdu e Materiais de Formação Oferecidos pelas DTIs da Unesp

Capacidades trabalhadas 6.4 - DigCompEdu	Materiais de Formação em Segurança Digital
Proteger dispositivos e conteúdo digital e compreender os riscos e ameaças em ambientes digitais.	• Atualize seu antivírus • Atualize seu sistema operacional • Instalação do Antivírus • Remover Vírus de <i>Pen-drive</i> • Mecanismos de segurança • Segurança de computador • Segurança em dispositivos móveis
Compreender medidas de segurança e proteção.	• Código de Verificação • Verificação Dois Fatores • VPN (<i>Virtual Private Network</i>) • Segurança de redes • <i>Links</i> Desconhecidos • Portal antispam
Proteger os dados pessoais e a privacidade em ambientes digitais.	• Contas e senhas • Crie senhas difíceis • Cuide dos dados pessoais • Privacidade • Proteção de dados • Não revele informações importantes sobre você • Saia usando <i>Logout</i>

	• Cuidado ao fazer cadastros • Login Social
Compreender como usar e compartilhar informações pessoais, sendo, simultaneamente, capaz de se proteger e aos outros de danos.	• Redes públicas • Redes Sociais • Exposição de filhos • Exposição de filhos online • Netiqueta • Uso seguro da Internet
Compreender que os serviços digitais utilizam uma política de privacidade para informar como são usados os dados pessoais.	• Privacidade • Proteção de dados • Cuide dos dados pessoais • Login Social • Cuidado ao fazer cadastros • Não revele informações importantes sobre você
Proteger os outros e a si próprio de possíveis perigos em ambientes digitais (p. ex., <i>cyberbullying</i>).	• <i>Cyberbullying</i> • <i>DeepFake</i> • Golpes em aplicativos • Golpes na Internet
Ter consciência das tecnologias digitais dedicadas ao bem-estar e à inclusão social.	• Atente-se ao usar mensageiros instantâneos • Dicas de Segurança • Navegação Anônima • Internet Segura
Ter consciência do impacto ambiental das tecnologias digitais e da sua utilização.	Este item não possui relação direta com os materiais listados
Monitorizar o comportamento dos aprendentes em ambientes digitais para salvaguardar o seu bem-estar.	• Exposição de filhos <i>online</i> • <i>Cyberbullying</i>
Reagir imediata e eficazmente quando o bem-estar dos aprendentes é ameaçado em ambientes digitais (p. ex., <i>cyberbullying</i>).	• <i>Cyberbullying</i> • <i>DeepFake</i>

Fonte: Elaborado pelo autor.

Os materiais de formação oferecidos pelas DTIs da UNESP possuem forte aderência com a competência 6.4 do DigCompEdu, que abarca o uso responsável em ambientes digitais. Esses materiais de autoformação abordam medidas práticas e essenciais para proteger dispositivos e conteúdos digitais, como: atualizações de antivírus, sistemas operacionais e segurança em redes móveis. Além disso, a oferta dos materiais destaca a importância da privacidade e da proteção de dados pessoais por meio de boas práticas, como criação de senhas seguras, cuidado ao realizar cadastros e uso consciente de redes sociais.

A prevenção de ameaças no âmbito digital, como golpes na internet, *cyberbullying* e *deepfake*, também é contemplada pelas DTIs, reforçando a necessidade de um ambiente seguro para todos a comunidade que o departamento presta serviços. Contudo, observa-se uma lacuna no tratamento

de aspectos relacionados ao impacto ambiental das tecnologias digitais, parte importante da competência 6.4. Integrar esses materiais de autoformação de forma mais acessível e alinhada às diretrizes do DigCompEdu pode fortalecer a conscientização e a aplicação de boas práticas na comunidade acadêmica, promovendo segurança digital e bem-estar.

O desenvolvimento de competências digitais dos professores é extremamente importante, considerando que esses profissionais desempenham um papel central no desenvolvimento das habilidades relacionadas às TIC nos alunos. No entanto, "para que os professores incentivem o desenvolvimento das competências digitais no âmbito educacional e no mundo do trabalho, é fundamental que eles participem de momentos de formação sobre o uso pedagógico das TDIC." (Peripolli; Barinb; 2022, p. 48).

É importante ressaltar que os documentos de formação fornecidos pelos DTIs são de extrema relevância para o desenvolvimento de habilidades e competências relacionadas à segurança digital. Estes documentos abrangem os quatro tópicos da Área 4 - Segurança e nove das dez capacidades trabalhadas na competência 6.4 do DigCompEdu. No entanto, a falta de divulgação dos materiais os deixa em uma espécie de ostracismo. Um exemplo analisado é o DTI do campus de Marília, que aborda três tópicos da Área 4 do DigComp 2.2. Contudo, a página foi atualizada pela última vez em 11 de abril de 2014, e os *links* para os materiais apresentam erro 404 (página não encontrada).

Quanto ao segundo levantamento, foram analisadas 491 portarias, criadas entre os anos de 2020, 2021, 2022 e o primeiro bimestre de 2023, este último marcando o fim da pandemia, conforme a Organização Mundial da Saúde (OMS). A partir da leitura dessas portarias, identificou-se que 8 documentos mencionam os termos "trabalho/atividades remotas/híbrido(a)".

No ano de 2020, das 188 portarias promulgadas, apenas duas abordam o termo "trabalho/atividades remotas/híbrido(a)", conforme apresentado abaixo:

Quadro 9 - Portarias Unesp de 2020 relacionadas a atividades remotas

Portarias	Menções que abordam os termos trabalho/atividade remotas ou híbridas
-----------	--

Nº 122	§ 2º - As atividades desenvolvidas remotamente serão creditadas aos estudantes que apresentarem as tarefas e cumprirem os critérios de avaliação definidos pelo docente responsável.
Nº 128	§ 4º - As atividades desenvolvidas remotamente serão creditadas aos estudantes que cumprirem os critérios de avaliação definidos pelo docente responsável.

Fonte: Elaborado pelo autor.

Das 158 portarias contidas do ano de 2021, apenas três documentos indicam o termo trabalho/atividades remotas/híbrido (a), os quais são:

Quadro 10 - Portarias Unesp de 2021 relacionadas a atividades remotas

Portarias	Menções que abordam os termos trabalho/atividade remotas ou híbridas
Nº 32	- a Deliberação CEE 195-2021, que fixa normas para a retomada tanto das atividades presenciais quanto das por meio remoto e para a organização dos calendários escolares para o ano letivo de 2021 no Sistema de Ensino do Estado de São Paulo, devido ao surto global do Coronavírus, e dá outras providências;
Nº 115	§1º - As disciplinas poderão ser oferecidas de forma totalmente virtual ou híbrida, mas não poderão exigir a participação presencial de estudantes externos à Unesp nas atividades previstas.
Nº 127	§2º - As disciplinas poderão ser oferecidas de forma totalmente virtual ou híbrida, mas não poderão exigir a participação presencial de estudantes externos à Unidade ofertante nas atividades previstas.

Fonte: Elaborado pelo autor.

Das 122 portarias contidas do ano de 2022, apenas a de n.º 74 - Dispõe sobre o oferecimento de Ensino Híbrido nos Programas de Pós-graduação, stricto sensu, da Unesp.

Até o término do levantamento para este estudo, em março de 2023, foram identificadas 23 portarias de 2023 e apenas três delas indicavam o termo trabalho/atividades remotas/híbrido(a), os quais são:

Quadro 11 - Portarias Unesp de 2023 relacionadas a atividades remotas

Portarias	Menções que abordam os termos trabalho/atividade remotas ou híbridas
Nº 07	Artigo 4º - O NUMIS Central terá reuniões ordinárias bimestrais presenciais ou remotas.
Nº 20	Artigo 3º - Permanece a critério dos Dirigentes das Unidades-Órgãos da Universidade, à vista da situação epidemiológica da infecção por SARS-CoV-2 e das peculiaridades e necessidades de cada caso, instituir às servidoras gestantes a modalidade de trabalho remoto ou híbrido, desde

	que a função exercida seja compatível com o trabalho remoto, sem prejuízo ao serviço público.
Nº 22	Artigo 1º - Ensino híbrido é um modelo de organização de ensino que combina interações presenciais e interações em ambientes virtuais simultâneas, ou seja, de maneira síncrona, de modo a promover a relação de ensino e de aprendizagem entre docentes e discentes. Parágrafo único - O ensino híbrido não prevê atividade em formato assíncrono, não caracterizando a modalidade EaD. Artigo 2º - O ensino híbrido dos cursos de Especialização na modalidade Lato Sensu da Unesp tem por objetivos: Artigo 3º - Os cursos de Especialização, na modalidade Lato Sensu da Unesp que optarem por oferecer o Ensino Híbrido deverão definir no Projeto Pedagógico do curso, em cada edição, os critérios e o percentual de carga horária de disciplinas que atendam às suas especificidades na seguinte conformidade: I - as disciplinas teóricas que optarem pelo ensino híbrido deverão ter previsão de atividades presenciais e de atividades em ambientes virtuais no formato síncrono; II - disciplinas práticas que optarem pelo ensino híbrido deverão justificar a parcela de atividades da disciplina em ambientes virtuais no formato síncrono. § 1º - Caberá à Unidade Universitária a que pertence o Curso de Especialização, na modalidade Lato Sensu, garantir a infraestrutura e o suporte adequados para o oferecimento do ensino híbrido. § 2º - O oferecimento de ensino híbrido pelos cursos de Especialização interinstitucionais respeitará as especificidades definidas para esse fim, conforme previstas em suas normas e devidamente acordadas por meio de convênio.

Fonte: Elaborado pelo autor.

A análise detalhada das portarias levantadas revelou que os documentos emitidos nos anos de 2020 (Portarias Nº 122 e Nº 128) e 2021 (Portarias Nº 32, Nº 115 e Nº 127) têm como foco principal a definição de diretrizes para a adaptação das disciplinas de graduação ao formato remoto. Essa mudança ocorreu devido à impossibilidade de oferecer aulas presenciais em função das restrições impostas pela pandemia de COVID-19. Já as portarias emitidas em 2023 abordam temas diversos, mas de igual relevância. A Portaria Nº 7 regulamenta que o Núcleo de Movimento, Inclusão e Saúde (Numis) Central deverá realizar reuniões ordinárias bimestrais, que podem ser presenciais ou remotas. A Portaria Nº 20 estabelece a possibilidade de trabalho remoto ou híbrido para servidoras gestantes, desde que suas funções sejam compatíveis com esse modelo, garantindo que o serviço público não seja prejudicado. A Portaria Nº 22 dispõe sobre o oferecimento de disciplinas de forma híbrida para discentes da pós-graduação.

Apesar de as portarias mencionadas abordarem adaptações importantes no contexto do ensino e trabalho remoto, nenhuma delas trata diretamente de orientações específicas relacionadas à segurança e privacidade no ambiente digital para a comunidade acadêmica. O conteúdo apresentado nos textos disponíveis no levantamento é superficial e carece de aprofundamento técnico sobre essas questões. Essa lacuna é preocupante, considerando que a Unesp é uma das maiores produtoras de pesquisa e ciência no Brasil. A ausência de diretrizes claras e robustas sobre segurança digital pode expor a comunidade acadêmica a riscos significativos em um momento em que a proteção de dados e a privacidade são fundamentais no contexto do ensino e trabalho remoto.

7 CONCLUSÃO

Durante a pandemia de COVID-19, inúmeras instituições de ensino superior foram alvo de ataques cibernéticos, evidenciando a fragilidade dos sistemas e a carência de competências relacionadas à segurança digital. Nesse contexto, entidades como o CERT.br, NIC.br, CGI.br e o Centro de Atendimento a Incidentes de Segurança (CAIS) produziram uma expressiva quantidade de cartilhas com o objetivo de orientar a população sobre o uso seguro da informação, a proteção de dados pessoais e de terceiros, entre outros aspectos. No âmbito internacional, os materiais norteadores foram o DigComp 2.2 e o DigCompEdu, que oferecem diretrizes amplas para o desenvolvimento de competências digitais.

Os objetivos da presente comunicação foram alcançados. O objetivo A, abordado na introdução do trabalho, está relacionado ao referencial teórico, que se fundamenta em documentos que tratam das temáticas de competência digital, segurança e privacidade no trabalho remoto. Esses documentos, além de serem analisados nos resultados, possuem grande relevância, pois estão diretamente vinculados aos levantamentos realizados.

Diante desse cenário, o objetivo B também foi atingido. Nos levantamentos iniciais, foi possível identificar os materiais de autoformação disponibilizados nas páginas web do STI, produzidos por instituições como CERT.br, NIC.br, CGI.br, CAIS, FGV e pela Coordenadoria de Tecnologia da Informação da UNESP (CETINF-Unesp). Esses materiais são de extrema

importância, pois abordam aspectos fundamentais da segurança digital, com conteúdos aplicáveis tanto no âmbito acadêmico quanto no pessoal. Entretanto, vale destacar que o DTI não é diretamente responsável pela formação ou autoformação de sua comunidade. A identificação desses materiais foi possível apenas devido a uma pesquisa extensa e detalhada, que contribuiu para compreender a relevância de iniciativas voltadas à disseminação de competências em segurança digital pela Universidade Estadual Paulista (Unesp).

Outro aspecto importante a ser pontuado diz respeito à atualização das páginas onde os documentos estão disponibilizados. Como a tecnologia é dinâmica, os materiais precisam ser constantemente atualizados para que a autoformação dos usuários não se torne defasada. No que se refere à atualização das páginas que contêm materiais destinados à comunidade acadêmica, os dados apontam que: 59% das páginas dos STIs analisadas foram atualizadas em 2024; 8,1% tiveram sua última atualização em 2021; 2,7%, em 2018; 5,4%, em 2014; 2,7%, em 2011; e 21,6% não possuem página ou material de autoformação relacionado à segurança digital.

Quanto ao Objetivo C, que aborda as publicações de portarias realizadas pela Reitoria da UNESP, constatou-se que, entre os 491 documentos analisados, nenhum apresentou orientações específicas sobre a proteção de dados de discentes e docentes ou sobre os riscos e ameaças cibernéticas a que a comunidade acadêmica esteve exposta em ambientes virtuais devido à adoção da modalidade remota entre os anos de 2020 e 2023.

Além disso, não foi identificada qualquer iniciativa voltada à qualificação ou ao desenvolvimento de habilidades digitais, especialmente no que diz respeito à segurança digital. Essa lacuna evidencia a ausência de diretrizes que poderiam promover a conscientização e o preparo da comunidade acadêmica frente aos desafios e vulnerabilidades associados ao trabalho e ao ensino em ambientes virtuais.

Essa carência está diretamente relacionada às competências descritas na Área 4 do DigComp 2.2, que trata da Segurança Digital, abrangendo temas como proteção de dados, privacidade e boas práticas para o uso de tecnologias. Da

mesma forma, é pertinente à Competência 6.4 do DigCompEdu, que aborda o uso responsável das tecnologias digitais no ambiente educacional. Ambas as referências são essenciais para a formação e qualificação da comunidade acadêmica em segurança digital, especialmente em um contexto de crescente digitalização das práticas pedagógicas e administrativas.

Portanto, a ausência de orientações ou medidas específicas nesses documentos reforça a necessidade de ações estratégicas que fomentem a capacitação digital na Unesp, tanto para prevenir riscos cibernéticos quanto para assegurar a privacidade e a proteção de dados de toda a comunidade universitária. Essa lacuna representa um ponto crítico, especialmente considerando a relevância da instituição como produtora de ciência e tecnologia no Brasil.

REFERÊNCIAS

- ALAVES, J. A. As vidas paralelas de Alan Turing e Edmundo Curvelo e a matematização da mente. In Espírito Santo, J. (ed.), **Alan Turing: cientista universal** (p. 137-163). Editora UMinho. DOI: <https://doi.org/10.21814/uminho>. Disponível em: <https://repositorium.sdum.uminho.pt/handle/1822/70116>. Acesso em: 10 ago. 2024
- ANJOS, A. M.; SILVA, G. E. G. **Tecnologias Digitais da Informação e da Comunicação (TDIC) na Educação**. Ministério da Educação – Universidade Aberta do Brasil, 2018. Disponível em: https://educapes.capes.gov.br/bitstream/capes/433309/2/TDIC%20na%20Educa%C3%A7%C3%A3o%20%20compilado_19_06-atualizado.pdf. Acesso em: 10 ago. 2024
- BARROS, D. M. V. et al. (orgs.). Educação e tecnologias: reflexão, inovação e práticas. Lisboa: [s.n.], 2011. Disponível em: https://www.researchgate.net/publication/288993534_Educacao_e_tecnologias_reflexao_inovacao_e_praticas. Acesso em: 09 out. 2024.
- BATLLE, J.; PUJOLÀ, J. T. La competencia digital docente en las prácticas de educación primaria: las reflexiones sobre el uso de la tecnología en las aulas. **Perspectiva**, [S.L.], v. 42, n. 1, p. 1-22, 1 fev. 2024. Universidade Federal de Santa Catarina (UFSC). <http://dx.doi.org/10.5007/2175-795x.2024.e93692>. Acesso em: 5 out. 2024.
- BRASIL. **Estratégia Brasileira para a Transformação Digital**. Brasília: Imprensa Nacional, 2018.
- BRASIL. IBGE (org.). **Internet já é acessível em 90,0% dos domicílios do país em 2021**. 2022. Editoria: Carmen Nery e Vinícius Britto. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/34954-internet-ja-e-acessivel-em-90-0-dos-domicilios-do-pais-em-2021>. Acesso em: 20 out. 2024.
- BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709, **Diário Oficial da União**, 14 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 ago. 2024.
- BITDEFENDER (Brasil). **O que é um Exploit?** Prevenção de Exploits. s.d. Disponível em: <https://www.bitdefender.com.br/consumer/support/answer/27646/>. Acesso em: 11 dez. 2024.
- CANTABRANA, J. L. L.; CERVERA, M. G. El desarrollo de la competencia digital docente a partir de una experiencia piloto de formación en alternancia en el Grado de Educación. **Educación**, [S.L.], v. 51, n. 2, p. 321-348, 1 jul. 2015. Universitat Autònoma de Barcelona. <http://dx.doi.org/10.5565/rev/educar.725>. Disponível em: <https://educar.uab.cat/article/view/v51-n2-lazaro-gisbert/725-pdf-es>. Acesso em: 18 set. 2024.
- CARVALHO, M. A. G.; MARRONI, L. S.; TAVARES, A. A. **Avaliação de competências digitais dos docentes do ensino superior brasileiro**.

MetaRed: Brasil, 2020. Disponível em:

<https://www.semesp.org.br/wpcontent/uploads/2021/04/Avaliacao-de-Competencias-Digitais-1.pdf>. Acesso em: 27 nov. 2024.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.BR). **Resumo Executivo TIC Educação 2020**: edição covid-19 metodologia adaptada. São Paulo: Cetic.Br, 2020. 8 p. Disponível em:

https://www.cetic.br/media/docs/publicacoes/2/20211124200731/resumo_executivo_tic_educacao_2020.pdf. Acesso em: 05 out. 2024.

CETIC.BR; NIC.BR; NIC.BR. (Brasil). **Segurança para Internet Proteção de Dados**. São Paulo: Cetic.Br, 2021. 8 p. Disponível em:

https://cartilha.cert.br/fasciculos/protec_ao-de-dados/fasciculo-protecao-de-dados.pdf. Acesso em: 12 out. 2024.

CORREIO BRAZILIENSE (Distrito Federal). **Registros de golpes na internet crescem 310% no DF durante a pandemia**. 2020. Elaborado por Jaqueline Fonseca. Disponível em:

<https://www.correiobrasiliense.com.br/cidadesdf/2020/08/4868977-mais-golpes-na-pandemia.html>. Acesso em: 12 nov. 2024.

COSTA, I. R.; PINTO, L. F. C. **A evolução dos dispositivos de armazenamento de dados na perspectiva da história**. 2017. 29 f.

Monografia (Graduação) - Curso de Informática, Universidade Federal do Maranhão, São Luís, 2017. Disponível em:

<https://monografias.ufma.br/jspui/bitstream/123456789/2830/1/IsraelReisCosta.pdf>. Acesso em: 13 nov. 2024.

CRESWELL, J. W. **Projeto de pesquisa métodos qualitativo, quantitativo e misto**. Tradução: Lúcia de Oliveira da Rocha. 5. ed. Porto Alegre: Artmed, 2007. Acesso em: 4 nov. 2024.

FLORESTA, K. B.; WEXLER, J. A primer on digital environments. In:

FLORESTA, Katherine B.; WEXLER, Jerrold. **Is Justice Real When reality Is Not?** Massachusetts, EUA: Academic Press, 2023. Cap. 1. p. 1-12. ISBN-13: 978-0323956208.

FLORIDI, L. Information ethics: on the theoretical foundations of computer ethics. **Ethics and Information Technology**, v. 1, n. 1, p. 37–56, 1999.

FOVINO, I. N. *et al.* **Cybersecurity, our digital anchor**: executive summary. EUR 30277 EN, Publications Office of the European Union, Luxembourg, 2020. Disponível em: <https://doi.org/10.2760/33974>. Acesso em: 14 fev. 2023.

FURNELL, S.; SHAH, J. N. Home working and cyber security – an outbreak of unpreparedness?. **Computer Fraud and Security**. v.8, 2020, p. 6–12.

Disponível em: [http://10.1016/S1361-3723\(20\)30084-1](http://10.1016/S1361-3723(20)30084-1). Acesso em: 19 set. 2024.

GOUVEIA, L. B. **Gestão da Segurança da Informação**. Porto: UFP, 2016. 42 p. Disponível em:

https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf. Acesso em: 20 ago. 2024.

HAYNES, D. Creating an Ontology of Risk: a human-mediated process. **The Human Position In An Artificial World: Creativity, Ethics and AI in Knowledge Organization**, [S.L.], p. 166-180, 2019. Ergon Verlag.

<http://dx.doi.org/10.5771/9783956505508-166>. Acesso em: 20 ago. 2024.

HUREL, L. M. Governing Cyber Incidents: challenges and opportunities for Brazil and the EU. Policy Papers, Rio de Janeiro, p. 185-203, 2021. **XVIII Forte de Copacabana Conferência de Segurança Internacional**, Rio de Janeiro, 2021. Disponível em:

<https://www.cebri.org/media/documentos/arquivos/XVIIIForte-KAS-CEBRI-UEausenc612e72f87749d.pdf>. Acesso em: 10 jun. 2024.

LALLIE, H. S. et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. **Computers & Security**, v. 105, 2021. Disponível em:

<https://doi.org/10.1016/j.cose.2021.102248>. Acesso em: 12 ago. 2024.

LOBATO, M. **Memórias da Emília**. 2. ed. São Paulo: Globo, 2009. Disponível em: <https://www.brejosanto.ce.gov.br/wp-content/uploads/2023/04/Memorias-da-Emilia.pdf>. Acesso em: 07 dez. 2024.

LUCAS, M; MOREIRA, A; TRINDADE, A. R. **DIGCOMP 2.2**: Quadro Europeu de Competência Digital para Cidadãos com exemplos de conhecimentos, capacidades e atitudes, Universidade de Aveiro, Portugal, 2022, 978-972-789-813-8, Disponível em:

<https://digital.dge.mec.pt/sites/default/files/documents/2023/237-afcfb229158fb9121960b0b96ea215d4.pdf>. Acesso em: 10 nov. 2024

LUCAS, M; MOREIRA, A; TRINDADE, A. R. **DigCompEdu**: Quadro Europeu de Competência Digital para Educadores. Universidade de Aveiro, Portugal, 2018, 978-972-789-580-9, Disponível em:

https://aefreamunde.com/attachments/article/185/2_DigCompEdu_Quadro%20Europeu%20Compet%C3%Aancia%20Digital%20Educadores.pdf. Acesso em: 10 nov. 2024

MALERBA, C. **Vulnerabilidade e Exploits**: técnicas, detecção e prevenção. 2010. 68 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010. Disponível em:

<https://www.lume.ufrgs.br/bitstream/handle/10183/26337/000757768.pdf>.

Acesso em: 10 nov. 2024

MARQUES, R. A resignificação da educação e o processo de ensino e aprendizagem no contexto de pandemia da covid-19. **Boletim de conjuntura (boca)**, ano II, vol. 3, n. 7, 2020. Disponível em:

<https://revista.ufrn.br/boca/article/view/Marques>. Acesso em: 29 out. 2024.

MASCARENHAS NETO, P. T.; ARAÚJO, W. J. **Segurança da Informação**: uma visão sistêmica para implantação em organização. João Pessoa: Ufpb, 2019. 159 p. Disponível em:

<http://www.editora.ufpb.br/sistema/press5/index.php/UFPB/catalog/download/209/75/905-1?inline=1>. Acesso em: 10 nov. 2024.

NACIONAL GEOGRAPHIC BRASIL (Brasil). **O que é um deepfake?** 2023. Disponível em: <https://www.nationalgeographicbrasil.com/ciencia/2023/11/o-que-e-um-deepfake>. Acesso em: 16 dez. 2024.

NAKAMURA, E.; GEUS, P. **Segurança de redes em ambientes corporativos**. São Paulo: Berkeley Brasil, 2002. Disponível: https://www.academia.edu/9475240/Seguran%C3%A7a_de_Nets_Cooperativos. Acesso em: 10 nov. 2024

NAVARRO, A. M. N. P.; LEONARDOS, G. V. Privacidade Informacional: Origem e Fundamentos no Direito Norte-Americano. In: CONPEDI/UFF. (Org.). **XXI Congresso Nacional do CONPEDI/UFF**. 1ed.: FUNJAB, 2012, v., p. 302-320. Disponível: <http://www.publicadireito.com.br/artigos/?cod=34f9a343f945196b>. Acesso em: 15 nov. 2024.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). **Aparelho celular é a principal ferramenta de estudo e trabalho na pandemia**. 2020. Disponível em: <https://www.nic.br/noticia/na-midia/aparelhocelular-e-a-principal-ferramenta-de-estudo-e-trabalho-na-pandemia/>. Acesso em: 20 nov. 2024.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Aparelho celular é a principal ferramenta de estudo e trabalho na pandemia**. 2020. Disponível em: <https://www.nic.br/noticia/na-midia/aparelhocelular-e-a-principal-ferramenta-de-estudo-e-trabalho-na-pandemia/>. Acesso em: 20 out. 2024.

PRODEST (Espanha). **Entenda o que é phishing e adote medidas para evitá-lo**. s.d. Disponível em: <https://prodest.es.gov.br/entenda-o-que-e-phishing-e-adote-medidas-para-evita-lo#:~:text=Ele%20consiste%20em%20tentativas%20de,e%2Dmail%20com%20conte%C3%BAdo%20duvidoso>. Acesso em: 11 dez. 2024.

PUNIE, Y.; AND BRECKO, B.; FERRARI, A. **DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe**, Publications Office of the European Union, Luxembourg, 2013, ISBN 978-92-79-31465-0, Disponível em: <https://publications.jrc.ec.europa.eu/repository/handle/JRC83167>. Acesso em: 10 out. 2024.

REMOTE PORTUGAL (Portugal). **O que é o Trabalho Remoto?: e como começar**. 2021. Disponível em: <https://remoteportugal.pt/o-que-e-o-trabalho-remoto-mitos-e-como-encontrar/>. Acesso em: 11 dez. 2024.

RODRIGUES, R. B. Identificando tecnologias emergentes em TIC. In: RODRIGUES, R. B. **Novas Tecnologias da Informação e da Comunicação**. Recife: Rede E-Tec Brasil, 2016. p. 42. Disponível em: https://www.ufsm.br/app/uploads/sites/413/2018/12/arte_tecnologias_informacao_comunicacao.pdf. Acesso em: 12 out. 2024.

SÃO PAULO. Dispõe sobre a colocação de placa informativa sobre filmagem de ambientes, e dá outras providências. nº 13.541, 24 de março de 2003. **Diário Oficial da Cidade**. São Paulo, 24 mar. 2003. Disponível em:

<http://legislacao.prefeitura.sp.gov.br/leis/lei-13541-de-24-de-marco-de2003/detalhe/5cc726c814119216b2030256>. Acesso em: 12 nov. 2024.

SECURITY LEADERS (Brasil). **Universidade Federal do Mato Grosso do Sul sofre ataque cibernético**. 2023. Elaborado por Bruno Silva. Disponível em: <https://securityleaders.com.br/universidade-federal-do-mato-grosso-do-sul-sofre-ataque-cibernetico/>. Acesso em: 10 out. 2024.

SHALLIT, J. **A Very Brief History of Computer Science**. 1995. Disponível em: <https://cs.uwaterloo.ca/~shallit/Courses/134/history.html>. Acesso em: 14 nov. 2024.

SILVA, K. K. A. D.; BEHAR, P. A. Competências digitais na educação: uma discussão acerca do conceito. **Educação em Revista**, v. 35, p. e209940, 2019. Disponível em: <https://www.scielo.br/j/edur/a/wPS3NwLTxtKgZBmpQyNfdVg/abstract/?lang=pt#ModalHowcite>. Acesso em: 5 de nov. 2024

SILVA, R. C. *et al.* História e Segurança da Informação: um estudo sobre a segunda guerra mundial e o desenvolvimento da criptografia a partir de uma perspectiva integrada. In: PEREIRA, Denise (org.). **A transversalidade da prática do profissional de história**. Ponta Grossa: Atena, 2019. Cap. 19. p. 179-194. Acesso em: 5 de nov. 2024

SOARES, H. J.; ARAÚJO, N. V. S.; SOUZA, P. Privacidade e Segurança Digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade. 2020, Cuiabá. **Anais do I Workshop sobre as Implicações da Computação na Sociedade**. Porto Alegre: Sociedade Brasileira de Computação, 2020. p. 97-106. ISSN 2763-8707. DOI: <https://doi.org/10.5753/wics.2020.11040>. Acesso em: 6 de nov. 2024

SONICWALL (Califórnia). **Tipos de ataques cibernéticos e como preveni-los**. Santa Clara: Sonicwall, 2017. 12 p. Disponível em: <https://www.sonicwall.com/medialibrary/pt/ebook/ebook-tipos-de-ataquesciberneticos-e-como-preveni-los.pdf>. Acesso em: 20 nov. 2024.

TRIBUNAL DE JUSTIÇA DE SANTA CATARINA (TJSC). **Entenda como funcionam os ataques de hackers na Internet**. Santa Catarina. s.d. Disponível em: https://www.tjsc.jus.br/web/servidor/dicas-de-ti/-/asset_publisher/OrjJEBzj2Oes/content/entenda-como-funcionam-os-ataques-de-hackers-na-internet. Acesso em: 11 dez. 2024.

UNIVERSIDADE ESTADUAL PAULISTA (UNESP). **Guia de profissões Unesp**. São Paulo: Unesp, 2024. 173 p. Disponível em: <https://vestibular.Unesp.br/Home/guiadeprofissoes51/guia-Unesp-de-profissoes-2025-1.pdf>. Acesso em: 12 nov. 2024.

UNICEF (Nova York). **Cyberbullying: O que é e como pará-lo**. 2021. Disponível em: <https://www.unicef.org/brazil/cyberbullying-o-que-eh-e-como-para-lo>. Acesso em: 11 dez. 2024.