Manual CYBER.VET.EU

Melhorar a prontidão em termos de cibersegurança do setor europeu do ensino e formação profissional

2020-1-DE02-KA226-VET-008327

REDE TANDEM PLUS com o consórcio CYBER.VET.EU:

Co-funded by the Erasmus+ Programme of the European Union

Sumário

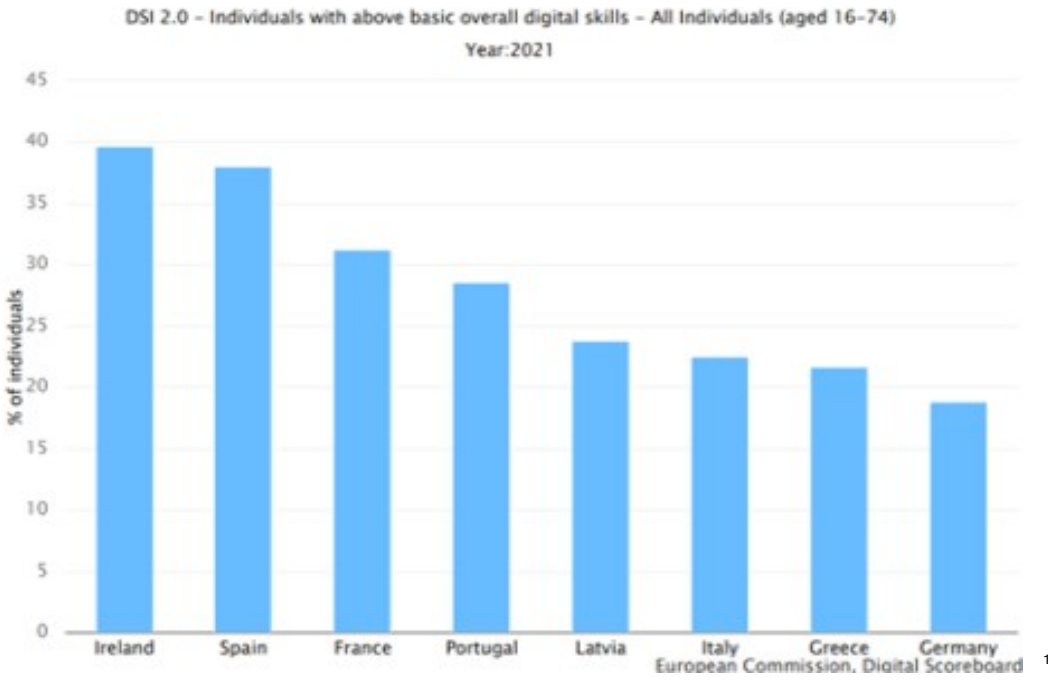
Sumário

a) A implementação do projeto CYBER.EU.VET

A União Europeia enfrenta um desafio histórico representado pela pandemia de Covid-19. Muitos setores são fortemente atingidos por estas crises e a educação é certamente um deles.

Cada vez mais utilizadores são forçados a recorrer a aulas ou formações online, como tal, a importância de reconhecer as ameaças diárias à nossa segurança é agora mais importante do que nunca. Este tema é reconhecido como fundamental também pela Comissão Europeia que organiza, todos os anos, um Mês Europeu da Cibersegurança, cujo website já inclui algum material educativo e campanhas de sensibilização específicas como a "Get cyber Skilled" em 2018.

O projeto CYBER.EU.VET inclui 8 parceiros (ONG NEST – Alemanha (COORDENADOR), MEATH COMMUNITY RURAL AND SOCIAL DEVELOPMENT PARTNERSHIP LIMITED – Irlanda, TANDEM PLUS – uma rede da UE sediada em França, COFAC COOPERATIVA DE FORMAÇÃO E ANIMAÇÃO CULTURAL CRL- Portugal , LATVIJAS ASOCIACIJA EIROPAS KOPIENAS STUDIJAM – Letónia, ASOCIACION EDUCATIVA POR LA INTEGRACION Y LA IGUALDAD – Espanha, INECIA DIGITAL – Espanha, Extrafondente Open Source – Itália)



[1]

[1] Perfil de Indicador ESMS Profile (ESMS-IP) Agência de compilação: Eurostat, o Serviço de Estatística da União Europeia.

O principal objetivo do **CYBER.EU.VET**é reforçar a capacidade do EFP europeu para reconhecer e gerir ameaças de cibersegurança (por exemplo, ataques de phishing, botnets, fraudes financeiras e bancárias, fraudes de dados) num contexto histórico em que a formação online é cada vez mais utilizada.

i. Impacto do Projeto:

O projeto teve impacto a nível local, regional e nacional, envolvendo diferentes níveis de partes interessadas, oferecendo soluções personalizadas para atender às necessidades dos níveis locais, mas alinhadas a um nível superior, desenvolvendo, através da parceria, material de formação e normas aplicáveis em toda a UE.

Em particular, o impacto nos participantes diretos e nos principais grupos-alvo foi:

- Educadores de EFP - Uma capacidade de ensino reforçada, acrescentando às suas competências um conhecimento das principais ameaças à segurança digital.
- Educadores e alunos de EFP - competências digitais melhoradas graças ao material de formação educativo.
- Educadores e alunos de EFP: uma maior sensibilização sobre as ameaças e os seus riscos reais, tanto económicos como sociais.
- As instituições de EFP estarão mais preparadas para enfrentar os riscos de cibersegurança com as ferramentas CYBER.VET.EU tanto para os seus educadores como para os seus alunos.

ii. Público-alvo do projeto

Espera-se que o projeto tenha um impacto positivo e de longo prazo nas diferentes partes interessadas envolvidas no projeto, em particular:

- - Estudantes do EFP
- - Voluntários especialistas em segurança cibernética
- - Redes de instituições de EFP
- Decisores políticos

iii. Objetivos do projeto CYBER.EU.VET

- O primeiro objetivo específico será ter educadores de EFP mais preparados em termos de gestão de ameaças à cibersegurança, dado o seu papel central na transferência de conhecimentos de boas práticas e competências para os seus alunos.
- O segundo objetivo específico é aumentar a sensibilização dos professores e alunos do EFP e dos seus familiares, assim como sensibilizar para importância de reconhecer esses riscos diários, que podem ter um impacto económico e social em todos os cidadãos europeus.
- O terceiro objetivo específico é apoiar as instituições públicas e as instituições de EFP a estarem mais preparadas para enfrentar este tipo de desafios, fornecendo-lhes orientações para futuras implementações.

iv. Resultados Intelectuais:

- O1: Análise da investigação: principais desafios de cibersegurança e melhores práticas (parceiro responsável: NGO NEST BERLIN EV - E10166639)
- O2: Material de formação de sensibilização de cibersegurança para o setor de EFP (parceiro responsável: INERCIA DIGITAL SL (E10145080,)
- O3: Toolkit formação para formadores (parceiro responsável INERCIA DIGITAL SL (E10145080)
- O4: Manual de Cibersegurança para instituições de EFP: melhores práticas, material de formação e orientações para implementações futuras (parceiro responsável TANDEM PLUS - E10103913)

Paralelamente ao desenvolvimento dos resultados intelectuais, o outro objetivo do projeto é divulgar os nossos resultados e produtos em toda a UE para potenciais participantes, multiplicadores e interessados com vista a aumentar o impacto e a relevância do CYBER.EU.VET.

v. O que é a cibersegurança?

A definição formal de **cibersegurança** na legislação da UE encontra-se no texto da Lei de Cibersegurança da UE: "*cibersegurança significa as atividades necessárias para proteger redes e sistemas de informação, os utilizadores desses sistemas e outras pessoas afetadas por ciberameaças*" (Art. 2.1).

A legislação da UE, ao adotar a abordagem de "*proteção de redes e sistemas de informação*", também salienta que a cibersegurança protege não apenas os sistemas de informação, mas também (e talvez mais importante) as pessoas, independentemente de serem utilizadores desses sistemas ou terceiros afetados de alguma forma por ciberameaças.

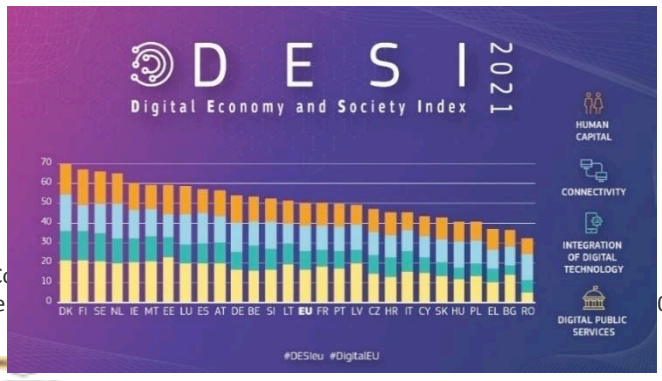
Em dezembro de 2020, a Comissão Europeia e o Serviço Europeu para a Ação Externa (SEAE) apresentaram uma nova estratégia de cibersegurança da UE com o objetivo de aumentar a resiliência às ciberameaças e garantir que os cidadãos e as empresas beneficiem de tecnologias digitais fiáveis.

O Regulamento (EU) 2021/887 que cria o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação estabelece o Centro Europeu de Competências em Cibersegurança (ECCC) e a Rede de Centros Nacionais de Coordenação (a "rede") e define as regras para os centros nacionais de coordenação (CNC) e para a criação da Comunidade de Competências em Cibersegurança.

O Centro Europeu de Competências em Cibersegurança ajuda a UE a reforçar a liderança da UE em cibersegurança,[2] melhorando a confiança e a segurança, incluindo a confidencialidade, a integridade e a acessibilidade dos dados, apoiando a resiliência e a fiabilidade das redes e sistemas de informação, incluindo infraestruturas críticas e hardware e software de utilização comum.

vi. Principal desafio de competências digitais na Europa

- Cerca de 70 milhões de europeus carecem de competências suficientes de leitura, escrita e numeracia
- 24% da população da UE não tem diploma do ensino secundário
- 13% dos europeus nunca utilizaram a Internet
- 43% da população da UE e 35% da força de trabalho da UE têm competências digitais insuficientes
- 42% das pessoas sem competências digitais estão desempregadas



[2] Regulamento (UE) 2021/887 do Parlamento Europeu e do Co de Competências Industriais, Tecnológicas e de Investigação em Cibe 02, 8.6.2021, pp. 1-31)

- Nativos digitais ≠ competência digital[3]

vii. Enquadramento

Mais de 70% das empresas afirmaram que a falta de pessoal com competências digitais adequadas é um obstáculo ao investimento. A Europa também enfrenta uma escassez de especialistas digitais que possam desenvolver tecnologias de ponta para o benefício de todos os cidadãos.

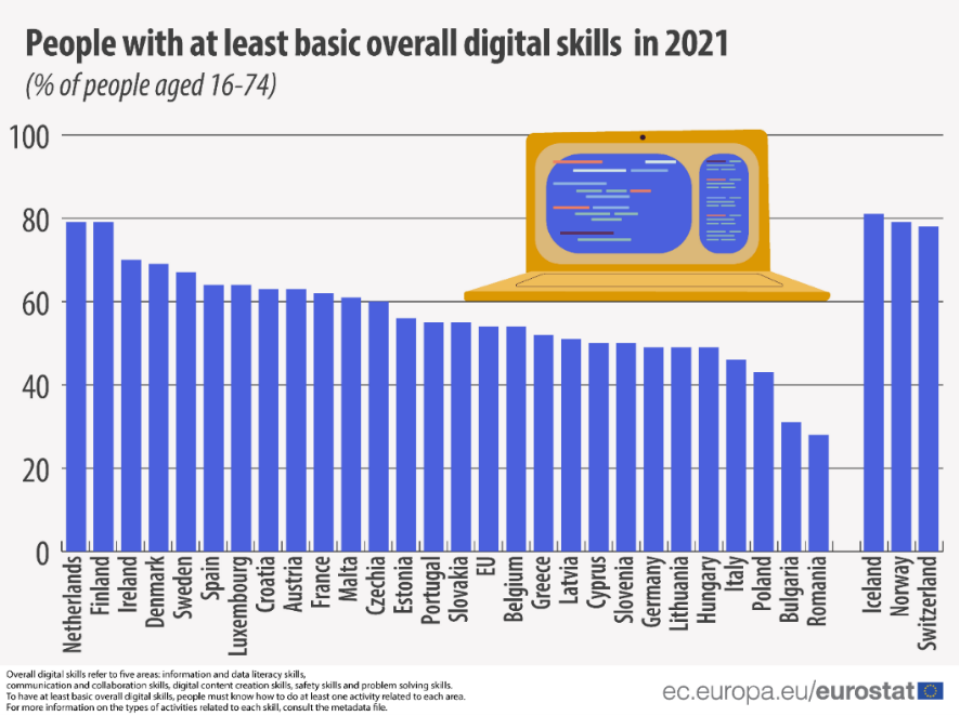
Uma economia digital forte impulsionada por europeus com competências digitais é vital para a inovação, o crescimento, o emprego e a competitividade europeia. A disseminação das tecnologias digitais está a ter um enorme impacto no mercado de trabalho e no tipo de competências necessárias na economia e na sociedade. Os Estados-Membros, as empresas, os fornecedores de formação, a Comissão Europeia e outras organizações têm de trabalhar em conjunto para colmatar o défice de competências digitais. Para acompanhar o desenvolvimento da transição digital e a lacuna de competências digitais, a Comissão publica anualmente o DESI [Indicador de Competências Digitais]. Segue o desempenho digital dos Estados Membros em diferentes áreas para monitorizar o progresso e identificar onde são necessários mais esforços.

Em 2021, 54% das pessoas na UE com idades compreendidas entre os 16 e os 74 anos tinham, pelo menos, competências digitais gerais básicas.

Em 2021, a percentagem de pessoas com idades compreendidas entre os 16 e os 74 anos que possuíam, pelo menos, competências digitais gerais básicas era mais alta nos Países Baixos e na Finlândia (ambos 79%), seguidos pela Irlanda (70%). Por outro lado, a percentagem mais baixa foi registada na Roménia (28%), seguida pela Bulgária (31%) e Polónia (43%).

Os indicadores de competências digitais são alguns dos principais indicadores de desempenho no contexto da Década Digital, que define a visão da UE para a transformação digital. O Digital Compass define o objetivo de que 80% dos cidadãos da UE com idades compreendidas entre os 16 e os 74 anos tenham, pelo menos, competências digitais básicas até 2030.

[3] Referências: Relatório DESI 2018 – Human Capital; 2017 Education and Training monitor, 2016 Skills Communication, ICILS 2013



Voltar para o conteúdo ↑

b) Competências digitais de educadores do EFP – uma visão do consórcio

i. Alemanha:

- O Relatório de Dados do EFP (2019) elaborado pelo Instituto Federal Alemão de Educação e Formação Profissional (BIBB) afirmou que "A digitalização vai reforçar as alterações estruturais do mercado de trabalho", apontando para a necessidade de uma mudança nas capacidades de formação nas respetivas áreas.

  Conforme delineado na Resolução da Conferência Permanente dos Ministros da Educação e dos Assuntos Culturais (2016-2017) na área do ensino profissional, a promoção de competências relacionadas com o trabalho no contexto do trabalho digital e dos processos empresariais é uma parte essencial da competência dos professores como ponto de partida para as suas atividades didáticas.

ii. Irlanda:

- Uma das principais estratégias da Irlanda em relação às competências digitais dos educadores de EFP é a Estratégia Digital Nacional, lançada em julho de 2013. A estratégia centra-se no envolvimento digital e destaca como a Irlanda pode beneficiar de uma sociedade digitalmente envolvida.

  Relativamente às competências digitais dos educadores de EFP, as evidências continuam a destacar que existir uma divisão crescente entre os educadores que utilizam dispositivos digitais nas suas aulas como ferramenta de aprendizagem e aqueles que não utilizam.

iii. Portugal:

- O sistema nacional de qualificações reorganizou o EFP num sistema único em que os programas conduzem a uma dupla certificação. O EFP para adultos é parte integrante do sistema nacional de qualificações, tendo como elementos-chave os programas de ensino e formação de adultos e o reconhecimento e validação das aprendizagens anteriores. Portugal tem feito progressos significativos em termos de escolaridade, mas continua abaixo da média da UE. Embora inferior a 2015 (73,7%), em 2019 a percentagem de pessoas com baixo nível ou nenhuma qualificação foi de 50,2%, a mais elevada da UE.

iv. Itália:

- Na área da educação, as ações foram realizadas principalmente através da implementação do Plano Nacional da Escola Digital. As diretrizes do Ministério da Educação, Universidade e Investigação lançaram uma estratégia global de inovação para a escola italiana e para um novo posicionamento do seu sistema educativo na era digital. A maior parte das ações de formação do pessoal escolar destinam-se às escolas primárias e secundárias, que representam a maioria das escolas em Itália, tendo sido dada pouca atenção ao setor do Ensino e Formação Profissional (EFP).

v. Espanha:

- A Agenda Digital para Espanha (ADpE, Agenda Digital para España) publicada em 2013 é o roteiro para o cumprimento dos objetivos definidos pela Agenda Digital para a Europa em 2015 e 2020, assim como a realização de objetivos específicos para o desenvolvimento da

economia e da sociedade digital em Espanha. Está estruturada em torno de seis grandes objetivos e vários planos específicos. O sexto objetivo é promover a inclusão e a literacia digital e a formação de novos profissionais de TIC.

vi. França

- Olhando para o ritmo de formação sobre a utilização das TIC nas universidades francesas que a oferecem, verifica-se que não existem políticas claras e sustentadas de formação de formadores sobre a utilização das TIC/E. Cerca de 58% relatam apenas uma sessão de formação por ano em comparação com 7,4% por mês e 0,5% por semana.
  As estatísticas mostram que a densidade da formação em TI varia de uma região de língua francesa para outra. Existem várias razões para isso, sendo que as mais significativas estão, sem dúvida, ligadas às instituições académicas e aos seus governos.

vii. Letónia

- Em 2020, o Ministério da Educação e Ciência da República da Letónia estabeleceu como meta prioritária de competência profissional a melhoria da competência digital dos educadores, atribuindo para o efeito financiamento adicional (0,5 milhões de euros). A necessidade de sensibilizar os alunos e educadores sobre a segurança da informação, a proteção da privacidade e a utilização de serviços eletrónicos fiáveis (Estratégia de Cibersegurança 2019-2022, área de ação "Sensibilização pública, ensino e investigação").

viii. Grécia

- Embora a aquisição de competências digitais seja uma componente que não deva estar ausente do conjunto de ferramentas educativas dos Educadores de EFP, pode identificar-se uma lacuna importante através da monitorização do atual sistema de ensino da Grécia. Apesar das muitas reformas do currículo educativo, as evidências sugerem que os educadores não estão suficientemente equipados com o conhecimento das TIC e, portanto, faltam ferramentas e técnicas pedagógicas e orientadas para o digital que possam atualizar o processo de ensino (Ministério da Educação, 2019).

Conclusões

A investigação desenvolvida para o projeto CYBER.EU.VET revelou que existe uma carência de dados e informações sobre as competências e desafios de cibersegurança dos educadores das instituições de

ensino a nível europeu, assim como um número limitado de iniciativas focadas nas questões de cibersegurança no EFP, indicando que o projeto CYBER.EU.VET abordou o tema emergente em todos os Estados-Membros. Atualmente, a maioria das atividades e projetos focam-se na sensibilização da população em geral para a cibersegurança e melhoria das competências digitais gerais dos educadores, o que foi influenciado pela rápida adaptação ao processo de aprendizagem/trabalho remoto.

O consórcio de parceiros é multifacetado e uma expressão clara de um grau diferente de competências digitais em toda a Europa. No entanto, independentemente da classificação do DESI dos países individuais, este Relatório de Investigação do Consórcio pode ser utilizado para extrair indicações significativas e válidas para todo o contexto europeu. O sentimento de necessidade de formação é óbvio, mesmo entre os professores de EFP que já receberam formação em TIC. Não existe rejeição da necessidade de formação, nem questionamento da sua utilidade. Constatamos igualmente que quanto mais os professores se sentem expostos a riscos psicossociais, éticos, jurídicos, técnicos ou de saúde, mais dizem sentir necessidade de formação. De acordo com um inquérito nacional, mais de metade dos professores que se sentem vulneráveis ao cyberbullying sentem que a formação é necessária. Para eles, a formação inicial e contínua é uma oportunidade de partilhar experiências e analisar métodos de atuação profissional neste campo. Ainda se acredita que a utilização de ferramentas digitais no ensino é uma forma de ensinar ou um objeto a ser ensinado aos alunos e não parte integrante da sua cultura geral. Deve desenvolver-se uma cultura de fontes de informação e práticas sobre riscos digitais (investigação e monitorização). Também é necessário intensificar a formação sobre os desafios da tecnologia digital e, em particular, sobre os problemas psicossociais, éticos, jurídicos e técnicos que podem surgir na utilização das ferramentas digitais e que preocupam os professores a ponto de os levar a desistirem de qualquer utilização.

Assim, o conhecimento dos riscos digitais pode influenciar positivamente as práticas pedagógicas para a formação de alunos em literacia digital. Um professor com uma forte cultura digital estará mais inclinado a utilizar a tecnologia digital na sala de aula com os seus alunos e a fazer da tecnologia digital um objeto de ensino-aprendizagem.

A influência óbvia da representação dos riscos é impossível de mudar positivamente sem uma cultura digital geral e plural, complementar a uma cultura da informação no sentido mais amplo, que evite a demonização do objeto técnico e permita explorar o potencial educativo.

Não se trata de educar com medo, mas de emancipar (e ser emancipado, como professor também) através de uma apreensão crítica e esclarecida do mundo digital.

Voltar para o conteúdo ↑

c) Toolbox CYBER.EU.VET

De acordo com o Plano de Ação para a Educação Digital 2021-2027, as competências digitais e os desafios de aprendizagem também têm alta prioridade na agenda europeia. A Comissão Europeia está determinada em combater a lacuna de competências digitais e a promover projetos e estratégias para melhorar o nível de competências digitais na Europa. Todos os europeus precisam de competências digitais para estudar, trabalhar, comunicar, aceder a serviços públicos online e encontrar informações fiáveis. No entanto, muitos europeus não possuem competências digitais adequadas. O Índice de Digitalidade da Economia e Sociedade (DESI) mostra que 4 em cada 10 adultos e cada três pessoas que trabalham na Europa não possuem competências digitais básicas. Também há uma baixa representação de mulheres em profissões e estudos relacionados com a tecnologia, sendo que apenas 1 em cada 6 especialistas em TIC e 1 em cada 3 diplomados em ciências, tecnologia, engenharia e matemática (STEM) são mulheres.

A Comissão Europeia estabeleceu metas na agenda europeia de competências e no plano de ação de educação digital para garantir que 70% dos adultos tenham competências digitais básicas até 2025. Estas iniciativas visam reduzir o nível de jovens entre os 13 e os 14 anos com desempenho inferior em informática e literacia digital de 30% (2019) para 15% em 2030. A Plataforma para as Competências e o Emprego na Área Digital é uma nova iniciativa lançada ao abrigo do Mecanismo Interligar a Europa. Oferece informações e recursos sobre competências digitais, assim como oportunidades de formação e financiamento.[4]

i. Quadros de competências digitais RC/CE

- Quadro Europeu de Competência Digital para Cidadãos (DigComp)
- Quadro Europeu de Competência Digital para Educadores (DigCompEdu)
- Quadro Europeu de Competência Digital para Organizações Educacionais (DigCompOrg) e uma ferramenta de autorreflexão para escolas (SELFIE)

Porquê todos estes quadros?

- Capacitação para a transformação digital de E&F e para enfrentar os desafios de competências do século XXI.

[4] Digital skills and jobs | Shaping Europe's digital future (europa.eu)

- Quadros de referência que fornecem uma compreensão geral, completa e partilhada: uma linguagem comum.

O quê?

- Modelo conceptual, níveis de proficiência e módulos de (auto)avaliação.
- Competência definida como Conhecimentos, Habilidades e Atitudes.

ii. O DigComp 2.2

Mais de 250 novos exemplos de conhecimentos, competências e atitudes para ajudar os fornecedores de educação e formação a atualizarem o seu currículo DigComp e material de cursos para enfrentar os desafios de hoje.

A lista de competências e áreas do DigComp permanece a mesma:

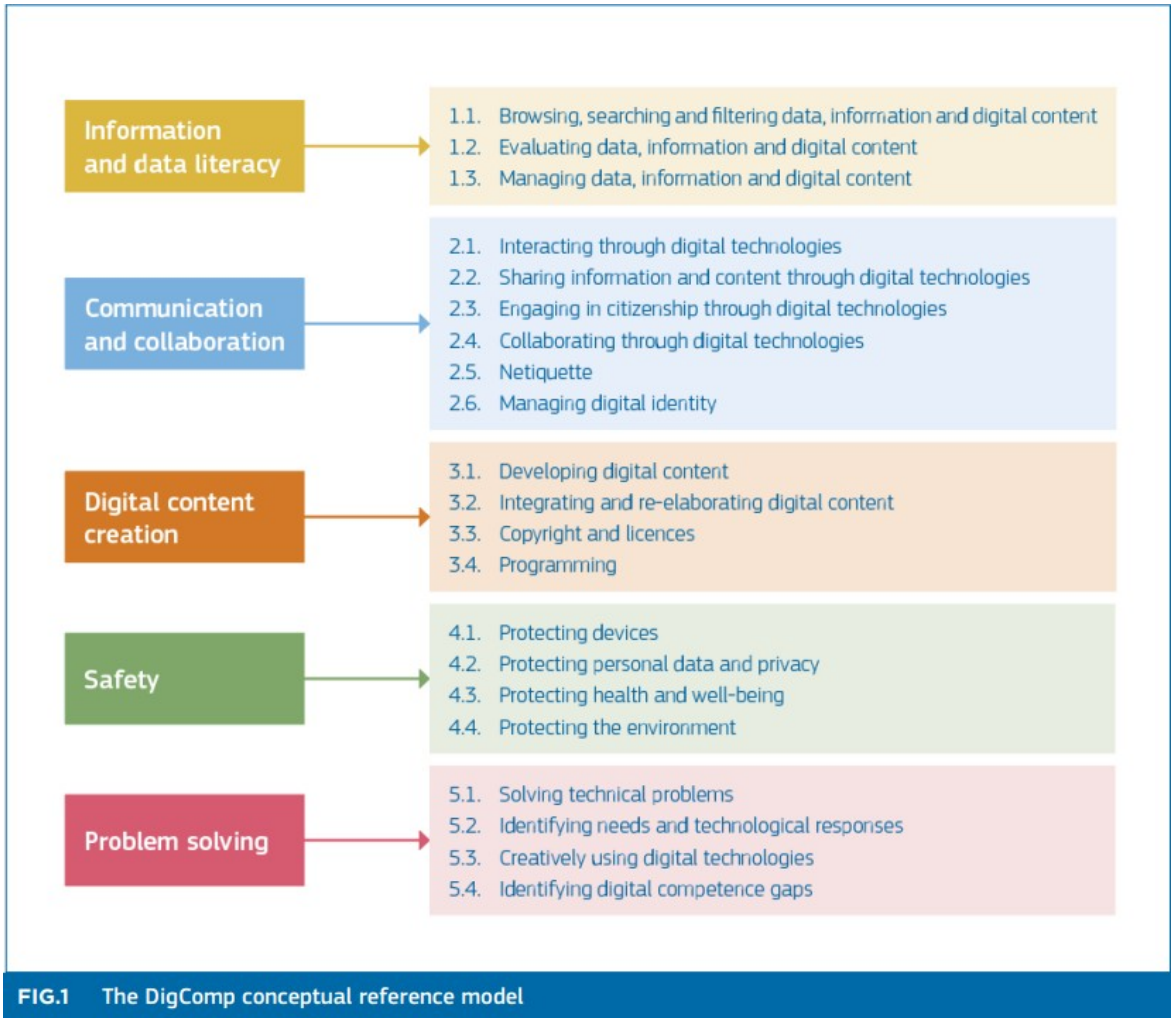


FIG.1 The DigComp conceptual reference model [5]

Um dos principais temas da atualização do DigComp 2.2 é o bem-estar e a segurança. Em cada área, existem 10-15 declarações por competência para ilustrar temas contemporâneos oportunos. Não representam uma lista exaustiva do que a competência em si implica e não estão organizados em níveis de proficiência, embora alguns sejam mais complexos do que outros, mas são úteis para o

[5] Commissão Europeia, Centro Comum de Investigação, Vuorikari, R., Kluzer, S., Punie, Y., DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes, Serviço das Publicações da União Europeia, 2022, https://data.europa.eu/doi/10.2760/115376

planeamento e atualização do currículo e para o desenvolvimento do programa de formação do DigComp ou dos conteúdos do curso.

SEGURANÇA: "proteger dispositivos e conteúdos digitais e compreender riscos e ameaças em ambientes digitais. Conhecer as medidas de segurança e proteção e ter o devido respeito pela fiabilidade e privacidade."[6]

35

DIMENSION 1 • **COMPETENCE AREA**

4. SAFETY

DIMENSION 2 • **COMPETENCE**

4.1 PROTECTING DEVICES

To protect devices and digital content, and to understand risks and threats in digital environments.

To know about safety and security measures and to have a due regard to reliability and privacy.

DIMENSION 3 • **PROFICIENCY LEVEL**

FOUNDATION	1	At basic level and with guidance, I can:	• **identify simple** ways to protect my devices and digital content, and • differentiate simple risks and threats in digital environments. • choose simple safety and security measures, and • **identify simple** ways to have due regard to reliability and privacy.
	2	At basic level and with autonomy and appropriate guidance where needed, I can:	• **identify simple** ways to protect my devices and digital content, and • differentiate simple risks and threats in digital environments. • follow simple safety and security measures. • **identify simple** ways to have due regard to reliability and privacy.
INTERMEDIATE	3	On my own and solving straightforward problems, I can:	• **indicate well-defined and routine** ways to protect my devices and digital content, and • differentiate well-defined and routine risks and threats in digital environments, and • **select well-defined and routine** safety and security measures. • **indicate well-defined and routine** ways to have due regard to reliability and privacy
	4	Independently, according to my own needs, and solving well-defined and non-routine problems, I can:	• **organise** ways to protect my devices and digital content, and • **differentiate** risks and threats in digital environments. • **select** safety and security measures. • **explain** ways to have due regard to reliability and privacy.
ADVANCED	5	As well as guiding others, I can:	• **apply different** ways to protect devices and digital content, and • **differentiate a variety** of risks and threats in digital environments. • **apply** safety and security measures. • **employ different** ways to have due regard to reliability and privacy.
	6	At advanced level, according to my own needs and those of others, and in complex contexts, I can:	• **choose the most appropriate** protection for devices and digital content, and • **discriminate** risks and threats in digital environments. • **choose the most appropriate** safety and security measures. • **assess the most appropriate** ways to have due regard to reliability and privacy.
HIGHLY SPECIALISED	7	At highly specialised level, I can:	• **create solutions to complex problems with limited definition** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments. • **integrate my knowledge to contribute to professional practice and knowledge and guide others** in protecting devices.
	8	At the most advanced and specialised level, I can:	• **create solutions to solve complex problems with many interacting factors** that are related to protecting devices and digital content, managing risks and threats, applying safety and security measures, and reliability and privacy in digital environments. • **propose new** ideas and processes to the field.

7

iii. O DigCompEdu

[6] Luxemburgo: Serviço das Publicações da União Europeia, 2018 KE-01-18-834-EN-N.pdf
[7] Ibidem

O Quadro Europeu de Competência Digital para Educadores (DigCompEdu) é um quadro cientificamente sólido que descreve o que significa para os educadores serem competentes digitalmente. Fornece um quadro de referência geral para apoiar o desenvolvimento de competências digitais específicas para educadores na Europa. O DigCompEdu dirige-se a educadores de todos os níveis de ensino, desde a primeira infância ao ensino superior e de adultos, incluindo ensino e formação geral e profissional, educação para necessidades especiais e contextos de aprendizagem não formal.

O quadro DigCompEdu reflete os esforços realizados a nível internacional para captar e definir as competências digitais específicas de professores e formadores.

O objetivo é fornecer um quadro para aqueles que trabalham no setor educativo e do ensino superior e são responsáveis pelo desenvolvimento de modelos de competências digitais, por exemplo, decisores políticos nos Estados-Membros, autoridades regionais/locais, organizações de ensino, instituições (públicas ou privadas) que prestam serviços de formação e desenvolvimento profissional.

Assim, o valor acrescentado do quadro DigCompEdu é fornecer:

- uma base sólida que pode guiar a política a todos os níveis;
- um modelo que permite que as partes interessadas locais avancem rapidamente para o desenvolvimento de um
- instrumento concreto, adequado às suas necessidades, sem terem de desenvolver uma base conceptual para este trabalho;
- uma linguagem e lógica comuns que podem ajudar a discussão e troca de melhores práticas;
- um ponto de referência para os Estados-Membros e outras partes interessadas validarem a integralidade e

– abordagem das suas próprias ferramentas e quadros existentes e futuros[8]

iv. CONSTRUIR A CAPACIDADE DE COMPETÊNCIAS DIGITAIS DO EDUCADOR DE EFP

Utilizar ou desenvolver estruturas ou ferramentas de autoavaliação é uma boa forma de determinar o nível básico de capacidade de competências digitais de um educador. A partir daí, é possível mapear as atividades de desenvolvimento profissional direcionadas. A juntar à crescente necessidade de utilizar tecnologias na sua prática docente, temos a exigência de mudar a pedagogia para garantir que as ferramentas digitais sejam utilizadas de forma eficaz não apenas no ensino, mas também na conceção e avaliação de cursos. O Quadro Europeu de Competência Digital para Educadores (DigCompEdu) descreve as principais áreas de competência exigidas pelos educadores à medida que aprofundam o seu envolvimento com a aprendizagem digital e as pedagogias digitais. As principais áreas de competência são mostradas na figura abaixo (Redecker 2017

[8] Redecker, C. Quadro Europeu de Competência Digital para Educadores: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Serviço das Publicações da União Europeia, Luxemburgo, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

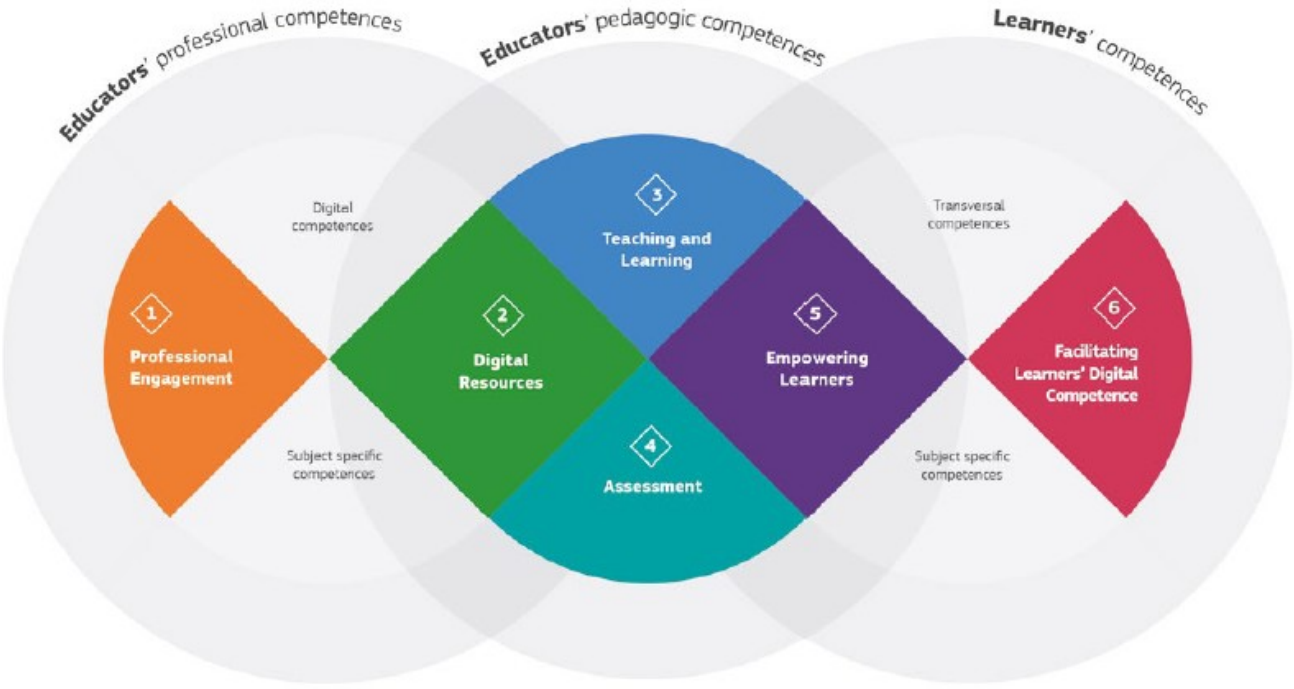
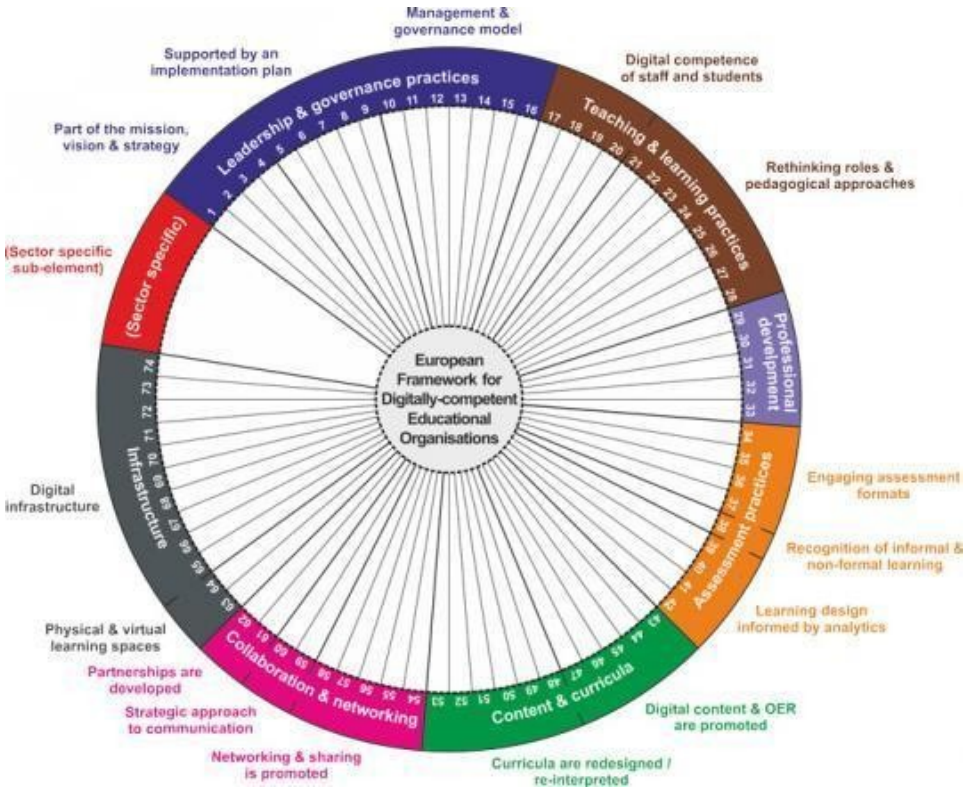


FIGURE 2: DIGCOMPEDU AREAS AND SCOPE

v. O Quadro DigCompOrg

Vários quadros e ferramentas de autoavaliação estão em utilização em vários países europeus, mas, até ao momento, não se fez qualquer tentativa para desenvolver uma abordagem pan-europeia para a capacidade digital organizacional. Um quadro de referência europeu que adote uma abordagem sistémica pode acrescentar valor ao promover transparência, comparabilidade e aprendizagem entre pares. O **quadro DigCompOrg** pode ser utilizado por organizações educacionais (ou seja, escolas primárias, secundárias e de EFP, assim como instituições de ensino superior) para orientar um processo de autorreflexão sobre o seu progresso rumo à integração abrangente e implementação efetiva de tecnologias digitais de aprendizagem.

Além disso, pode facilitar a transparência e a comparabilidade entre iniciativas relacionadas em toda a Europa e também pode desempenhar um papel na resolução da fragmentação e do desenvolvimento desigual nos Estados-Membros. O quadro DigCompOrg também pode ser utilizado como ferramenta de planeamento estratégico para os decisores políticos promoverem políticas abrangentes para a adoção efetiva de tecnologias de aprendizagem digital por organizações educacionais ao nível regional, nacional e europeu. Também pode ser utilizado como meio para chamar a atenção para a abordagem sistémica necessária para a utilização eficaz das tecnologias digitais de aprendizagem.



Os principais objetivos do DigCompOrg são:

- incentivar a autorreflexão e a autoavaliação nas organizações educacionais à medida que aprofundam progressivamente o seu envolvimento com a aprendizagem e as pedagogias digitais;
- capacitar os decisores políticos (a nível local, regional, nacional e internacional);

– conceber, implementar e avaliar programas, projetos e intervenções políticas para a integração de tecnologias digitais de aprendizagem em sistemas de E&F.

vi. SELFIE

A SELFIE for Work-based Learning (WBL - Aprendizagem Baseada no Trabalho) é uma ferramenta online gratuita que apoia escolas e empresas de Ensino e Formação Profissional (EFP) para aproveitar ao máximo as tecnologias digitais para ensino, aprendizagem e formação. A SELFIE WBL apoia escolas e empresas a adequarem-se à era digital. Desta forma, apoia a transição digital, uma das principais prioridades políticas da Comissão Europeia. Esta adaptação da SELFIE aos requisitos específicos da Aprendizagem Baseada no Trabalho é um passo necessário para **apoiar as escolas de EFP**.[9]

No total, cerca de **35,000 participantes** de cerca de **150 escolas de EFP** e **250 empresas** em França, Alemanha, Hungria, Polónia, Roménia, Geórgia, Montenegro, e Turquia estiveram envolvidos no piloto. Os resultados destes pilotos estão disponíveis para download [LINK para recursos].[10]

O Fórum Europeu de Ensino e Formação Técnica e Profissional (EfVET) e a Fundação Europeia de Formação (ETF) deram um apoio inestimável.

Voltar para o conteúdo ↑

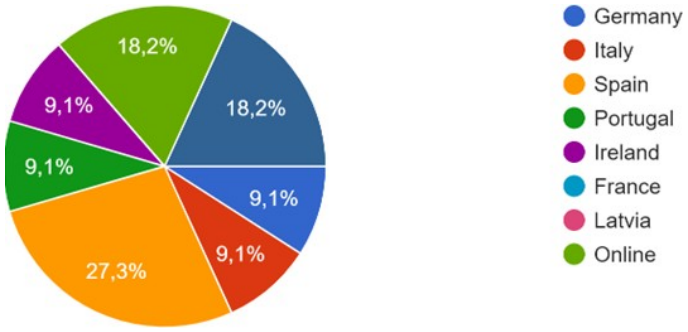
[9] SELFIE for work-based learning | Espaço Europeu da Educação (europa.eu)
[10] Recursos SELFIE | Espaço Europeu da Educação (europa.eu)

d) Orientações CYBER.EU.VET

O principal objetivo do projeto CYBER.EU.VET procura contribuir para o reforço da capacidade do EFP europeu para reconhecer e gerir ameaças à cibersegurança (por exemplo, ataques de phishing, botnets, fraudes financeiras e bancárias, fraudes de dados) num contexto histórico em que a formação online é cada vez mais utilizada.

Para tal, visa melhorar as competências e aptidões dos educadores do EFP na gestão de ameaças à cibersegurança, dado o seu papel central na transferência de conhecimentos de boas práticas e competências para os seus alunos, aumentando igualmente a sensibilização dos professores do EFP, alunos e as suas famílias, assim como a importância de reconhecer estes riscos diários, que podem ter um impacto económico e social em todos os cidadãos europeus. O projeto conta com uma circulação conjunta local, nacional e transnacional de capacidades e conhecimentos e um bom nível de acesso e usabilidade da informação digital.

8 Sessões Gamejam com 54 alunos e 15 formações específicas nacionais para formadores são organizados para debater os resultados da investigação, as ferramentas digitais partilhadas e as novas ferramentas criadas, trocando experiências e comentários para desenvolver uma espécie de "narrativa coletiva temática" preparatória para passar da exploração e análise à gestão e resolução de problemas digitais.



Estes eventos permitiram que os jovens trabalhassem em conjunto e mostrassem que também instituições que são percebidas como distantes do cidadão comum (ex. Comissão Europeia) oferecem oportunidades interessantes para a população jovem.

Uma **sessão de formação** é definida neste guia como como uma única sessão de formação que ocorre ao longo de um dia ou parte de um dia. Pode durar 30 minutos, uma hora ou até um dia inteiro. Uma sessão de formação pode incluir pausas ao longo do dia e abranger um ou mais tópicos. Uma sessão pode ser realizada numa sala de aulas, num pequeno grupo com uma única família, ou mesmo

individualmente. Para efeitos deste guia, um programa de formação é um conjunto de sessões de formação que completam um ciclo de formação. Por exemplo, uma agência pode oferecer um programa de formação de 8 semanas, uma vez por semana. O programa de formação poderia então ser reiniciada para um novo grupo de pessoas. (*Workshops and Courses, 2021*)

I. A Base de um Workshop: Conhecimentos, Competências e Atitudes

Este guia segue um quadro com vista à sensibilização dos alunos sobre as ameaças digitais, que se baseia nos conhecimentos, competências e aptidões. Da mesma forma, os supervisores do programa e os professores/formadores melhoram os seus conhecimentos, competências e atitudes para serem mais eficazes.

Conhecimentos, competências e atitudes são as bases de uma formação eficaz. Os formadores eficazes têm conhecimentos, competências e atitudes sobre a formação e os tópicos que ensinam, e os programas e sessões de formação que oferecem devem incluir conhecimentos, competências e atitudes para os participantes que estão focados no tópico e nos conteúdos.

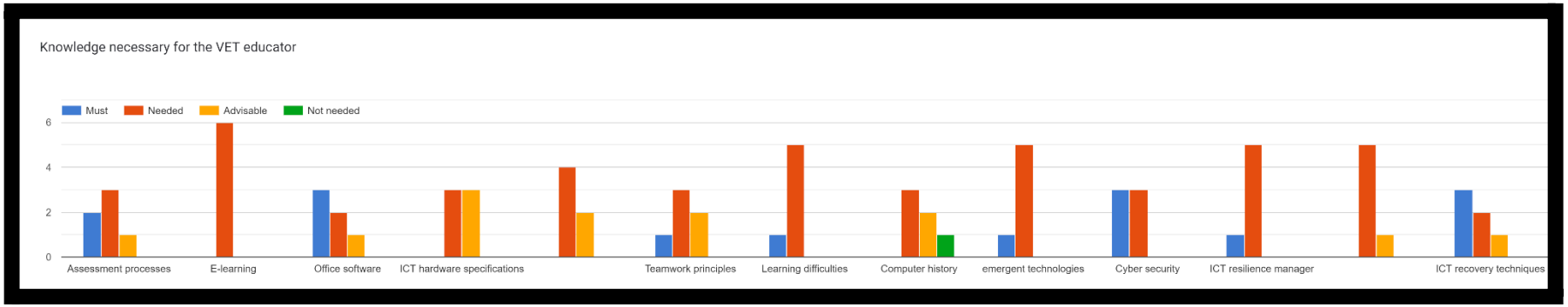
Pergunta para o próprio: A quem pode recorrer se tiver dúvidas sobre as normas e os conteúdos do programa como um novo profissional do EFP?

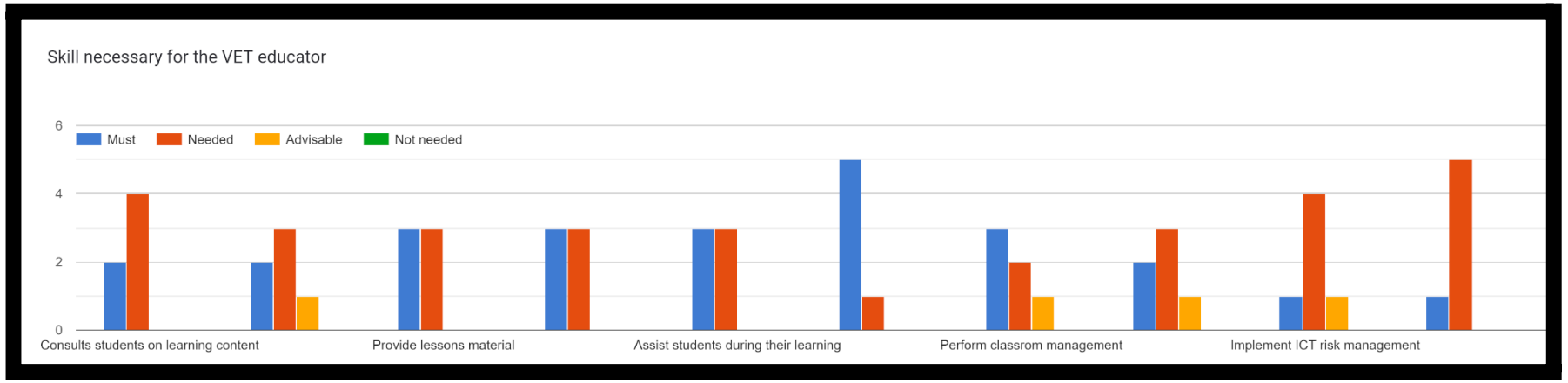
Os formadores devem ter um compreensão ampla dos conteúdos principais para responderem às perguntas que possam surgir. Se um profissional não souber a resposta a uma pergunta, é fundamental que o profissional afirme que não sabe a resposta, mas que analisará e voltará ao tema.

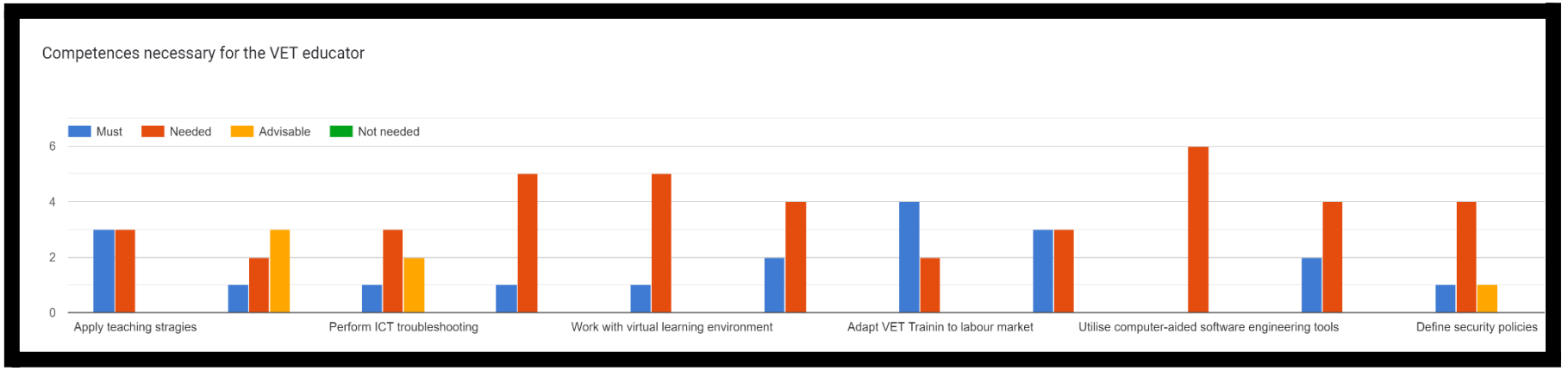
Os profissionais não devem dar informações falsas ou inventar respostas só para satisfazerem o bem-estar e compreensão dos participantes. É responsabilidade de um formador realizar investigação, encontrar respostas e acompanhar os participantes com vista a assegurar que estes estão a receber informações precisas.

Quer saber mais sobre o que um professor pode fazer quando lida com o assunto?

Apresentamos, a seguir, exemplos de conhecimentos, competências e atitudes adequados que um formador eficaz deve possuir de acordo com os parceiros do consórcio.







Co-funded by the
Erasmus+ Programme
of the European Union

Atividade: Como professor/formador, quais são alguns exemplos dos seus conhecimentos, competências e atitudes? Preencha os espaços em branco no quadro. Apresenta-se um exemplo.

Exemplos de conhecimentos	Exemplos de competências	Exemplos de atitudes
Estou familiarizado com a cibersegurança e as tecnologias emergentes.	Sou capaz de desenvolver materiais educativos digitais e adaptar o ensino ao grupo-alvo.	Sou apaixonado por tornar as sessões o mais eficazes possível para os nossos participantes e estou empenhado em fazê-lo.

- **Conhecimentos**: Resultado da assimilação da informação através da aprendizagem. O conhecimento é o corpo de factos, princípios, teorias e práticas relacionadas com uma área de estudo ou trabalho.

- **Competência**: Capacidade de aplicar os conhecimentos e utilizar o know-how para concluir tarefas e resolver problemas.

- **Aptidão**: Capacidade de aplicar os resultados da aprendizagem adequadamente num contexto definido (ensino, trabalho, desenvolvimento pessoal ou profissional. [11]

Voltar para o conteúdo ↑

[11] O Quadro Europeu de Qualificações para a Aprendizagem ao Longo da Vida (QEQ)

Co-funded by the Erasmus+ Programme of the European Union

II. O websiteCYBER.EU.VET

O consórcio do projeto criou desde a primeira etapa do projeto um website desenvolvido com tecnologias open-source (Wordpress) e uma abordagem modular, que pode permitir que novos parceiros de diferentes países adicionem e façam a gestão dos seus próprios conteúdos (uma vez aceites os termos das condições estabelecidas pelos parceiros do projeto). Plataformas digitais como a CYBER.EU.VET podem ser abertas de duas formas para promover a inovação e a geração de valor (Boudreau 2010).

É óbvio que as plataformas digitais e, neste caso específico, a plataforma concebida como Recurso Educacional Aberto, podem ser mais exploradas para atividades de acompanhamento. Este novo sistema permite relacionar o mundo físico tradicional com uma interface digital capaz de ligar e organizar a procura e oferta de uma ferramenta ou serviço num único espaço virtual.

Karhu, Gustafsson, and Lyytinen: *Exploiting and Defending Open Digital Platforms*
Information Systems Research, 2018, vol. 29, no. 2, pp. 479–497, © 2018 The Author(s)

Table 1. Two Forms of Platform Openness and Related Resources

Platform openness	Boundary resources	Shared resources	Actor who shares	Type of sharing	Platform owner's rationale
Access openness	API, app store	Complement, e.g., apps	Complementor	Shared for distribution	Generate network effects, and extract value from complementarities
Resource openness	Open-source license	Platform core, e.g., AOSP	Platform owner	Shared IPR	Strategic forfeiture of IPR while recovering costs from somewhere else

Estas plataformas criam redes que ligam pessoas e serviços ao longo do tempo.

A integridade da rede está relacionada não apenas com os fatores da infraestrutura de informação, a sua segurança e o fluxo de dados dentro da rede, mas também com as mudanças sociais e ambientais que interferem nos componentes humanos.

Por esse motivo, organizou-se uma campanha Multiplier Event para disseminar e divulgar as ferramentas tecnológicas e o manual CYBER.EUY.VET desenvolvidos.

Esta campanha teve igualmente o objetivo de aumentar a sensibilização dos professores e alunos do EFP e dos seus familiares, assim como sensibilizar para importância de reconhecer esses riscos diários, que podem ter um impacto económico e social em todos os cidadãos europeus.

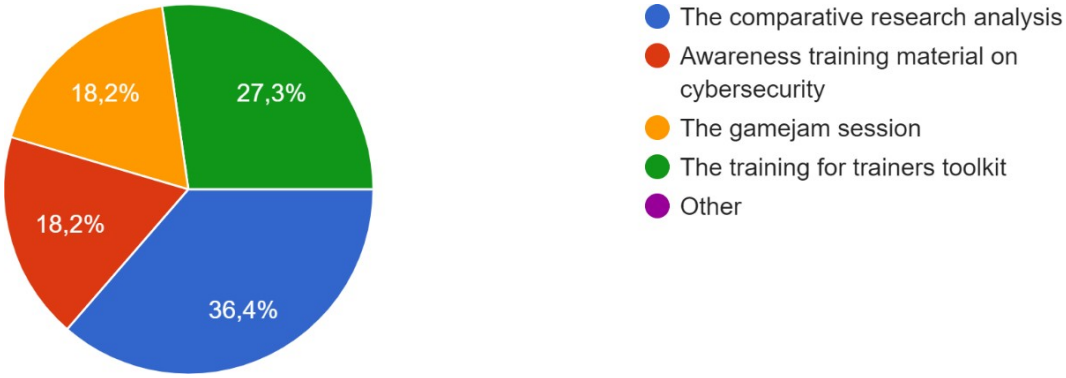
Sistemas de TIC que alavancam o "efeito de rede" emergente através da combinação de redes sociais online abertas, criação de conhecimento distribuído e dados de ambientes reais com vista a **sensibilizar para problemas e possíveis soluções que exigem esforços coletivos, possibilitando novas formas de inovação social.**

III. "Uma visão do profissional"

Os parceiros e profissionais que estiveram envolvidos no projeto CYBER.EU.VET afirmaram ter beneficiado os seus objetivos de investigação com uma melhor compreensão da perceção dos estudantes de cibersegurança no contexto local e europeu. Os intercâmbios entre partes interessadas tão diferentes entre si foram uma oportunidade para obter diferentes perspetivas e abordagens a questões partilhadas e aprender a traduzi-las para uma linguagem mais comum. Nas palavras do nosso parceiro: *"Foi muito benéfico aprender mais sobre o estado da arte atual no campo da cibersegurança e sobre as principais ciberameaças nos países parceiros. Também é interessante estar atento e poder acompanhar as tendências em termos de ciberataques que parecem ser muito semelhantes em cada país"*. 81,8% dos parceiros afirmaram que pretendem utilizar o material partilhado ou criado no âmbito do projeto CYBER.VET.EU no futuro, 36,4% localmente, 36,4% nacional e 27,3% ao nível internacional, durante as sessões de formação e oficinas, fóruns e, claro, redes sociais.

Os contextos dos países participantes no projeto são muito diferentes, embora como países europeus partilhem algumas semelhanças. A cibersegurança é muito variável, pois as ameaças são diferentes ao longo do tempo. Como tal, é interessante que os resultados obtidos sejam atualizados tanto pelos formadores como pelos investigadores para que sejam válidos no momento da sua utilização.

Significativo é o gráfico que mostra quais foram as ferramentas partilhadas mais úteis para os operadores dos diferentes serviços dos 8 parceiros do consórcio:



IV. Uma nota final

O manual CYBER.EU.VET foi concebido para ajudar os formadores do EFP e profissionais digitais com a utilização de ferramentas para cibersegurança, assim como instruções sobre como utilizar o material CYBER.EU.VET listado no Apêndice. O manual oferece sugestões sobre como organizar a formação, assim como recomendações operacionais para permitir que os profissionais forneçam aos alunos os conhecimentos e as ferramentas necessárias para reconhecerem ameaças à cibersegurança. Este e-book foi desenvolvido para professores do EFP, alunos do EFP, famílias de alunos e instituições de EFP a nível internacional ou local. Profissionais (ou assistentes sociais/gerentes) que dão formação e orientação, supervisores ou coordenadores de formação e quem dá orientação, como voluntários, estagiários, outro pessoal de apoio à reinstalação, outros prestadores de serviços e membros da comunidade, todos podem beneficiar. Uma maior sensibilização para os riscos causados por fraudes de dados, malware e outras ameaças à segurança online, a todos os níveis, desde a gestão da instituição de EFP às famílias do aluno, são passos fundamentais para defender os cidadãos da UE dos danos causados por ameaças à cibersegurança, num momento já caracterizado por uma crise histórica.

Este e-book contém várias sugestões que esperamos que levem os professores e profissionais do EFP do programa a repensarem os objetivos da sua formação e como podem melhorar a qualidade do ensino, desenvolvendo formas inovadoras de e-learning.

e) Apêndice

I. Glossário

I. GLOSSÁRIO

DADOS

uma sequência de um ou mais símbolos a que é atribuído um significado por ação(ões) específica(s) de interpretação (os dados não têm significado intrínseco). Os dados podem ser analisados ou utilizados num esforço para obter conhecimentos ou tomar decisões. Os dados digitais são representados com recurso ao sistema numérico binário de uns (1) e zeros (0) por oposição à sua representação analógica. [12]

COMUNICAÇÃO DIGITAL

Comunicação com recurso a tecnologia digital. Existem vários modos de comunicação, por exemplo, comunicação síncrona (comunicação em tempo real, por exemplo, com recurso ao Skype ou chat por vídeo ou Bluetooth) e assíncrona (comunicação simultânea não por exemplo, e-mail, sms) utilizando, por exemplo, modos um-para-um, um-para-muitos ou muitos-para-muitos.[13]

COMPETÊNCIA DIGITAL

A competência digital pode ser amplamente definida como a utilização confiante, crítica e criativa das TIC para atingir objetivos relacionados com trabalho, empregabilidade, aprendizagem, lazer, inclusão e/ou participação na sociedade.[14]

CONTEÚDOS DIGITAIS

Qualquer tipo de conteúdo que exista na forma de dados digitais codificados num formato legível por máquina e que possam ser criados, visualizados, distribuídos, modificados e armazenados com recurso a tecnologias digitais. Exemplos de conteúdos digitais incluem: páginas da web e websites, redes sociais, dados e bases de dados, áudio digital como mp3s e e-books, imagens digitais, vídeo

[12] Adaptado de: en.wikipedia.org/wiki/Data_(computing)
[13] Fonte: *Quadro DigComp* https://ec.europa.eu/jrc/digcomp
[14] *Ibidem*

digital, videojogos, programas de computador e software. Para o quadro DigCompEdu, os conteúdos digitais são divididos em recursos digitais e dados.[15]

AMBIENTE DIGITAL

um contexto, ou um "lugar", habilitado por tecnologia e dispositivos digitais, muitas vezes transmitidos pela internet, ou outros meios digitais, por exemplo, rede de telefonia móvel. Os registos e evidências da interação de um indivíduo com um ambiente digital constituem a sua pegada digital. No DigComp, o termo ambiente digital é utilizado como pano de fundo para ações digitais sem nomear uma tecnologia ou ferramenta específica.

SERVIÇO DIGITAL

??permite que um utilizador (cidadão, consumidor) crie, processe, armazene ou aceda a dados em formato digital e partilhe ou interaja com dados em formato digital carregados ou criados pelo mesmo ou por outros utilizadores desse serviço (Diretiva (UE) 2019/770).

TECNOLOGIA DIGITAL

Qualquer produto que possa ser utilizado para criar, visualizar, distribuir, modificar, armazenar, recuperar, transmitir e receber informações eletronicamente em formato digital. Por exemplo, computadores e dispositivos pessoais (por exemplo, desktop, laptop, netbook, computador tablet, smartphones, PDA com recursos de telemóvel, consolas de jogos, leitores de media, leitores de e-book), televisão digital, robôs.[16]

FERRAMENTAS DIGITAIS

Tecnologias digitais utilizadas para um determinado fim ou para a realização de uma função específica de, por exemplo, processamento de informações, comunicação, criação de conteúdos, segurança ou resolução de problemas.[17]

CONTEÚDOS EDUCATIVOS

Conteúdos (digitais) relevantes, de uma forma ou de outra, para o contexto educativo. Este termo é mais amplo do que "recurso educativo" na medida em que também compreende conteúdos marginais ao processo de instrução, por exemplo, comunicação com alunos, pais, colegas; conteúdos administrativos, etc.

RECURSOS EDUCATIVOS

Recursos (digitais ou não) concebidos e destinados a serem utilizados para fins educativos.[18]

LTERACIA DOS MEDIA

??refere-se a competências, conhecimentos e compreensão que permitem aos cidadãos utilizarem os media de forma eficaz e segura. Com vista a permitir que os cidadãos acedam a informações e utilizem, avaliem criticamente e criem conteúdos de media com responsabilidade e segurança, os cidadãos precisam de ter competências avançadas de literacia dos media. A literacia dos media não deve limitar-se a aprender sobre ferramentas e tecnologias, mas deve ter como objetivo equipar os cidadãos com as competências de pensamento crítico necessárias para exercer julgamento, analisar realidades complexas e reconhecer a diferença entre opinião e facto. [19]

RECURSOS EDUCATIVOS ABERTOS

---

[15] Redecker, C. Quadro Europeu de Competência Digital para Educadores: DigCompEdu. Punie, Y. (ed). EUR 28775 EN. Serviço das Publicações da União Europeia, Luxemburgo, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

[16] Adaptado da fonte: http://www.tutor2u.net/business/ict/intro_what_is_ict.htm

17Ibidem

18 Ibidem

[19] Fonte: Diretiva de Serviços de Comunicação Social Audiovisual da UE (2018)

Materiais de ensino, aprendizagem e investigação em qualquer meio, digital ou outro, que sejam do domínio público ou tenham sido lançados sob uma licença aberta que permita acesso, utilização, adaptação e redistribuição sem custos por outros, sem restrições ou com restrições. [20]

AUTOAVALIAÇÃO

A autoavaliação envolve a capacidade de ser um juiz realista do próprio desempenho. Os proponentes da autoavaliação sugerem que esta tem muitas vantagens, por exemplo; dá feedback oportuno e eficaz e permite que os alunos avaliem a sua própria aprendizagem rapidamente; permite que os instrutores compreendam e deem feedback rápido sobre a aprendizagem; promove a integridade académica através do autorrelato do aluno sobre o progresso da aprendizagem; promove as competências de prática reflexiva e automonitorização; desenvolve a aprendizagem autorregulada; aumenta a motivação dos alunos; melhora a satisfação de participar num ambiente de aprendizagem colaborativa; ajuda os alunos a desenvolverem uma série de competências pessoais e transferíveis para atender às expectativas dos futuros empregadores.[21]

INCLUSÃO SOCIAL O processo de melhorar as condições para que indivíduos e grupos participem na sociedade (pelo Banco Mundial). A inclusão social visa capacitar as pessoas pobres e marginalizadas a aproveitarem as oportunidades globais crescentes. Garante que as pessoas tenham voz nas decisões que afetam as suas vidas e que desfrutem de igualdade de acesso a mercados, serviços e espaços políticos, sociais e físicos.[22]

AMBIENTE ESTRUTURADO

onde os dados residem num campo fixo dentro de um registo ou ficheiro, por exemplo bases de dados relacionais e folhas de cálculo. A resposta/solução tecnológica refere-se à tentativa de utilizar a tecnologia (e/ou engenharia) para resolver um problema.

Referências

Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. (JRC Technical Notes No. JRC67075). IPTS.

Baron G.-L. et Baudé J. (1992), L'intégration de l'informatique dans l'enseignement et la formation des enseignants, Tours: EPI - INRP.

BIBB (2016), “Economy 4.0 needs Education 4.0”, Strengthening the media competence of training staff and trainees.

https://doi.org/10.13140/RG.2.2.18046.00322
Brodnik, A., Csizmadia, A., Futschek, G., Kralj, L., Lonati, V., Micheuz, P., & Monga, M. (2021). Programming for All: Un-derstanding the Nature of Programs. ArXiv:2111.04887 [Cs].

http://arxiv.org/abs/2111.04887

[20] Fonte: Definição da UNESCO
http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/open-educational-resources/what-are-open-educational-resources-oers/
[21] Fonte: *Centro para Excelgncia em Ensino da Universidade de Cornell*
http://www.cte.cornell.edu/
[22] Fonte: *Quadro DigComp* https://ec.europa.eu/jrc/digcomp

Buisán García,M.; Valdés, F. (2017), La industria Conectada 4.0., Revista de economía, No 898.

Bihouix P, Mauvilly, K (2016), Le Désastre de l'école numérique, Le Seuil.

Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: Carretero, S., Vuorikari, R., & Punie, Y. (2017). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Serviço das Publicações da União Europeia. https://data.europa.eu/doi/10.2760/38842

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf (consultado em 3 de julho de 2021).

EFVET (2021), Digital Balance: Balancing Digital Competences and Wellbeing.

Comissão Europeia. (2022). Translations of DigComp 2.0 in the European Skills, Competences and Occupations classification (ESCO). Serviço das Publicações da União Europeia. DOI:10.2767/316971

União Europeia. (2018). Recomendação do Concelho de 22 de maio de 2018 sobre as competências-chave para a aprendizagem ao longo da vida (ST/9009/2018/INIT).

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:O-J.C_.2018.189.01.0001.01.ENG
Ferrari, A. (2012). Digital competence in practce: An analysis of frameworks. Serviço das Publicações da União Europeia.

https://data.europa.eu/doi/10.2791/82116
Ferrari, A. (2013). DIGCOMP: A framework for developing and understanding digital competence in Europe. Serviço das Publicações. doi:10.2788/52966

Ferrari, A., Brecko, B., & Punie, Y. (2014). DIGCOMP: a Framework for Developing and Understanding DigitalCompetence in Europe. ELearning Papers, 38, 1–14.

Ferrari, A., Punie, Y., & Redecker, C. (2012). Understanding digital competence in the 21st century: An analysis of current frameworks. In EC-TEL 2012: 21st Century Learning for 21st Century Skills (pp. 79–92).

Governo da Letónia, (2020), Digital Transformation Guidelines 2021-2027.

Huismann, A. (2020), Vocational education and training for the future of work: Germany, Cedefop ReferNet thematic perspectives series.

Information Technology Security Incident Response Institution, (2021), CERT.LV Annual Report 2020.

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā.

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes.

Janssen, J., & Stoyanov, S. (2012). Online Consultation on Experts' Views on Digital Competence. Serviço das Publicações da União Europeia. https://publications.jrc.ec.europa.eu/repository/handle/JRC73694

Kampylis, P, Punie, Y & Devine, J 2015, Promoting effective digital-age learning: a European framework for digitally competent educational organisations, Serviço das Publicações da União Europeia, Luxemburgo

Relatório de Defesa Digital da Microsoft.
https://www.microsoft.com/de/security/business/security-intelligence-report

Ministério da Educação, Universidade e Investigação, Governo de Itália (2021), Innovare e potenziare le competenze digitali nella scuola, Memorando de Entendimento nº. 785 de 22 de janeiro de 2021

Ministério da Inovação Tecnológica e Transição Digital (2020), 2025 – Strategia per l'innovazione tecnologica e la digitalizzazione del Paese.

OCDE. (2014). Assessing problem-solving skills in PISA 2012. In PISA 2012 Results: Creative Problem Solving (Volume V): Students' Skills in Tackling Real-Life Problems. OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264208070-6-en

Vuorikari, R., Punie, Y., Carretero Gomez, S., & Van den Brande, L. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. Serviço das Publicações da União Europeia. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254

DISCLAIMER

É possível rastrear o documento através do seguinte código QR:

Voltar para o conteúdo ↑