YBER.EU.VET

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

CYBER.EU.VET

KA226 – Partnerships for Digital Education Readiness

Project N. 2020-1-DE02-KA226-C31C2976

Relatório de Consórcio

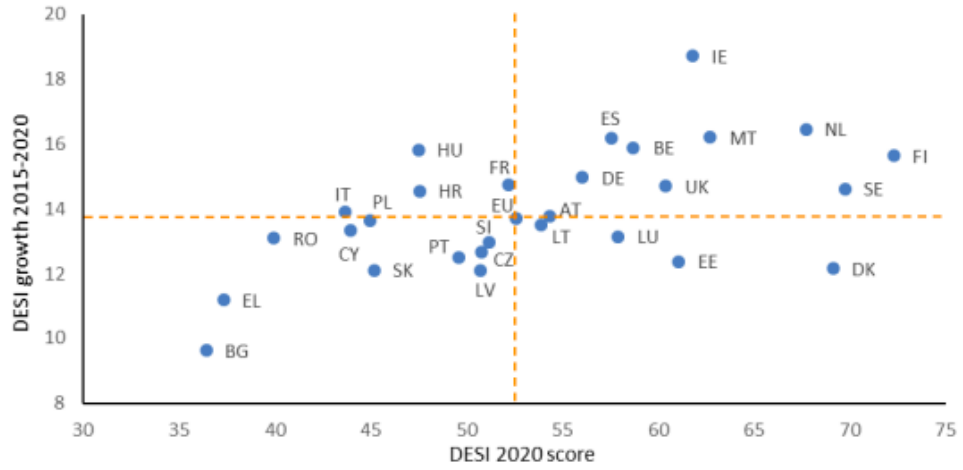
sobre principais desafios e melhores práticas de cibersegurança

Índice

Introdução

Como o mundo se está a tornar cada vez mais digitalizado, tornou-se mais importante que a prática deve ser combinada com as políticas. Existe um foco significativo nas políticas de alfabetização digital e política de segurança cibernética no contexto europeu, no entanto, existem menos exemplos de iniciativas que são vistas como cumprindo esses objetivos alinhados com as políticas desenvolvidas. Para observar cuidadosamente até que ponto as competências digitais e de segurança cibernética são um tópico central e divergente, é útil considerar o índice de economia e sociedade digital de 2020 (DESI).

Como parte de sua imagem geral, a DESI monitora o desempenho digital geral da Europa e mede o nível de competitividade digital nos países da UE. Ao fornecer informações sobre o status de digitalização em cada estado membro, ajuda a identificar áreas para investimento e ações adicionais. Em direção a um futuro digital adaptado às necessidades das pessoas e do seu respeito com os valores fundamentais da UE, a Comissão apresentou uma visão para a transformação digital "moldando o futuro digital da Europa" em fevereiro de 2020. O Relatório DESI 2020 avalia a economia e a sociedade digital no início de a pandemia usando dados de 2019.

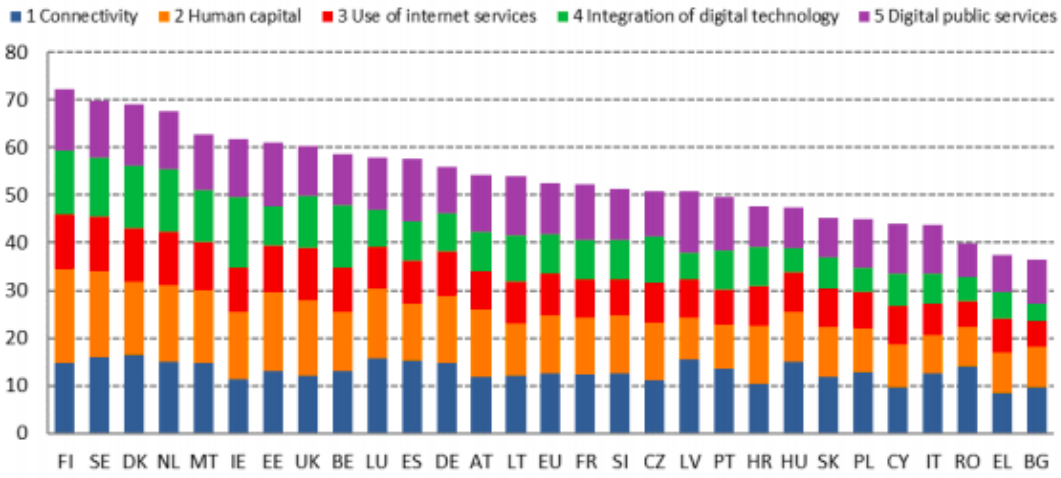


Source: DESI 2020, European Commission.

Especificamente, este índice investiga e reúne dados sobre:

- Conectividade: a disponibilidade de acesso rápido e confiável à Internet (incluindo conexões fixas e móveis) é vital na era atual da entrega on -line dos principais serviços sociais e econômicos;
- Capital humano: a espinha dorsal da sociedade digital são as habilidades digitais da população. Utilizadores de serviços digitais e pessoas com limitações no uso de sistemas móveis podem-se envolver em atividades básicas on-line;
- Uso da Internet: À medida que a pandemia progredia, mais e mais pessoas usavam a Internet. O confinamento generalizado resultou no acesso regular a redes sociais e plataformas de entretenimento, bem como em serviços de teletrabalho e comércio eletrónico;
- Integração da tecnologia digital: as empresas adotaram rapidamente novos acordos de trabalho para se adaptar às medidas do governo que reduziram a interação social;
- No meio das medidas de distanciamento social, é necessário continuar as atividades governamentais para garantir que os serviços públicos digitais forneçam benefícios. Serão necessários serviços públicos digitais robustos em todos os Estados-Membros para obter uma estratégia de saída bem-sucedida da pandemia atual.

Essa análise é útil ao considerar que os parceiros do consórcio estão em países membros que se diferenciam em termos de performances digitais e de segurança cibernética. De fato, três deles (em melhor classificação, Irlanda, Espanha e Alemanha) alcançam uma pontuação melhor do que a média, enquanto os outros quatro (França, Letónia, Portugal e Itália) têm desempenho inferior.



Source: DESI 2020, European Commission.

É importante referir que os resultados do DESI 2020 parecem não confirmar uma correspondência linear entre o PIB do país e a disseminação de habilidades digitais. De fato, a Espanha, por exemplo, classificada como a 5ª economia da UE, está classificada apenas como 10º no índice de economia e sociedade digital. Várias iniciativas foram recentemente introduzidas em alguns dos países que compõem o consórcio para melhorar a digitalização da economia e da sociedade. Como principal país da UE para a prontidão 5G, a Alemanha tomou várias medidas para promover a digitalização, incluindo iniciativas nas áreas de segurança de TI, supercomputação, IA e blockchain. Houve inúmeros esforços para facilitar a digitalização de empresas e serviços públicos na França, incluindo esforços para estabelecer um ecossistema para apoiar as startups de tecnologia. O governo italiano adotou 'Italia 2025' em dezembro de 2020, um plano de 5 anos que coloca inovação e digitalização no centro de um "processo de transformação radical e estrutural do país". Nos próximos anos, essas iniciativas - que exigem implementação sustentada ao longo do tempo e também provavelmente exigem investimentos - podem resultar no progresso desses estados membros no DESI.

Outro aspecto significativo, ao considerar o nível de habilidades digitais e de segurança cibernética, é o do impacto da pandemia covid-19 em relação a esses tópicos. Embora o vínculo

entre a emergência da saúde e o número de ataques cibernéticos não seja imediatamente claro para o público mais em geral, na realidade, o primeiro resultou no aumento nos últimos em cibercrimes com a exploração de novos eventos, tal como se tem visto recentemente em ataques na área da saúde. Com tantas empresas se mudando para novas estratégias digitais em 2020 (ou seja, trabalho remoto), elas inadvertidamente abriram uma série de novos vetores de ataque que os criminosos rapidamente exploraram. Entre outros, a ocorrência inesperada covid-19 foi usada para espalhar tentativas de malware: por exemplo, e-mails em nome da Organização Mundial da Saúde, indicando que o anexo inclui as informações mais recentes sobre a pandemia; Links para gráficos mostrando a propagação do vírus, cuja funcionalidade era roubar dados do utilizador; E-mails maliciosos para instituições de saúde sobre a entrega de equipamentos de proteção CoVID-19 e muitos outros.

Ao concluir este relatório de pesquisa do consórcio, utilizamos pesquisas, que consistiram em localizar e recolher dados, publicações, relatórios da UE, legislações nacionais e europeias, seguindo as referências fornecidas ao longo do relatório. Especificamente, o estudo explorou a questão da alfabetização digital e da segurança cibernética nos diferentes contextos nacionais, com foco no treinamento de professores veterinários. Além disso, este relatório de pesquisa do consórcio destaca alguns dos principais atores envolvidos no setor de segurança cibernética, incluindo os órgãos nacionais e a Agência da União Europeia para a segurança cibernética (ENISA), que coopera com os Estados-Membros e os órgãos da UE e auxilia a Europa na preparação para futuros desafios cibernéticos .

1. Pesquisa sobre as habilidades digitais dos educadores de ensino profissional

Alemanha:

- Relatório de dados VET (2019) elaborado pelo Instituto Federal Alemão de Educação e Formação Profissional (BIBB), incluiu “digitalização” entre as três tendências principais para ocupações de formação vocacional e ensino profissional em geral.
- Mais especificamente, o relatório afirmou que “a digitalização reforçará mudanças estruturais do mercado de trabalho”, indo para a necessidade de uma mudança nas capacidades de formação nos respectivos campos. Como consequência do futuro, o mercado de trabalho alemão e europeu terão uma necessidade particular de especialistas profissionais mais qualificados.
- Conforme descrito na Resolução da Conferência Permanente dos Ministros da Educação e Assuntos Culturais (2016-2017)-“Bildung em Dig Digitalen Welt” (Educação no mundo digital) - na área de educação profissional, a promoção do emprego - competências relacionadas no contexto do trabalho digital e processos de negócios são uma parte essencial da competência dos professores como ponto de partida para suas atividades didáticas.
- O Ministério Federal de Educação e Pesquisa (BMBF) e o Instituto Federal de Educação e Treinamento Profissional (BIBB) abordam desde 2015 questões em pesquisa, desenvolvimento e prática, relacionadas à transformação digital do mundo do trabalho e da educação profissional e Treinamento.

Irlanda:

- Uma das principais estratégias da Irlanda em relação às habilidades digitais dos educadores de ensino profissional é a estratégia digital nacional lançada em julho de 2013.
- A estratégia concentra-se no compromisso digital e destaca como a Irlanda pode beneficiar de uma sociedade digitalmente integrada.
- A estratégia define uma visão clara do avanço digital da Irlanda através da implementação de várias ações práticas para ajudar a aumentar o número de cidadãos e empresas envolvidas on -line por meio da indústria e da empresa, formação em cidadãos, escolas e educação.
- Em relação às competências digitais dos educadores de ensino profissional, as evidências continuam a destacar que há um aumento da divisão entre educadores que usam dispositivos digitais nas aulas como uma ferramenta de aprendizagem e aqueles que não o fazem.
- Muitos formadores declararam que acham que os dispositivos digitais podem "provocar distrações" aos alunos. No entanto, pelo contrário, muitos outros acreditam que dispositivos e aplicativos digitais nas atividades de aprendizagem podem capacitar os alunos e apoiá -los a envolverem-se em competências adequadas do século XXI, como pagar contas on-line/candidatar-se a empregos.

Portugal:

- O sistema nacional de qualificações reorganizou o ensino profissional num único sistema no qual os programas levam a uma certificação dupla. O ensino profissional para adultos é parte integrante do sistema de qualificação nacional, com programas de educação e formação para adultos e reconhecimento e validação do conhecimento anterior como elementos-chave.

- Portugal fez um progresso significativo em relação melhorias da educação, mas permanece menor que a média da UE. Embora menos de 2015 (73,7%), em 2019, a parcela de pessoas com nível baixo ou nenhuma qualificação digital foi de 50,2%, a mais alta da UE.

Itália:

- No campo da educação, as ações foram realizadas principalmente através da implementação do Plano Nacional da Escola Digital (Piano Nazionale Scuola Digitale-PNSD).
- Este é o documento de diretrizes do Ministério da Educação, Universidade e Pesquisa para o lançamento de uma estratégia geral de inovação para a escola italiana e para um novo posicionamento de seu sistema educacional na era digital.
- A maioria das ações para a formação de equipas da escola foi destinada a escolas primárias e secundárias, que representam a maioria das escolas na Itália, enquanto a falta de atenção foi dada ao setor de educação e treinamento profissional (EFP).
- Nesse sentido, os projetos foram implementados para os institutos de educação técnica pós-secundária e formaçãoprofissional (Istituti Tecnici Superiori - ITS), com um foco particular no fortalecimento das habilidades dos alunos.
- Por exemplo, em 2019, o projeto “ITS 4.0” envolveu mais de 1,170 alunos e cerca de 130 empresas parceiras em 106 projetos de inovação tecnológica com foco em tecnologias como impressão 3D, realidade virtual e big data.

Espanha:

- A agenda digital da Espanha (ADPE, Agenda Digital para Espanha) publicada em 2013, é o roteiro para cumprir os objetivos estabelecidos pela agenda digital para a Europa em 2015 e 2020, bem como a obtenção de objetivos específicos para o Desenvolvimento da economia e da sociedade digital na Espanha. É estruturado em seis objetivos principais e vários planos específicos. O sexto objetivo é promover a inclusão digital e a alfabetização

e o formação de novos profissionais de TIC. Entre suas medidas específicas, as seguintes medidas podem ser destacadas para os fins desta análise:

- Atualiza o catálogo nacional de qualificações profissionais em termos de habilidades e formação de TIC e inclui esta atualização nas ofertas de formação que credenciam as qualificações profissionais;
- Maximiza a eficiência na gestão e alocação de fundos de formação contínua nas TIC, tanto para trabalhadores do setor público e privado, com atenção especial ao uso de plataformas de formação virtual on-line;
- Atribui parte dos recursos disponíveis para o CVET à aquisição e atualização de competências digitais de profissionais de TIC;
- Reajusta a formação vocacional relacionado às TIC, incluindo, entre outras ações, cursos de especialização na educação;
- Promove uma melhoria na oferta da Universidade destinada a treinar profissionais de TIC através de sua adaptação às necessidades do mercado, contemplando novos perfis profissionais no campo das TIC e aumentando a eficiência do sistema.

França:

- Verificando que o ritmo de formação no uso de TIC nas universidades francesas que o oferecem, pode-se ver que não há políticas claras e sustentadas para a formação de formadores sobre o uso de TIC/E. Cerca de 58% relatam apenas uma sessão de formação por ano, em comparação com 7,4% ao mês e 0,5% por semana.
- A Agência Nacional Francesa para a Segurança dos Sistemas de Informação (ANSSI) observou um aumento muito rápido no nível da ameaça cibernética na França. Continuando uma trajetória iniciada em 2019, o número de ataques cibernéticos explodiu e o número de vítimas multiplicou-se por 4 num ano.

- As estatísticas mostram que a densidade da formação TI varia de uma região para outra. Existem várias razões para isso as mais significativas, sem dúvida, estão ligadas às instituições académicas e aos seus governos.
- Mais estudos para ver a diferença podem ser realizados posteriormente pelos escritórios regionais ou pelos CNFs, de acordo com suas próprias políticas de educação digital local ou regional.

Letónia:

- Embora atualmente haja falta de pesquisa e dados na Letónia sobre segurança cibernética e outras habilidades digitais dos educadores no ensino profissional e em outras instituições educacionais, é óbvio que a transição para o ensino à distância, devido às crises Covid-19, provou ser um grande desafio para muitos professores.
- Em relação às estratégias nacionais, os documentos de planeamento do novo período de orçamento (2021-2027) destacam os seguintes aspectos:
    - O desenvolvimento de competências digitais no setor educacional (Diretrizes de transformação digital 2021-2027) - prevê o desenvolvimento de competências digitais de educadores e chefes de instituições educacionais, desenvolvimento e uso de competências digitais no processo educacional, bem como apoio para apoio a o desenvolvimento de competências digitais de adultos empregados;
    - O desenvolvimento de competências digitais está incluído no Programa de Desenvolvimento de Competências Profissionais para Educadores (Diretrizes de Desenvolvimento da Educação 2021-2027). Em 2020, o Ministério da Educação e a Ciência da República da Letónia estabeleceu a melhoria da competência digital dos educadores como uma meta prioritária de competência profissional, alocando para esse fim financiamento adicional (0,5 milhões de euros);
    - A necessidade de aumentar a consciencialização dos alunos e educadores sobre segurança da informação, proteção à privacidade e uso de serviços eletrónicos

confiáveis (estratégia de segurança cibernética 2019-2022, área de ações "conscientização, educação e pesquisa");

- O desenvolvimento das competências digitais da Sociedade Geral (Diretrizes de Desenvolvimento da Educação 2021-2027, Diretrizes de Transformação Digital 2021-2027), pois as competências digitais agora são equiparadas à alfabetização e numeracia em termos de sua importância e, pelo menos, no nível básico que são necessárias para Todos, independentemente da área de atividade (habilidades digitais = habilidades transversais). As medidas devem ser tomadas para educar a população sobre as competências digitais básicas, a alfabetização da rede e a alfabetização da informação, que inclui todo o conjunto de competências básicas, incluindo competências cibernéticas;

A atenção que foi dada ao índice DESI acima mencionado na introdução deste relatório de pesquisa é justificado da precisão com que descreve o estado da arte e o caráter divergente de acordo com os diferentes países europeus. Essa precisão também é confirmada pelos relatórios nacionais únicos sobre as habilidades digitais dos educadores de veterinário.

Acreditamos que é particularmente benéfico comparar os dois extremos do consórcio, a fim de entender como diferentes graus nas habilidades digitais afetam a população nacional e os educadores veterinários especificamente. Em primeiro lugar, consideraremos a Irlanda, classificada como 6ª na classificação DESI.

De acordo com o Irish Central Statistics Office (CSO), a partir de 2018, 89 % das famílias têm Acesso à Internet em casa. Além disso, mais de 30 % de todos os dados da UE estão alojados na Irlanda, pois muitas das maiores empresas de tecnologia do mundo têm sua sede localizada na Europa. Quando ambas as estatísticas são acopladas, não é preciso dizer, garantir que a Irlanda seja um país que esteja pronto para segurança cibernética é de importância crucial. Ao longo

deste relatório nacional, será feita referência à legislação-chave que existe na Irlanda em relação à alfabetização digital e cibersegurança. À medida que o mundo continua a adaptar-se a 'viver com covid-19', é necessário garantir que o cenário anti-cibercrime e os modelos de melhores práticas continuem a influenciar políticas e práticas.

Uma das principais estratégias da Irlanda em relação às habilidades digitais é a estratégia digital nacional lançada em julho de 2013. A estratégia concentra-se no compromisso digital e destaca como a Irlanda pode beneficiar de uma sociedade digitalmente integrada. A estratégia estabelece uma visão clara do avanço digital da Irlanda através da implementação de várias ações práticas para ajudar a aumentar o número de cidadãos e empresas envolvidas on -line por meio da indústria e da empresa, treinamento em cidadãos, escolas e educação. Em 2021, a Ministra da Educação Norma Foley anunciou o desenvolvimento de uma nova estratégia digital para escolas de nível primário. A estratégia deve se concentrar principalmente no uso da tecnologia digital na educação e aprimorar o conhecimento através da incorporação de tecnologia no futuro. Dentro do espaço do ensino superior na Irlanda, um dos desenvolvimentos mais notáveis é um roteiro para o aprendizado digital no ensino superior: 2015 - 2017, desenvolvido para apoiar uma “abordagem coordenada e multinível para promover a alfabetização digital, habilidades e confiança entre os alunos em todos os níveis de educação ”.

Em relação à educação e formações adicionais, foi estabelecido um departamento relativamente novo de ensino superior e superior, pesquisa, inovação e ciência. Dentro da estratégia de três anos de departamentos, uma área-chave de foco é sobre as competências digitais nas quais eles pretendem implementar uma nova estratégia de 10 anos para melhorar a alfabetização, a numeracia e as competências digitais. Além disso, eles se concentram em reformar a formação de competências e investir na promoção de competências digitais. Em relação às competências digitais dos educadores de VET, as evidências continuam destacando

que há um aumento da divisão entre educadores que usam dispositivos digitais nas suas aulas como uma ferramenta de aprendizado e aqueles que não o fazem.

Muitos educadores declararam que acham que os dispositivos digitais podem "provocar distrações" entre os alunos. No entanto, pelo contrário, muitos educadores acreditam que dispositivos e aplicativos digitais nas atividades de aprendizagem podem capacitar os alunos e apoiá -los a se envolver em habilidades para a vida do século XXI, como pagar contas on -line/se candidatar a empregos. Uma estratégia final entre governos que vale a pena notar da perspectiva irlandesa é a iniciativa Future Future Jobs Ireland de 2018, que enfatiza uma filosofia de aprendizado ao longo da vida. Dentro de seus cinco temas -chave, o segundo se concentra na "inovação e tecnologia, incluindo a preparação para a transição para a economia digital". A estratégia é central para as discussões sobre a necessidade de mais pesquisas e investimentos na área de literacias digitais.

Um entendimento e apreciação tão partilhados dos meios digitais confirmam a Irlanda como um país líder em termos de integração da tecnologia digital. Entre outros, uma integração resulta como uma das principais questões para o contexto italiano.
Na Itália, menos da metade da população possui habilidades digitais básicas e a porcentagem de especialistas em TIC, que constitui apenas 1% dos graduados italianos, ainda está abaixo da média da UE, embora tenha aumentado nos últimos anos. Além disso, os dados da Pesquisa Internacional de Ensino e Aprendizagem da OCDE (2013), consulte a Itália em primeiro lugar para as necessidades de treinamento de TIC de seus professores. Pelo menos 36% dos professores italianos declararam que não estavam suficientemente preparados para o ensino digital, em comparação com uma média da OCDE de 17%, mostrando que é necessário treinamento específico.

Nos últimos anos, em termos de resposta à política, a Itália incorporou medidas sobre competências digitais em várias estratégias setoriais. No campo da educação, as ações foram realizadas principalmente através da implementação do Plano Nacional da Escola Digital (Piano Nazionale Scuola Digitale - PNSD), que é o documento de diretrizes do Ministério da Educação, Universidade e Pesquisa para o lançamento de um geral Estratégia de inovação para a escola italiana e para um novo posicionamento de seu sistema educacional na era digital. É um pilar fundamental de La Buona Scuola (Lei 107/2015), uma visão operacional que reflete a posição do governo em relação aos desafios de inovação mais importantes do sistema público e, no centro desta visão, existem os Inovação do sistema escolar e as oportunidades da educação digital. As áreas de intervenção identificadas pelo PNSD são: acesso, espaços e ambientes de ensino, administração digital, identidade digital, habilidades para alunos, empreendedorismo e mercado de trabalho, conteúdo digital, formação de pessoal. Em relação a esse último ponto, o PNSD argumenta que a formação de professores deve ser centrado na inovação educacional, levando em consideração as tecnologias digitais como suporte para a implementação de novos paradigmas educacionais e o planejamento operacional das atividades. Os objetivos desta ação são:

- fortalecer a preparação da equipe no campo das competências digitais, atingindo toda a comunidade escolar;
- Promover o vínculo entre inovação educacional e tecnologias digitais;
- Desenvolver padrões eficazes, sustentáveis e contínuos ao longo do tempo para a formação em inovação educacional;
- Fortalecer a formação em inovação educacional em todos os níveis (inicial, intermédio, profissional).
- Para promover a formação dos professores sobre assuntos de TI, um memorando de entendimento foi assinado com órgãos de treinamento e recursos financeiros foram fornecidos para facilitar a participação nos cursos, como:
    - Memorando de entendimento no. 785 de 22 de janeiro de 2021 entre o Ministério da Educação e o Cisco "inovando e aprimorando as habilidades digitais na escola" e o programa de formação "conectado e seguro".

- Memorando de entendimento no. 4 de 28 de outubro de 2020 entre o Ministério da Educação e a S.O.S. O Telefono Azzurro Onlus para realizar atividades educacionais e de formação conjuntas para promover a educação para a cidadania digital e o uso consciente de tecnologias digitais, redes sociais e cursos de formação para professores.

Até agora, a maioria das ações para o treinamento da equipe da escola tem como objetivo as escolas primárias e secundárias, que representam a maioria das escolas da Itália, enquanto a falta de atenção foi dada ao setor de educação e treinamento profissional (VET). Nesse sentido, os projetos foram implementados para os institutos de educação técnica e de treinamento profissional pós -secundários (Istituti Tecnici Superiori - ITS), com um foco particular no fortalecimento das habilidades dos alunos. Por exemplo, em 2019, o projeto “ITS 4.0” envolveu mais de 1,170 seus alunos e cerca de 130 empresas parceiras em 106 projetos de inovação tecnológica com foco em tecnologias como impressão 3D, realidade virtual e big data.

Outra ferramenta que contribuirá para a aquisição de habilidades digitais está incluída no Plano Nacional de Recuperação e Resiliência (Piano Nazionale Di Ripresa E Resilienza - Pnrr), que faz parte do programa da próxima geração da UE, um pacote de 750 bilhões de euros, onde quase a metade dos quais é composto por subsídios, acordados pela União Europeia em resposta à crise pandêmica. O PNRR promoverá o desenvolvimento de habilidades digitais da equipe da escola para incentivar uma abordagem acessível, inclusiva e inteligente da educação digital. O principal objetivo é a criação de um ecossistema de habilidades digitais, capaz de acelerar a transformação digital da organização escolar e os processos de aprendizado e ensino, de acordo com a estrutura de referência européia para habilidades digitais DigComp 2.1 (para estudantes) e DigCompedu (para professores). A implementação dessa linha de ação é garantida pelo Ministério da Educação e envolverá cerca de 650.000 pessoas, incluindo professores e funcionários da escola e mais de 8.000 instituições educacionais. O governo pretende fortalecer

a educação profissional, em particular o sistema de treinamento profissional (ITS) e a educação STEM, com uma forte prioridade na igualdade de gênero.

Os contextos acima mencionados representam dois contextos nacionais diferentes. Para ter uma indicação mais próxima da estrutura europeia em geral, pode ser útil analisar o cenário de competências digitais na França, um país que na escala DESI está muito próximo e imediatamente após a média européia.

A Agência Nacional Francesa para a Segurança dos Sistemas de Informação (ANSSI) observou um aumento muito rápido no nível da ameaça cibernética na França. Continuando uma trajetória iniciada em 2019, o número de ataques cibernéticos explodiu: o número de vítimas multiplicou-se por 4 num ano. Isso é particularmente preocupante, especialmente num contexto em que qualquer ataque cibernético provavelmente terá um impacto exacerbado devido à crise da pandemia. A falta de consciência dos riscos cibernéticos, a falta de controlo sobre os sistemas de informação, a falha em respeitar as medidas de higiene do computador, a escassez de especialistas em segurança cibernética e, até certo ponto, o aumento da superfície de ataque devido ao uso generalizado de teletrabalho, são todas as fraquezas exploradas pelos cibercriminosos. As campanhas de ataque que atingiram a França em 2020 interromperam com sucesso muitas empresas e causaram perdas financeiras significativas. O uso macivo de serviços digitais de terceiros, geralmente menos seguros, é uma prática generalizada que os invasores não deixam de explorar. As estatísticas mostram que a densidade de formação em TI varia de uma região francesa para outra. Há várias razões para isso. Entre eles, o mais significativo está sem dúvida relacionado às instituições académicas e dos seus governos. Estudos adicionais para ver a diferença podem ser realizados posteriormente pelos escritórios regionais ou pelo CNFS de acordo com suas próprias políticas de educação digital local ou regional. As estatísticas de formação mostram que as necessidades temáticas que foram objeto de oficinas de formação

também variam de uma região para outra. A frequência temática nesse sentido também depende de fatores endógenos relacionados à demanda e oferta de acordo com as necessidades e níveis de avanço nos campos das TIC/E e ODL dos parceiros locais.

2.Pesquisa sobre os principais problemas de segurança digital em países terceiros

Alemanha:

- Analisar o contexto alemão específico e desenhar uma análise de necessidades, é especialmente significativa a revisão do barómetro digital de 2020, uma pesquisa on-line representativa de cidadãos particulares sobre segurança cibernética, conduzida em conjunto pelo BSI e pela Comissão de Prevenção ao Crime do Estado e Federal Alemão.
- Nos últimos anos, no contexto alemão e europeu, o cibercrime tem sido a principal causa de ataques cibernéticos recentes. O relatório BSI de 2020 confirmou fuga de dados e vulnerabilidades críticas encontradas em produtos de software e hardware. Esta pesquisa também notou um aumento de crimes cibernéticos em massa visando cidadãos particulares, empresas comerciais e outras instituições usando malware.
- A vulnerabilidade mais comum explorada por malware é uma vulnerabilidade no sistema host. No caso de software ou produtos de hardware, as vulnerabilidades podem ser encontradas em gateways, como aqueles que operam entre escritórios ou redes de produção, ou podem ser causados por erro humano na engenharia social.
- Esse grau de digitalização não deixa de ter seus riscos e perigos. Um em cada quatro entrevistados relatou que haviam sido vítimas de crimes cibernéticos no ano passado. A taxa geral de crime cibernética em 2020 permanece constante. Compras on-line e acesso de terceiros a contas on-line são os tipos mais comuns de fraude que afetam as vítimas (44%) e (30%), respectivamente.

Apesar das análises, dois terços dos entrevistados expressaram um desejo de mais informações sobre a prevenção de roubo de dados (66%). Os conselhos procurados com mais frequência

consistem em dicas práticas, como maneiras de garantir senhas seguras para várias contas on-line (59%), seguidas de conselhos sobre qual software é mais adequado para proteger contas on-line (52%) e conselhos sobre os prós e contras de gestores de senha (49%).

Irlanda:

- As ameaças de segurança cibernética na Irlanda continuam a aumentar, com o mais recente ataque de segurança cibernética ocorrendo em 2021 no Executivo do Serviço de Saúde da Irlanda (HSE), que tem e continua tendo efeitos elevadores negativos no sistema de saúde da Irlanda.
- A Irlanda abriga mais de 30% dos dados da UE devido ao número de centros de segurança cibernética com sua sede no país. Embora isso ofereça muitas oportunidades, também resulta em aumento do nível de ameaça de crimes cibernéticos. Como a Irlanda é uma democracia liberal aberta, é vista como particularmente vulnerável aos chamados ataques do tipo "hack e fuga de dados".
- A segunda estratégia nacional de segurança cibernética da Irlanda 2019 - 2024 foi lançada em uma tentativa de aumentar a prontidão para segurança cibernética do país. Os principais objetivos da estratégia são:
    - Garantir a prontidão da segurança cibernética da Irlanda e responder e gerenciar incidentes de segurança cibernética, incluindo os relativos à segurança nacional,
    - Para proteger e gerenciar qualquer interrupção de serviços que envolvam infraestrutura nacional crítica de ataques cibernéticos,
    - Para crescer e desenvolver ainda mais o setor de segurança cibernética na Irlanda e estar pronto para cibernética,
    - Para implementar a melhor tecnologia e medidas disponíveis internacionalmente em empresas irlandesas,

- Para aumentar a conscientização e desenvolver conjuntos de habilidades entre organizações e indivíduos particulares em torno da segurança cibernética.

- Em 2018, um plano de ação para segurança on-line foi lançado e contém vinte e cinco ações sob cinco objetivos principais centrados na legislação de ofensas criminais em relação ao crime cibernético, removendo material ilegal e prejudicial e impulsionando a segurança on-line.

Portugal:

- Os principais tópicos de segurança digital, em curso e desenvolvidos como recomendações pelo Centro Nacional de Cibersegurança, a serem garantidos em formações são:
  - o nível base
    - Identificação da exposição da sua infraestrutura e aplicações escolares no ambiente on-line e adote medidas de mitigação de riscos (estruturais e comportamentais);
    - Identificar e mitigar vulnerabilidades;
    - Identificar informações pessoais na Internet que podem ser usadas em um ataque;
    - Adquirir um conjunto de comportamentos apropriados no uso do ciberespaço;
  - Níveis intermediários e avançados:
    - Ambientes técnicos de programação de segurança
    - Engenharia Social
    - Explorando fontes de dados abertos
    - Redes sem fio
    - Criptografia e senhas

Itália:

- O problema de segurança mais difundido nos últimos três anos na Itália é o Phishing, indicado por 48% dos gerentes italianos, contra 36% dos gerentes europeus. Além disso, 28% dos gerentes italianos têm problemas relacionados ao acesso e identidade (de acordo com a porcentagem europeia), seguidos pelo problema dos malware baseado em engenharia social (24%).
- Além disso, apenas 42% das pessoas entre 16 e 74 anos têm competências digitais básicas e a percentagem de licenciados em indivíduos com TI e TIC é muito baixa em comparação aos dados europeus.
- O governo aborda as competências digitais em “Italia 2025”, uma estratégia de cinco anos para inovação e digitalização lançada em 2019. Em particular, a estratégia inclui “República Digital”, uma iniciativa promovida e coordenada pelo Ministério da Inovação e Digitalização tecnológica.
- A iniciativa visa construir uma aliança entre organizações públicas e privadas e cidadãos e convidá-los a tomar medidas concretas para promover competências digitais. Concentra-se em três linhas de ação:
    - Aumentar competências digitais básicas;
    - Promoção de Upskilling e Rescatilling of the Workforce;
    - Desenvolvendo habilidades em tecnologias emergentes.
    - Um avanço adicional será dado com "Italia Digitale 2026", que define cinco objetivos ambiciosos a serem alcançados nos próximos anos:
- Disseminar a identidade digital, garantindo que seja usada por 70% da população;
    - Ponte a lacuna de competências digitais, com pelo menos 70% da população sendo digitalmente capaz;
    - Traga cerca de 75% dos PAs italianos para usar serviços em nuvem;
    - Atingir pelo menos 80% dos serviços públicos essenciais fornecidos on-line;

- Alcance, em colaboração com o Mise, 100% das famílias e empresas italianas com redes Ultrabroadband.

Espanha:

- A estratégia de ativação espanhola para o emprego 2017-20 pretende consolidar a recuperação económica, promovendo programas e recursos de segurança cibernética para as instituições do VET enfrentarem os desafios do presente e futuro mercado de trabalho, derivando da globalização e digitalização. Estabelece as medidas a serem executadas, tanto no nível estadual quanto na regional, pelos Serviços de Emprego Público (PESS);
- Em termos quantitativos, um dos objetivos é a formação em competências digitais de pelo menos 225.000 jovens: 75% em competências básicas e 25% em competências digitais avançadas, o que representa 40% e 38%, respectivamente, da população jovem abaixo de 30 anos .
    - Suporte inicial a projetos baseados em tecnologia para mulheres jovens, fornecendo a um consultor para aconselhar esses empreendedores sobre seu plano de negócios e oferecer serviços de monitoramento;
    - Ações de formação específicas para mulheres jovens de áreas rurais em tecnologias de TIC e novos setores futuros, aproveitando as possibilidades de novas tecnologias e com treinadores e tutores, incluindo ensino on -line;
    - Promoção do empreendedorismo, trabalho por conta própria e novas oportunidades de emprego oferecidas pela economia digital e pelas diferentes fórmulas da economia social e da economia das plataformas digitais, dentro das políticas de ativação do emprego;
    - Melhorando a visibilidade das melhores práticas desenvolvidas para entender quais são os principais tópicos de segurança digital.

- Programa Operacional Nacional de Emprego da Juventude (orçamento de 39 milhões de euros). Como exemplo, o programa inclui um caminho de formação sobre transformação digital para emprego.
- O projeto, implementado pela EOI com a parceria do Google, visa melhorar a empregabilidade dos jovens que abandonaram a escola desde tenra idade, perderam o emprego ou têm dificuldades para encontrar seu primeiro emprego.

França:

- Os Ministros do Ensino Superior do mundo de língua francesa reuniram-se em 5 de junho de 2015 em Paris na Iniciativa Conjunta da França, na OIF (Organização Internacional de la Francophonie) e a AUF (Agence Universitaire de la Francophonie) para examinar o estado de e perspectivas para o desenvolvimento digital do espaço universitário e profissional de língua francesa.
- O principal objetivo deste trabalho foi contribuir para a elaboração de uma estratégia francófona para a formação de formadores no campo da educação digital e avaliar as necessidades e expectativas de treinamento dos grupos -alvo em questão e depois determinar o que é necessário para alcançar essas necessidades e expectativas, principalmente em termos de serviços, conteúdo e competências.
- De acordo com o estudo “Étude sur l'dentification des besoins em formação tic/e dans les paga francófonos du sud, 2016”, as necessidades dos professores são fortemente marcados por uma tendência unânime para a formação em TIC/E e Capacitação de Capacitação relacionado à educação digital (80,4%).
- Os riscos digitais estão muito presentes nas representações de jovens professores, que transmitem facilmente o discurso da rede. Os três riscos que os professores acham que

enfrentam mais pessoalmente são técnicos (66,20%), éticos e legais (55,80%) e informativos (54,70%).

Letónia:

- De acordo com a estratégia nacional de segurança cibernética 2019-202215, o ciberespaço da Letónia continua enfrentando ameaças em larga escala - phishing, extorsion e malware, tenta invadir os sistemas, redes e sites, ataques de perda de serviço (DOS) em sistemas de informação crítica bem como campanhas fraudulentas de e-mail e engenharia social para recuperar dados pessoais ou de autenticação para desacreditar uma pessoa, empresa ou instituição específica ou para cometer crimes.
- Tanto na Europa quanto na Letónia, os seguintes incidentes tornaram-se tópicos - tentativas de extorsão em dinheiro destinadas principalmente a instituições financeiras ou empresas do setor privado (os invasores realizaram uma série de ataques de teste, ameaçando suspender a operação de sites da empresa ou outros recursos por meio de ataques de ataques de até 2 TB/s).
- No 2021, fraude, malware e vulnerabilidades continuam sendo ativos - contas roubadas do WhatsApp através de códigos de ativação que solicitados por contas hackeadas da lista de contatos da pessoa; Uma nova onda de e-mails de chantagem ameaçam distribuir material comprometedor, se o utilizador de email não fará um resgate.
- O ano 2020 com suas mudanças globais demonstraram que, para os formadores do ensino profissional e de outras instituições educacionais, é importante ter um aumento de conhecimentos/habilidades no trabalho remoto seguro ao organizar aulas on-line e usar ferramentas digitais (e-mails, whatsapp, aprender plataforma, etc.), bem como estar ciente dos golpes e fraudes tópicos, especialmente nas redes sociais, para aumentar a consciencialização de seus alunos e estudantes.

Embora o vínculo entre a pandemia covid-19 e o ponto de ataques cibernéticos não seja imediatamente claro para o público mais em geral, na realidade, o primeiro resultou em um aumento no segundo. Os cibercriminosos são muito flexíveis quando se trata de explorar novos eventos, como vimos com a recente emergência de saúde. Com tantas empresas a mudarem para novas estratégias digitais este ano (ou seja, trabalho remoto), elas inadvertidamente abriram-se para uma série de novos vetores de ataque que os criminosos foram rápidos em explorar.

Os escritórios nacionais oferecem uma perspectiva multifacetada sobre os principais problemas digitais e de segurança cibernética. À medida que o ensino à distância se torna o novo normal, os cibercriminosos estão encontrando novas maneiras de alavancar técnicas como phishing, ransomware, engenharia social e muito mais para lançar seus ataques. Aqui estão alguns dos riscos mais críticos encontrados.

1. Acesso remoto seguro

À medida que o ensino à distância assume o ensino físico, os alunos e os professores precisam acessar as ferramentas de aprendizado on-line localizadas principalmente na nuvem, ou seja, aplicativos de compartilhamento de arquivos, e-mails, aplicativos, e às vezes precisam acessar recursos na rede escolar remotamente. Se o acesso remoto não estiver protegido, os hackers poderão penetrar no sistema e assumir o controle de toda a rede.

2. Acesso a dados confidenciais

As instituições educacionais contêm um tesouro de dados confidenciais que podem ser vendidos na Dark Web. Os dados pessoais de estudantes, professores, ex-alunos e funcionários administrativos, bem como dados sensíveis relacionados à pesquisa e propriedade intelectual de uma escola, podem ser um verdadeiro tesouro para um hacker vender ou resgatar. Portanto,

é essencial implementar o acesso baseado em identidade, permitindo que os usuários autorizados acessem apenas os recursos necessários para fazer seu trabalho.

3. Malware

A mudança para o ensino à distância significa que muitos dispositivos ligados à rede escolar são BYOD (traga seu próprio dispositivo). É difícil saber se os dispositivos e aplicativos utilizados são atualizados corretamente com patches e se o próprio antivírus está atualizado. A menos que esses dispositivos remotos se conectem por meio de uma VPN, você precisa garantir que eles estejam seguros antes que possam acessar recursos na rede de treinamento. É importante implementar recursos avançados de proteção da Web que podem identificar e bloquear as mais recentes ameaças da Web.

4. Phishing

Os ataques de engenharia social e phishing são grandes riscos de segurança cibernética para centros de treinamento francês. Treinadores e professores ou funcionários que são enganados a clicar em links maliciosos podem dar ao cibercriminal acesso à rede da escola e aos recursos valiosos. A melhor maneira de combater os ataques de engenharia social e phishing é através da consciencialização e formação do utilizador. Treinar e testar os utilizadores com ataques simulados ajudará a criar uma cultura positiva de conciencialização sobre segurança e torná-los-á menos vulneráveis a vários ataques on-line.

5. Fraude

Em relação à fraude, o ano de 2020 foi muito intenso, incluindo ataques de engenharia social. Entre as tentativas de fraude mais ativas foram campanhas de extorsão, onde os hackers alegaram ter invadido o dispositivo de um utilizador e obteve material comprometedor para o qual um resgate foi definido; Concursos fraudulentos em nome das marcas conhecidas, oferecendo-se para ganhar os smartphones mais recentes ou outros preços valiosos.

Uma nova tendência foi observada e-mails de extorsão com a ameaça de fuga de dados. Em muitas ocasiões, as empresas foram direcionadas. Anúncios enganosos nas redes sociais usando os nomes de pessoas famosas sem seu conhecimento, convidou os utilizadores da Internet a investir em criptomoeda. Os golpistas também fizeram telefonemas e tentaram convencer as pessoas a investir. Em certos casos, foram observadas tentativas fraudulentas repetidas, onde as vítimas de fraude financeira receberam ajuda para recuperar seus recursos perdidos.

Esquemas falsos telefónicos - falsificando os números de telefone de diferentes instituições de crédito e fingindo ser representantes bancários, os atacantes, usando o pouco conhecimento do público sobre métodos adicionais de autenticação, realizaram fraudes sobre recursos financeiros de vários milhares de pessoas. A adaptação dos hackers à necessidade de iniciar o trabalho remoto, considerando as necessidades das empresas para mudar rapidamente para uma condição de trabalho remoto e implementação da circulação dos documentos eletrónicos, os hackers usaram a situação para publicidade. Vários financeiros da empresa receberam e-mails em nome do diretor ou de outro funcionário para fazer um pagamento urgente ou alterar a conta da folha de pagamento.

A interferência na correspondência comercial de empresas, comprometendo os e-mails das empresas ou seus parceiros de colaboração, permitiu que os invasores escolhessem um momento adequado para enviar uma fatura de uma conta com uma conta alterada.

Muitos utilizadores da Internet eram alvos de mensagens fraudulentas com links de atalho (EJ.UZ), usados para mascarar o destino real do link, em nome das instituições estatais sobre o estado de emergência e a situação epidemiológica no país.

Lojas on-line falsas foram observadas durante a temporada de férias em anúncios de redes sociais e devido às restrições Covid-19 que forçaram as empresas a vender seus produtos on-line.

Pode ser útil usar alguns dados relatados pelos relatórios nacionais. Por exemplo, em França, os riscos digitais estão muito presentes nas representações de jovens professores, que transmitem facilmente o discurso das redes. Os três riscos que os professores acham que enfrentam mais pessoalmente são técnicos (66,20%), éticos e legais (55,80%) e informativos (54,70%). Os riscos psico-social, cognitivos e socioeconómicos parecem preocupá-los menos. Existe uma discrepância sistemática entre as representações dos riscos para si mesmas em comparação com os dos alunos. De fato, os três riscos que os professores acham que seus alunos enfrentam são psico-social (69,95%), informativos (70,75%) e técnicos (62,80%). Os professores, portanto, sentem a mesma vulnerabilidade que seus alunos em relação aos riscos técnicos, mas consideram seus alunos mais expostos a problemas relacionados a assédio ou informação falsa em particular. A amplificação dos riscos para os alunos pode ser explicada pelo fato de que os professores os consideram muito vulneráveis. Uma professora descreveu as seus alunos da quarta classe como muito vulneráveis, bastante ingénuos, não necessariamente cientes do perigo potencial das redes.

O Relatório do Escritório Federal de Segurança da Informação (BSI) da Alemanha observou que várias campanhas exploraram a confusão e o medo criados pelo Covid-19, incluindo campanhas de malware, phishing e fraude. Além disso, o BSI disse que esses eventos podem ter aumentado as chances de sucesso para tais ataques por causa dos medos, preocupações e inseguranças associadas a esses eventos. Nos últimos anos, na paisagem alemã e européia, o cibercrime tem sido a principal causa de ataques cibernéticos recentes. Para analisar o contexto alemão específico e desenhar uma análise de necessidades, é especialmente significativa a revisão do barômetro digital de 2020, uma pesquisa on -line representativa de cidadãos particulares sobre segurança cibernética, conduzida em conjunto pelo BSI e pela Comissão de Prevenção ao Crime do Estado e Federal Alemão. A transição digital está moldando ativamente nossas vidas cotidianas de compras on-line de vestuário (como braçadeiras de rastreamento de fitness, relógios inteligentes ou óculos inteligentes), novos esquemas de pagamento e identificação.

No entanto, esse grau de digitalização não deixa de ter seus riscos e perigos. Um em cada quatro entrevistados relatou que haviam sido vítimas de crimes cibernéticos no ano passado. A taxa geral de crime cibernética em 2020 permanece constante. Compras on-line e acesso de terceiros a contas on-line são os tipos mais comuns de fraude que afetam as vítimas (44%) e (30%), respectivamente. A maioria dos entrevistados da pesquisa estava familiarizada com as recentes recomendações de segurança cibernética sobre a prevenção do crime cibernético. Essas recomendações geralmente são seguidas apenas quando faz sentido para a pessoa fazê-lo (41%) ou que acabou de aprender sobre um conselho específico (39%). Pesquisas mostram que as pessoas que já foram vítimas várias vezes têm maior probabilidade de prestar atenção apenas quando surge um problema (33%), mesmo que já estivessem cientes disso. Eventualmente, apesar das descobertas, dois terços dos entrevistados expressaram um desejo de mais informações sobre a prevenção de roubo de dados (66%). Os conselhos procurados com mais frequência consistem em dicas práticas, como maneiras de garantir senhas seguras para várias contas on-line (59%), seguidas de conselhos sobre qual software é mais adequado para proteger contas on-line (52%) e conselhos sobre os prós e contras de gerentes de senha (49%).

Eventualmente, outra perspectiva significativa é oferecida pela Irlanda e as ameaças de segurança cibernética ocorreram em 2021. Um ataque maciço e coordenado começou em maio de 2021, interrompeu o serviço de saúde e os sistemas de computador em todo o país, roubou dados pessoais de uma alta percentagem de pacientes e continua a exigir um resgate pelo retorno dos dados. Em resposta, o Executivo do Serviço de Saúde (HSE) teve que fechar os sistemas de TI do Hospital and Health Service para proteger contra outros dados roubados. Muitos serviços foram interrompidos e as informações pessoais e médicas foram roubadas. No entanto, deve-se notar que não há evidências para apoiar a aquisição de que outros golpes envolvendo as informações das pessoas ocorreram. A Irlanda abriga mais de 30% dos dados da UE devido ao número de centros de segurança cibernética com sua sede no país. Embora isso ofereça muitas oportunidades, também resulta em um aumento no nível de ameaça de crimes

cibernéticos. Como a Irlanda é uma democracia liberal aberta, é vista como particularmente vulnerável aos chamados ataques do tipo "hack e vazamento". Geralmente, esses ataques são vistos como politicamente motivados e estão centrados em desinformação e "notícias falsas" usadas como uma tentativa de desestabilizar o estado.

Muitos envolvidos no setor de segurança cibernética estão pedindo maior investimento em órgãos governamentais, como o Centro Nacional de CiberSegurança (NCSC) na Irlanda. Outras ameaças/riscos que continuam a prevalecer são os riscos representados para a infraestrutura nacional crítica (CNI), sistemas e dados do setor público que foram descritos brevemente nos parágrafos anteriores. Novos problemas que começam a surgir são aqueles conectados à implantação das tecnologias 5G. Embora isso dê origem a novas tecnologias e serviços, a segurança cibernética precisa estar na vanguarda de pensar, pois muitos países começam a se adaptar.

Fora de uma perspectiva nacional e comercial, os crimes de segurança cibernética continuam a ocorrer diariamente em pessoas comuns. Eles geralmente não são relatados à aplicação da lei, com apenas cinco por cento dos crimes cibernéticos supostamente relatados à polícia na Irlanda em 2019. Além disso, um relatório de 2019 encomendado pela Microsoft na Irlanda descobre que os funcionários ainda são vistos como o 'link fraco' na segurança Sistema devido à falta de formação de segurança, má gestão de palavras-passe, ao uso de dispositivos pessoais com dados relacionados ao trabalho e possíveis violações do regulamento geral de proteção de dados da UE.

3. Melhores práticas de programas e recursos de cibersegurança para instituições de ensino na União Europeia e em cada país parceiro

Conforme especificado na Introdução, o projeto Cyber.eu.vet envolve um consórcio multifacetado e diversificado. Em relação às competências digitais e de cibersegurança, os países parceiros do consórcio apresentam diferentes graus de eficácia, conforme perfeitamente descrito pelo índice DESI.

A análise académica e a avaliação de boas práticas foram parte integrante do trabalho de pesquisa realizado em nível nacional por cada parceiro no Consórcio do Projeto. Esta pesquisa teve como orientação comum uma análise de necessidade dos problemas de ensino a nível local e nacional. Ao realizar este trabalho, os sete parceiros nacionais compartilharam algumas dificuldades relacionadas à busca de iniciativas de formação e cibersegurança, projetadas especificamente para professores de ensino vocacional. Embora isso tenha dificultado essa tarefa, também mostrou ainda mais claramente a importância e a necessidade de desenvolver projetos nessa área, razão pela qual há uma importância deste espírito extremamente inovador do projeto Cyber.eu.vet. Aqui está uma coleção das boas práticas mais relevantes encontradas por cada parceiro.

3.1 Alemanha – Iniciativa VET 4.0

O VET 4.0 é uma iniciativa global, desenvolvida em colaboração pelo Ministério Federal de Educação e Pesquisa (BMBF) e pelo Instituto Federal de Educação e Formação Profissional (BIBB) a partir de 2016, que reuniu uma ampla gama de projetos em três pilares principais. O pilar 2 desta iniciativa abrangente (que ainda está em andamento) é completamente dedicada à "competência digital de alfabetização/media" e tem como objetivo definir competências digitais, que devem ser consideradas como um requisito de entrada e como uma competência

importante entre as ocupações no ensino vocacional (para aprendizes, professores e formadores). Programas de financiamento para equipar melhor os centros de formação e apoiar pequenas e médias empresas (PMEs), tendo em vista a digitalização, complementam essa abordagem de promover a competência digitais no ensino vocacional. Através do programa de digitalização üBS especial (71), o BMBF e o BIBB estão ajudando a acelerar a digitalização de processos na formação de aprendizes no contexto do 'VET 4.0'. O programa especial consiste em duas linhas de financiamento:

1) O financiamento é fornecido para comprar equipamentos digitais selecionados (dispositivos digitais, máquinas, sistemas e software, como tecnologias domésticas inteligentes, 21 robôs industriais, impressoras 3D e mídia digital de ensino e aprendizagem, como tablets e telas sensíveis ao toque), a fim de modernizar a formação de aprendizes, especialmente para aqueles formados pelas PME;
2) O programa também financia 8 projetos piloto em centros de competência que identificam os impactos da digitalização nos perfis de atividade profissional e determinam requisitos e conseqüências resultantes disso para a qualificação de pessoal qualificado e pessoal de treinamento. Em uma segunda etapa, eles desenvolvem conceitos inovadores de ensino e aprendizagem para o veterinário 4.0 e os disseminam como multiplicadores. O objetivo é garantir que os resultados sejam transferíveis e que exista uma ampla gama de aplicações.

A seguir, alguns exemplos dos projetos piloto mencionados acima:

- “Media digital no Ensino Vocacional” que terminará em 2022 e que é composto por vários subprogramas com diferentes prioridades de financiamento estão financiando projetos de formação digital nacional que desenvolvem novos cenários de aprendizagem e cursos de formação inicial e continuada modernos que promovem a aquisição de competência digital ;

- "Iniciativa de qualificação Digital Change - Q 4.0", que, de 2018, está a financiar o desenvolvimento e o teste de conceitos adicionais de formação de formadores de ensino profissional na empresa. O projeto consiste em dois subprojetos: 1) Seminários Mika (media e competência de TI para o pessoal de formação) para promover a competência pedagógica básica digital, o desenvolvimento e o teste de módulos de educação continuada para fortalecer a competência digital básica e as TI do pessoal de formação; 2) Q 4.0 Rede com o objetivo de adaptar o processo de formação à mudança digital, levando também em consideração as diferenças regionais e específicas do setor. Nos dois projetos, o resultado final pode ser um protótipo de uma oferta de seminário testada que poderia ser disponibilizada para ensino profissional em todo o país;
- "Digitalização II" desde 2018 para identificar estratégias para projetar processos de formação que usam o potencial digital para apoiar o ensino bem-sucedido, tanto para indivíduos quanto para grupos.

3.2 França - Internet Sans Crainte

(Como há uma falta de boas práticas de campo de ensino profissional neste país específico, este estudo de caso foi selecionado como uma prática que atende às restrições necessárias, mas não diz respeito especificamente ao setor do ensino profissional).

Tendo por base os constantes casos de cyberbullying, dependência da Internet, encontros perigosos na web e suas consequências para estudantes muito jovens, tornou-se necessário chamar a atenção de todos para os direitos e limites do comportamento on-line e, acima de tudo, apresentar a Internet como uma ferramenta para enriquecimento e entretenimento livre de perigo. Criado em 2000, pioneiro em pedagogia digital e especialista em comunicação

pública jovem, a Tralalere é um dos principais produtores de programas educacionais do digital: desenhos animados para produções multimedia, jogos sérios, aplicativos móveis, e-books etc. Aumentando a consciencialização sobre os riscos na internet: www.internetsanscrainnte.fr.

Desenvolvido pela Tralalere desde 2008, a "Internet sans Crainte" é o programa nacional para ajudar os jovens a obter melhor controlo sobre a sua vida digital. Em termos concretos, a "Internet sans Crainte" oferece cem recursos gratuitos ou mais para ajudar professores, educadores e pais a apoiar jovens de 6 a 18 anos em direção a um uso responsável de tecnologia digital. A "Internet sans Crainte" também oferece conselhos e conhecimentos sobre como apoiar os jovens em sua educação digital através de arquivos temáticos. Tralalere e "Internet sans Crainte" também coordenam a Internet mais segura da França, Programa Nacional e Europeu para a proteção de menores na Internet, juntamente com a linha líquida Ecoute (E15 Enfance) e o ponto de contato. Nessa vertente, a "Internet sans Crainte" organiza o Dia da Internet mais seguro na França, um dia mundial para aumentar a consciencialização entre os jovens para usar melhor a Internet. Este programa é apoiado pela Comissão Europeia como parte da rede INOPE/INSAFE, que inclui 38 países.

BENEFICIÁRIOS

"Internet sans Crainte" oferece os recursos digitais durante todo o ano adaptados a diferentes públicos, incluindo:

- Mediadores educacionais (professores, animadores, bibliotecários, etc.);
- pais e famílias;
- Instituições e associações.

3.3 Irlanda - Cybersafe Kids

(Como existem boas práticas do campo do ensino vocacional neste país específico, foi selecionada uma prática que atenda às restrições necessárias, mas não diz respeito especificamente ao setor do ensino).

A CyberSafe Kids começou como projeto em 2015 e agora tornou-se uma instituição de caridade reconhecida e financiada por vários fundos filantrópicos irlandeses, como os fundos da Irlanda. A CyberSafe Kids oferece vários programas de formação focados na cibersegurança em escolas de todo o país da Irlanda. A visão do CyberSafe Kids é para um mundo onde as crianças estão usando a tecnologia de maneira segura, positiva e bem-sucedida. As principais partes interessadas da CyberSafe Kids são as escolas de toda a Irlanda (estudantes, professores, diretores e responsáveis), universidades de investigação em parceria, financiadores da instituição de caridade e a equipa envolvida na entrega dos programas. O principal objetivo da instituição de caridade é avançar, promover e fornecer educação e formação a crianças, pais e professores da comunidade para garantir uma navegação segura e responsável do mundo on-line. Em relação ao impacto, até o momento, o CyberSafe Kids alcançou 24.000 crianças entre 8 e 13 anos por meio de seus programas de escolas. Só em 2020, os programas entraram em contato com 5.986 crianças e 1.554 pais em 56 escolas na Irlanda. Além disso, foi distribuída uma pesquisa on-line anónima, que reuniu dados de 3.764 crianças de 8 a 12 anos em relação ao uso on-line. De acordo com o Relatório dos Diretores (2019), as principais áreas de impacto incluíram o seguinte:

- A entrega de um programa educacional e o lançamento de um projeto de medição de mudança de comportamento em parceria com a Universidade de Dublin e o Comité de Crianças e Pessoas Jovens (CYPSC);

- Realização de uma forte campanha de "Dia da Internet segura";
- Lançamento de conteúdo e recursos on-line direcionados aos pais de crianças mais novas (de 2 a 10 anos). Nos anos anteriores, o material foi publicado para crianças mais velhas;
- Desenvolvimento de uma série de políticas 'Asks' que visam impactar a política de país abrangente sobre cibersegurança.

3.4 Espanha – SPACE: Competências para profissionais da escola contra eventos de cyberbullying

Enquadramento

A difusão e o uso generalizado de novas tecnologias estão ligados ao fenómeno do cyberbullying. Em 2009, na Europa, aproximadamente 18% dos jovens europeus de 13 a 19 anos foram intimidados/assediados/perseguidos pela Internet e via telemóveis, as taxas atuais variaram de 10% a 52%. O Parlamento Europeu destaca que o cyberbullying aumentou entre as crianças de 11 a 16 anos de 7% em 2010, para 12% em 2014.

Necessidades dos grupos-alvo

O espaço do projeto responde às necessidades de formação dos professores da escola, a fim de os fazer adquirir competências para prevenir/contrastar o cyberbullying. De facto, apesar dos Estados-Membros da UE lançarem muitas iniciativas e projetos para prevenir e combater o cyberbullying, parece estar a crescer: como é um novo fenómeno, falta um sistema orgânico de conhecimento, competências e ações educacionais estruturadas, garantindo que os professores adquiram o Conhecimento na sua dinâmica, o controlo das tecnologias digitais para um uso seguro da Web e as competências para planear a ação de prevenção, informação e formação.

Objetivos

Muitos recursos e conteúdos sobre o cyberbullying foram desenvolvidos por escolas e instituições; No entanto, eram iniciativas isoladas, não armazenadas num único local na web e, portanto, não foram valorizadas. O Space adotou esse desafio e desenvolveu um MOOC - Curso Open Online gratuito - sobre cyberbullying para professores e uma biblioteca digital pública multilíngua de recursos de educação aberta sobre cyberbullying. Projetos principais:

- Mapear e descrever as competências necessárias para prevenir e detetar cyberbullying;
- Desenvolver uma biblioteca digital de OER no cyberbullying, com recursos avançados de pesquisa;
- Desenvolver um MOOC para professores de escolas sobre cyberbullying, usando o OER desenvolvido;
- Para potenciaar e melhorar os professores envolvidos, em competência digital, saber, cibersegurança, risco da Web e ética na Internet;
- Apoiar professores que adquirem as competências para intervir no caso de cyberbullying na escola e planear, realizar atividades de informação e formação com alunos.

Participantes

O principal grupo-alvo envolvido no projeto é representado pelos professores da escola (níveis de Proced2 e ISCED3). Grupos-alvo indiretos eram gestores escolares e funcionários; estudantes; pais; autoridades escolares e decisores. 139 Professores estavam envolvidos no estudo MOOC e 300 participaram dos eventos multiplicadores organizados nos países parceiros. A biblioteca digital pública recebeu mais de 8.000 visitas durante o ciclo de vida do projeto.

Atividades

O projeto durou 24 meses, durante os quais ocorreram as seguintes atividades:

- Realização de um mapa de competências e um modelo MOOC;
- Design e desenvolvimento de uma biblioteca digital on-line sobre cyberbullying;
- Recuperação, catalogação e identificação do OER no cyberbullying e implementação desses recursos na biblioteca digital;
- Configurar e personalizar uma plataforma CMS para suportar o MOOC;
- Projeto, desenvolvimento e teste de um MOOC multilíngua em cyberbullying;
- Criação de um kit de ferramentas com indicações, diretrizes e recomendações sobre o sistema e ferramentas espaciais;
- Realização de 10 eventos multiplicadores nos países parceiros e em uma conferência final;
- Realização de 4 reuniões de consórcio;
- Disseminação através da criação de um site, folhetos, apresentações e participação como repórter convidado para a Didacta Fair em Florença, artigos em revistas e jornais.

Impacto

O projeto produziu um impacto positivo, promovendo a consciencialização sobre o cyberbullying, um maior conhecimento de sua dinâmica e métodos de prevenção e deteção e desenvolveu um conjunto multidimensional de conhecimento e competências no grupo de professores europeus envolvidos. Professores e organizações envolvidas nos testes adquiriram competências para prevenir e detetar cyberbullying, competências digitais especializadas em cibersegurança, riscos da Web e ética na Internet, desenvolveram competências estratégicas e competências metodológicas-didáticas, melhorando o profissional de ensino, os quais ficaram mais disponíveis e mais eficazes a realizar informações e atividades de formação aos seus alunos para impedir o cyberbullying.

3.5 Letónia – Programa “Improvement of Teachers' Digital Competence in the Form of E-Environment for the Use of Educational Technologies”

Objetivo

O objetivo do programa é melhorar a competência digital dos educadores - ensinar sobre tecnologias e ferramentas que ajudarão os educadores a organizar o seu processo de trabalho com mais eficiência. O programa é implementado desde 2014 pelo Ministério da Educação e Ciência da República da Letónia.

Beneficiários

O conteúdo dos cursos em 2020 foi projetado para:

- equipas de gestão de instituições educacionais;
- Educadores de escolas de formação profissional (VET) e de educação geral;
- Professores da escola primária;
- Professores pré-escolares;
- Professores de vários assuntos (matemática, idioma letão, ciência dos computadores, engenharia, design e tecnologia, física, química e biologia).

Descrição

Em 2020, o Ministério da Educação e Ciência estabeleceu a melhoria da competência digital dos educadores como uma meta prioritária de competência profissional, alocando financiamento adicional. O programa oferece um curso gratuito para educadores com diferentes níveis de conhecimento representando vários assuntos (campo de especialização).

Os implementadores dos cursos desenvolveram tarefas detalhadas de aprendizagem, atraíram líderes de grupo - consultores para garantir um regime de formação favorável para os educadores. O conteúdo dos cursos é projetado de acordo com os requisitos do ambiente moderno de aprendizado.

Resultados Alcançados.

4339 Educadores participaram cursos longos (com a possibilidade de trabalhar como professor de ciência da computação)

e cursos curtos de desenvolvimento de competências profissionais (2014-2020).

Inovação

A abordagem inovadora dificulta a organização do processo - cada participante do curso pode aprender o conteúdo num ritmo e tempo adequado a cada um. Durante o curso, são analisadas tecnologias e ferramentas que podem ser usadas no processo de estudo, a fim de promover a colaboração e simplificar a organização do processo de trabalho do processo de estudo/educadores.

3.6 Portugal

Apesar de algumas iniciativas ad-hoc, não foram identificadas ações de formação na área de cibersegurança de ensino profissional. Apenas vários cursos de ensino superior, pós-graduações ou de natureza empresarial foram identificados no mercado; portanto, a formação em cibersegurança para o ensino profissional deve ser uma prioridade fundamental para sustentar o futuro mais cibernético do país, ou seja, capaz de garantir a segurança pessoal e empresarial.

O Centro Nacional de CiberSegurança, com a missão de promover o compartilhamento de conhecimento e uma cultura nacional de segurança cibernética, desenvolveu o programa de consciencialização e formação em cibersegurança “Cidadão Ciberseguro”, através da qual se destina a massificar a formação e consciencialização dos cidadãos e funcionários das organizações para os perigos de uso desinformado do ciberespaço, realizando ações para aumentar a consciencialização e formações em cibersegurança em diferentes partes do país, de norte a sul, passando pelas ilhas, com o apoio de parceiros, mas nada direcionado às instituições de ensino profissional.

3.7 Italy - Docenti connessi e sicuri (Professores ligados e seguros)

Enquadramento

O programa tem o objetivo geral realizar ações destinadas a inovar e fortalecer as competências digitais nas escolas. Especificamente, o programa visa melhorar as competências e conhecimentos dos professores sobre novas experiências de ensino digital integradas, o funcionamento e os benefícios da Internet das coisas e a importância da cibersegurança. O programa é promovido sob o novo memorando de entendimento entre o Ministério da Educação (Itália) e a Cisco.

Grupos-Alvo

Os beneficiários do programa são professores de escolas italianas de qualquer escolaridade.

Atividades

O programa de formação oferecido pela Cisco aos professores consiste em três webinars aos quais três cursos adicionais de maior detalhe são possíveis de realizar. A participação em todo o programa é totalmente gratuita.

1. Um webinar mundial digital online “Pai e novas experiências de ensino digital integrado” desenvolvido pela Cisco ou parceiros da Cisco e curso on-line “se conecte”. Tempo estimado para concluir: 30 horas. Visão geral do curso: O curso ensina a desenvolver conhecimento digital básico. A estrutura particularmente interativa do curso cria um ambiente facilmente acessível para um público que se aproxima do mundo digital pela primeira vez.

2. Cidadãos digitais conscientes: webinar “Smart City e Internet of Things: Novos Serviços Digitais para Cidadãos” mantidos pela Cisco ou seus parceiros e pelo curso on-line “Introdução à Internet das Coisas (IoT)”. Tempo estimado para concluir: 20 horas. Visão geral do curso: O curso Introdução ao IoT (Internet das Coisas) apresenta aos professores as tecnologias que suportam a IoT e as oportunidades geradas pelo crescente número de ligações de rede entre pessoas, processos, dados e coisas.

3. Segurança de TI: webinar “Como se proteger de ameaças de rede” mantidas pela Cisco ou seus parceiros e curso on-line “Introdução à cibersegurança”. Tempo estimado para concluir: 20 horas. Visão geral do curso: O curso “Introdução à cibersegurança” analisa tendências no mundo da TI, ameaças e o fato de estar em segurança total no ciberespaço, protegendo dados pessoais.

Impacto

Desde que o projeto terminou em 3 de junho, os números relativos aos professores formados ainda estão a ser elaborados. No entanto, o projeto é inovador porque combina formação relacionada à tecnologia com empreendedorismo digital, mas também com programação.

Conclusão

A pesquisa realizada para o Projeto Cyber.eu.vet revelou que há uma falta de dados e informações sobre as competências e desafios de cibersegurança dos educadores das instituições de educação em nível europeu, bem como que há um número limitado de iniciativas focadas em problemas de cibersegurança dentro do ensino profissional, indicando que o Projeto Cyber.eu.vet abordou um tópico emergente nos Estados -Membros.

No entanto, as iniciativas existentes são abrangentes e provaram ser eficientes (consulte as boas práticas da seção). Atualmente, a maioria das atividades e projetos está focada na conscienciali zação da cibersegurança da população em geral e na melhoria das competências digitais gerais dos educadores, que foram influenciados pela rápida adaptação ao processo de trabalho/aprendizagem remota.

O consórcio deste projeto é multifacetado e tem uma expressão clara de diferentes competências digitais em toda a Europa. No entanto, independentemente do ranking DESI dos países individuais, este relatório de pesquisa do consórcio pode ser usado para atrair indicações significativas e válidas para todo o contexto europeu.

O sentimento de necessidade de formação é claro, mesmo entre os professores de ensino profissional que já foram formados em TIC. Não há rejeição à necessidade de formação, nem quanto à utilidade dos seus questionários. Também observamos que quanto mais professores se sentem expostos a riscos psico-social, ético, legal, técnico ou à saúde, mais eles dizem que sentem a necessidade de formação.

De acordo com uma pesquisa nacional, mais da metade dos professores que se sentem vulneráveis ao cyberbullying sentem que é necessário formação. Para eles, a educação inicial e continuada é uma oportunidade de partilhar experiências e analisar métodos de prática profissional nesse campo. Ainda se acredita que o uso de ferramentas digitais na educação é

apenas uma maneira de ensinar ou um objeto a ser ensinado aos alunos, em vez de ser parte integrante de uma cultura geral.

Uma cultura de fontes e práticas de informação sobre riscos digitais (pesquisa e monitorização) deve ser desenvolvida. A formação também deve ser intensificada sobre os desafios da tecnologia digital e, em particular, os problemas psico-social, éticos, legais e técnicos que podem surgir no uso de ferramentas digitais e que preocupam os professores a ponto de levá-los a desistir de todos usar.

Assim, o conhecimento dos riscos digitais pode influenciar positivamente as práticas pedagógicas para educar os alunos em alfabetização digital. Um professor com uma forte cultura digital estará mais inclinado a usar a tecnologia digital na sala de aula com seus alunos e tornar a 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, complementando uma cultura da informação no sentido mais amplo, que evita a demonização do objeto técnico e permite que o potencial educacional seja explorado. Não se trata de educar com medo, mas também emancipando (e ser emancipado, como professor) através de uma apreensão crítica e esclarecida do mundo digital.

Referências

ADEI (2017), *El trabajo del futuro*. Technical Note.

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

Andries B. et Beigbeder I. (coordonné par) (1993), *La culture scientifique et technique pour les professeurs des écoles*, Paris: Hachette éducation, CNDP.

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

Baron G.-L. et Bruillard É. (2000), *Technologies de l'information et de la communication dans l'éducation : Quelles compétences pour les enseignants?,* Éducation et Formation, No 56.

Baron G.-L. et Bruillard É. (sous la direction) (2002), *Les technologies en éducation: perspectives de recherche et questions vives*, Actes du Symposium international francophone, Paris : INRP, IUFM de Basse-Normandie, MSH.

BIBB (2016), *"Economy 4.0 needs Education 4.0", Strengthening the media competence of training staff and trainees*

Blanco, R., Fontrodona, J., Poveda, C. (2017), *La industria 4.0: el estado de la cuestión,* Revista Economía Industrial, No 406.

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.

Capelle, C., Cordier, A., Lehmans, A., (2018), *Usages numériques en éducation : l'influence de la perception des risques par les enseignants*, Open Edition Journals.

Carrizosa Prieto, E (2018), *Lifelong learning e industria 4.0. Elementos y requisitos para optimizar el aprendizaje en red.*, Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, No 1.

Central Statistics Office (CSO) (2018), Information Society Statistics – Households: https://www.cso.ie/en/releasesandpublicatons/er/isshh/informationsocietystatisticshouseholds2018/ (accessed on 6th July, 2021).

CEFEDOP, (2021), *Vocational education and training in Portugal*, EU Agenda.

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf(accessed on 3rd July, 2021).

Database of National Education Opportunities – Niid.lv, study programmes in cybersecurity

Department of Education and Skills, Government of Ireland (2015), *Digital Strategy for Schools (2015-2020)-Enhancing Teaching, Learning and Assessment.*

Department of Education and Skills, Government of Ireland (2017), *Higher Education System Performance Framework 2018-2020.*

Department of Enterprise, Trade and Employment (2018), *Future Jobs Ireland – Preparing Now for Tomorrow's Economy.*

Department of Further and Higher Education, Research, Innovation and Science, Government of Ireland (2021), *Statement of Strategy 2021-2023.*

Department of Justice (2021). Cybercrime: www.justice.ie/en/jelr/pages/cybercrime (accessed on 2nd July, 2021).

Department of Tourism, Culture, Arts, Gaeltach, Sport and Media (2019), *Action Plan for Online Safety 2018 – 2019.*

Dig8tal (2020), *Is German Cybersecurity ready for 2021?,* https://dig8ital.com/resources/library/is-german-cyber-security-ready-for-2021

Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program
for VET Teachers, Trainers and Potential I-Coaches)

Escuela de organizacion industrial, *Activa industria 4.0.*

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

European Commission (2020), *Italy in the Digital Economy and Society Index.*

European Commission (2020), *Latvia in the Digital Economy and Society Index.*

Federal Office For Information Security, (2019),*The State of IT Security in Germany in 2019.*

Federal Office For Information Security, (2020), *The State of IT Security in Germany in 2020.*

Federal Office For Information Security, (2020). *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.*

Government of Ireland (2018), *National Cyber Security Strategy 2019-2024.*

Government of Italy (2020), *Piano Nazionale di Ripresa e Resilienza -PNRR.*

Government of Latvia, (2019), *Informative report, Cybersecurity Strategy of Latvia.*

Government of Latvia, (2020), *Education Development Guidelines 2021-2027 "Future Skills for the Future Society".*

Government of Latvia, (2020), *Digital Transformation Guidelines 2021-2027.*

Guir R. (2002), *Pratiquer les TICE : Former les enseignants et les formateurs à de nouveaux usages*, Bruxelles: De Boeck et Larcier.

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.*

Joseph, V. (2020). *Vocational education and training for the future of work: France*, Cedefop ReferNet thematic perspectives series.

Kultusministerkonferenz (2016), "*Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz"*

Lardellier P., Moatti, D. (2014), *Les ados pris dans la Toile. Des cyberaddictions aux techno-dépendances*, Paris: Éditions Le Manuscrit, Coll. « Addictions : Plaisir, Passion, Possession »

Latvian Safer Internet Centre (Project-platform "Drossinternets.lv"): https://drossinternets.lv/

LIKTA (Latvian Information and Communication Technologies Association): https://likta.lv/digitalasparmainas-izglitiba/

Likumi.lv, Noteikumi par pedagogiem nepieciešamo izglītību un profesionālo kvalifikāciju un pedagogu profesionālās kompetences pilnveides kārtību. https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

Microsoft Digital Defense Report. https://www.microsoft.com/de-de/security/business/security-intelligence-report.

Ministry of Education, University and Research, Government of Italy, *Piano Nazionale Scuola Digitale – PNSD.*

Ministry of Education, University and Research, Government of Italy, (2018), *La Buona Scuola* (Law No. 107/2015)

Ministry of Education, University and Research, Government of Italy (2020), *Accordo di collaborazione per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'utilizzo consapevole delle tecnologie digitali e dei social media*, Memorandum of Understanding n. 4 of 28 October 2020.

Ministry of Education, University and Research, Government of Italy (2021), *Innovare e potenziare le competenze digitali nella scuola*, Memorandum of Understanding n. 785 of 22 January 2021.

Ministry of Industry, Trade and Tourism, Government of Spain, Industria Conectada 4.0, Agenda Digital para Espana.

Ministry of Technological Innovation and Digital Transition (2020), *2025 – Strategia per l'innovazione tecnologica e la digitalizzazione del Paese.*

Mokhtar Ben Henda (2016), *Identification des besoins en formation tic/e dans les pays francophones du sud. Étude réalisée par: Initiatives pour le Développement numérique de l'espace universitaire francophone francophone*, [Rapport de recherche] Agence universitaire de la Francophonie.

National Centre for Vocational Education Research, (2020), *Teaching digital skills: Implications for VET educators - good practice guide.*

OECD (2021), Going Digital in Latvia

OECD, (2018), TALIS - The OECD Teaching and Learning International Survey TALIS - OECD Teaching and Learning International Survey

Pridzans, Dzerviniks (2019), *The Topicality of Educators' Digital Competence Development*, SOCIETY. INTEGRATION. EDUCATION Proceedings of the International Scientific Conference. Volume V, May 24th -25th.

Principes et organisation de la deuxième année de la formation des enseignants stagiaires en IUFM, (2002). La circulaire du 4 avril 2002 parue au Bulletin officiel n° 15 du 11 avril 2002.

Saldus Technical School, Study Programme Civil Security and Defence: https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja

Stolterman, E (2004), *Information Technology and the Good Life*, International Federation for Information Processing Digital Library; Information Systems Research. Volume 143.

Télé-enseignement : *les 5 risques majeurs en matière de cybersécurité* – Sophos News

Thélot C. (sous la direction) (2004), *Pour la réussite de tous les élèves, rapport officiel de la Commission du débat national sur l'avenir de l'École*, Paris : La documentation Française.

Disclaimer

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

It is possible to trace the document through the following qr code :