Manual CYBER.VET.EU

Mejora de la preparación en materia de ciberseguridad del sector europeo de la formación profesional

2020-1-DE02-KA226-VET-008327

RED TANDEM PLUS con el consorcio CYBER.VET.EU:

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

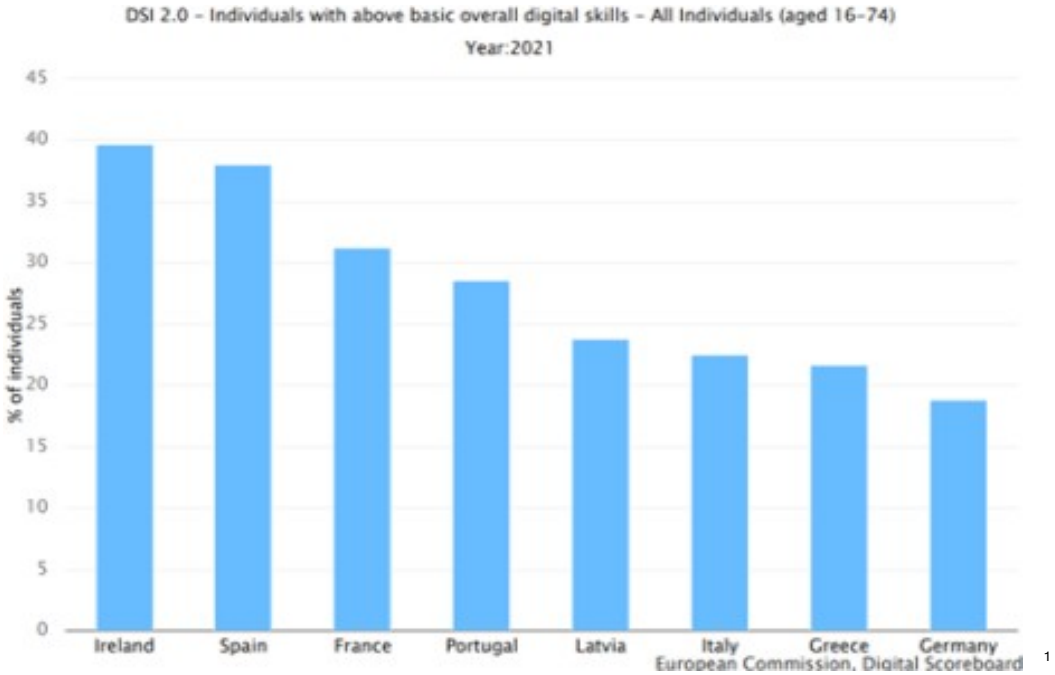
Co-funded by the
Erasmus+ Programme
of the European Union

Resumen

a) Ejecución del proyecto CYBER.EU.VET

La Unión Europea se enfrenta a un reto trascendental representado por la pandemia de Covid-19. Muchos sectores se ven fuertemente afectados por estas crisis y la educación es sin duda uno de ellos. Cada vez son más los usuarios que se ven obligados a utilizar las clases o la formación en línea, por lo que la importancia de reconocer las amenazas cotidianas a nuestra seguridad es ahora más importante que nunca. Este tema es reconocido como fundamental también por la Comisión Europea que cada año organiza un Mes Europeo de la Ciberseguridad, de cuya página web ya se incluyen algunos materiales educativos y campañas de concienciación específicas como la de "Get cyber skilled" en 2018 .

El proyecto CYBER.EU. VET incluye 8 socios (NGO NEST - Alemania (LEADER), MEATH COMMUNITY RURAL AND SOCIAL DEVELOPMENT PARTNERSHIP LIMITED - Irlanda, TANDEM PLUS - Una red de la UE con sede en Francia, COFAC COOPERATIVA DE FORMACAO E ANIMACAO CULTURAL CRL- Portugal, LATVIJAS ASOCIACIJA EIROPAS KOPIENAS STUDIJAM - Letonia, ASOCIACION EDUCATIVA POR LA INTEGRACION Y LA IGUALDAD - España, INECIA DIGITAL - España, Extrafondente Open Source - Italia)



[1]

El principal objetivo de CYBER.EU.VET es reforzar la capacidad de la EFP europea para reconocer y gestionar las amenazas a la ciberseguridad (por ejemplo, ataques de phishing, botnets, fraudes financieros y bancarios, fraude de datos) en un contexto histórico en el que se utiliza cada vez más la formación en línea.

i. Impacto del proyecto:

El proyecto tuvo un impacto a nivel local, regional y nacional al involucrar a diferentes niveles de actores, ofreciendo soluciones que se adaptan a las demandas de los niveles locales, pero que se alinean a un nivel superior, desarrollando, a través de la asociación, material y normas de formación aplicables a toda la UE. En particular, el impacto sobre los participantes directos y los principales grupos destinatarios ha sido el siguiente:

- Educadores de EFP - Una capacidad de enseñanza reforzada, añadiendo a sus habilidades un conocimiento de las principales amenazas a la seguridad digital.
- Educadores y estudiantes de EFP: mejora de las competencias digitales gracias al material didáctico.

[1] Perfil del Indicador ESMS (ESMS-IP) Agencia compiladora: Eurostat, la oficina estadística de la Unión Europea.

- Educadores y estudiantes de EFP: una mayor concienciación sobre las amenazas y sus riesgos reales, tanto económicos como sociales.
- Los centros de FP estarán más preparados para hacer frente a los riesgos de ciberseguridad con las herramientas de CYBER.VET.EU, tanto para sus educadores como para sus estudiantes.

ii. Project Target

Se espera que el proyecto tenga un impacto positivo y a largo plazo en las diferentes partes interesadas que participan en el proyecto, en particular:

- Estudiantes de FP
- Voluntarios expertos en ciberseguridad
- Redes de instituciones de EFP
- Responsables políticos

iii. Objetivos del proyecto CYBER.EU.VET:

- El primer objetivo específico será contar con educadores de EFP más preparados en la gestión de las amenazas de ciberseguridad, dado su papel central en la transferencia de conocimientos de buenas prácticas y habilidades a sus estudiantes.
- El segundo objetivo específico es aumentar la concienciación entre los profesores de EFP, los estudiantes y sus familiares sobre la importancia de reconocer estos riesgos diarios, que pueden tener un impacto tanto económico como social en todos los ciudadanos europeos.
- El tercer objetivo específico es apoyar a las instituciones públicas y a los centros de EFP para que estén más preparados para afrontar este tipo de retos, proporcionándoles directrices para futuras implementaciones.

iv. Resultados intelectuales:

- O1: Análisis de la investigación: principales retos de la ciberseguridad y mejores prácticas (socio responsable: ONG NEST BERLIN EV - E10166639)
- O2: Material formativo de sensibilización en ciberseguridad para el sector de la FP (socio responsable: INERCIA DIGITAL SL - E10145080)

- O3: Kit de herramientas de formación para formadores (socio responsable INERCIA DIGITAL SL (E10145080)
- O4: Manual de ciberseguridad para centros de FP: mejores prácticas, material de formación y directrices para futuras implementaciones (Socio responsable TANDEM PLUS - E10103913)

Paralelamente al desarrollo de los resultados intelectuales, el otro objetivo del proyecto es difundir nuestros resultados en toda la UE entre los participantes potenciales, los multiplicadores y las partes interesadas, para impulsar el impacto y la relevancia de CYBER.EU.VET.

v. ¿Qué es la ciberseguridad?

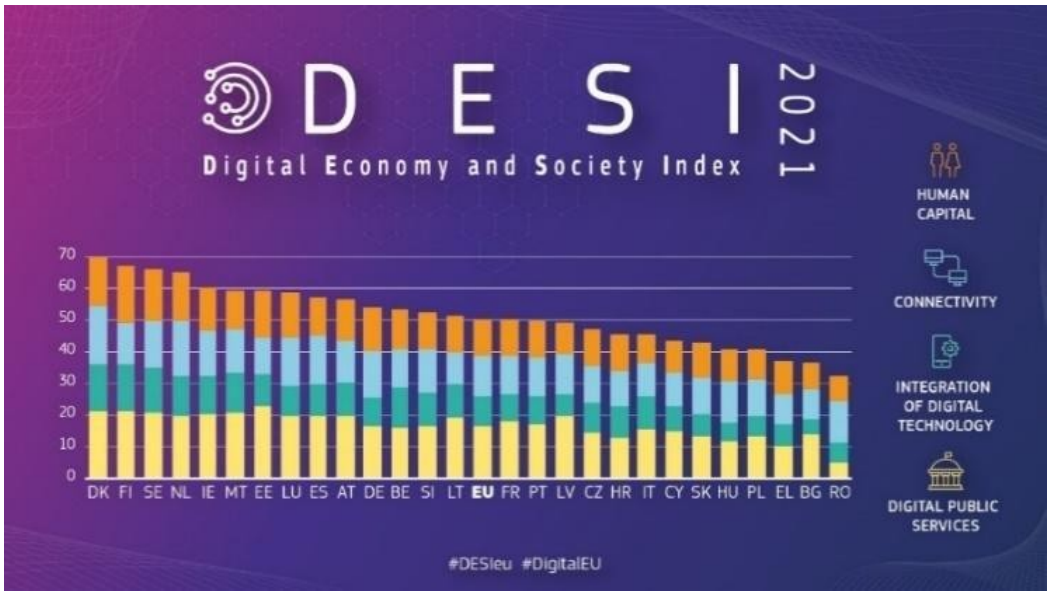
La definición formal de **ciberseguridad** en la legislación de la UE se encuentra en el texto de la Ley de Ciberseguridad de la UE: "se entiende por ciberseguridad las actividades necesarias para proteger las redes y los sistemas de información, los usuarios de dichos sistemas y otras personas afectadas por las ciberamenazas" (art. 2.1).

La legislación de la UE, al tiempo que adopta el enfoque de "protección de los sistemas de red y de información", también subraya que la ciberseguridad no solo protege los sistemas de información, sino también (y quizás más importante) a las personas, independientemente de que los usuarios de dichos sistemas o terceros se vean afectados de algún modo por las ciberamenazas.

En diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) presentaron una nueva estrategia de ciberseguridad de la UE con el objetivo de aumentar la resistencia a las ciberamenazas y garantizar que los ciudadanos y las empresas se beneficien de tecnologías digitales fiables.

El Reglamento (UE) 2021/887 por el que se crea el Centro de Competencia Europeo en materia de Ciberseguridad Industrial, Tecnológica y de Investigación y la Red de Centros Nacionales de Coordinación establece el Centro de Competencia Europeo en materia de Ciberseguridad (CCCE) y la Red de Centros Nacionales de Coordinación (la "red") y fija las normas para los centros nacionales de coordinación (CNC) y para la creación de la Comunidad de Competencia en materia de Ciberseguridad.

El Centro Europeo de Competencia en Ciberseguridad ayuda a la UE a reforzar el liderazgo de la UE en materia de ciberseguridad mediante la mejora de la confianza y la seguridad, incluida la confidencialidad, la integridad y la accesibilidad de los datos, apoyando la resistencia y la fiabilidad de las redes y los sistemas de información, incluidas las infraestructuras críticas y el hardware y el software de uso común.



vi. Principal reto de las competencias digitales en Europa

- Alrededor de 70 millones de europeos carecen de conocimientos suficientes de lectura, escritura y cálculo
- El 24% de la población de la UE no tiene un título de educación secundaria superior
- El 13% de los europeos no ha utilizado nunca Internet
- El 43% de la población de la UE y el 35% de la población activa de la UE no tienen suficientes competencias digitales
- El 42% de los que no tienen competencias digitales están desempleados
- Nativos digitales ≠ competencia digital

vii. Contexto

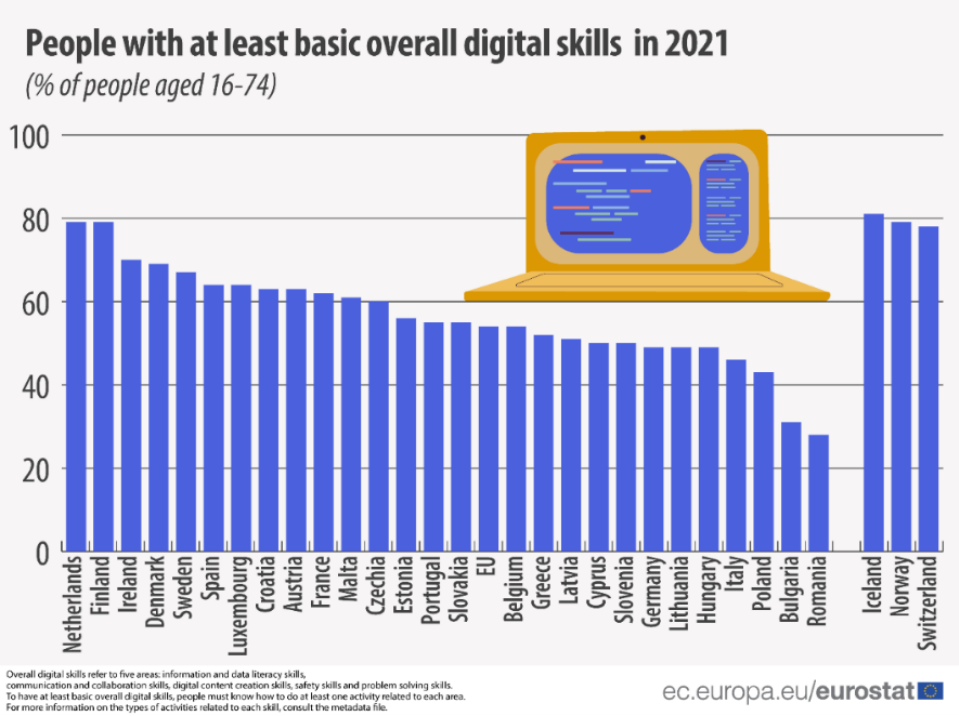
Más del 70% de las empresas han manifestado que la falta de personal con conocimientos digitales adecuados es un obstáculo para la inversión. Europa también se enfrenta a una escasez de expertos digitales que puedan desarrollar tecnologías de vanguardia en beneficio de todos los ciudadanos.

Una economía digital fuerte impulsada por europeos con competencias digitales es vital para la innovación, el crecimiento, el empleo y la competitividad europea. La difusión de las tecnologías digitales está teniendo un impacto masivo en el mercado laboral y en el tipo de competencias necesarias en la economía y en la sociedad. Los Estados miembros, las empresas, los proveedores de formación, la Comisión Europea y otras organizaciones deben trabajar juntos para hacer frente a la brecha de competencias digitales. Para seguir el desarrollo de la transición digital y la brecha de competencias digitales, la Comisión publica anualmente el DESI [Indicador de Competencias Digitales]. En él se hace un seguimiento de los resultados digitales de los Estados miembros en diferentes ámbitos para supervisar los avances y señalar dónde es necesario realizar más esfuerzos.

En 2021, el 54% de los habitantes de la UE de entre 16 y 74 años tenía al menos unas competencias digitales generales básicas.

En 2021, el porcentaje de personas de entre 16 y 74 años que tenían al menos competencias digitales generales básicas era más alto en los Países Bajos y Finlandia (ambos con un 79%), seguidos de Irlanda (70%). Por otro lado, la proporción más baja se registró en Rumanía (28%), seguida de Bulgaria (31%) y Polonia (43%).

Los indicadores de competencias digitales son algunos de los principales indicadores de rendimiento en el contexto de la Década Digital, que establece la visión de la UE para la transformación digital. La Brújula Digital establece el objetivo de que el 80% de los ciudadanos de la UE de entre 16 y 74 años de edad tengan al menos las competencias digitales básicas para 2030.



Volver al contenido ↑

b) Competencias digitales de los educadores de EFP: una visión del consorcio

i. Alemania:

- VET Data Report (2019) elaborado por el Instituto Federal Alemán de Educación y Formación Profesional (BIBB) afirmó que "la digitalización va a reforzar los cambios estructurales del mercado laboral", lo que lleva a la necesidad de un cambio en las capacidades de formación dentro de los respectivos campos. Como se indica en la Resolución de la Conferencia Permanente de Ministros de Educación y Asuntos Culturales (2016-2017) el área de la educación profesional, la promoción de las competencias relacionadas con el trabajo en el contexto de los procesos digitales de trabajo y de negocios es una parte esencial de la competencia de los profesores como punto de partida para sus actividades didácticas.

ii. Irlanda:

- Una de las estrategias clave de Irlanda en relación con las competencias digitales de los educadores de EFP es la Estrategia Digital Nacional, que se puso en marcha en julio de 2013. La estrategia se centra en el compromiso digital y destaca cómo Irlanda puede beneficiarse de una sociedad digitalmente comprometida.

  En lo que respecta a las competencias digitales de los educadores de EFP, los datos siguen poniendo de manifiesto que existe una brecha cada vez mayor entre los educadores que utilizan los dispositivos digitales en sus clases como herramienta de aprendizaje y los que no lo hacen.

iii. Portugal:

- El sistema nacional de cualificaciones ha reorganizado la EFP en un sistema único en el que los programas conducen a una doble certificación. La EFP para adultos es parte integrante del sistema nacional de cualificaciones, y sus elementos clave son los programas de educación y formación para adultos y el reconocimiento y la validación del aprendizaje previo. Portugal ha hecho progresos significativos en lo que respecta al nivel de estudios, pero sigue siendo inferior a la media de la UE. Aunque menos que en 2015 (73,7%), en 2019 la proporción de personas con bajo nivel o sin cualificación era del 50,2%, la más alta de la UE.

iv. Italia:

- En el ámbito de la educación las acciones se llevaron a cabo principalmente a través de la aplicación del Plan Nacional de Escuela Digital. Las directrices del Ministerio de Educación, Universidad e Investigación pusieron en marcha una estrategia global de innovación para la escuela italiana y para un nuevo posicionamiento de su sistema educativo en la era digital. La mayoría de las acciones para la formación del personal escolar se han dirigido a los centros de enseñanza primaria y secundaria, que representan la mayoría de los centros educativos en Italia, mientras que se ha prestado poca atención al sector de la Formación Profesional.

v. España:

- La Agenda Digital para España (ADpE, Agenda Digital para España) publicada en 2013, es la hoja de ruta para el cumplimiento de los objetivos marcados por la Agenda Digital para Europa en 2015 y 2020, así como la consecución de objetivos específicos para el desarrollo de la economía y la sociedad digital en España. Se estructura en torno a seis grandes objetivos y varios planes específicos. El sexto objetivo se refiere al fomento de la inclusión y la alfabetización digital y a la formación de nuevos profesionales de las TIC.

vi. Francia:

- Si observamos el ritmo de la formación sobre el uso de las TIC en las universidades francesas que la imparten, vemos que no existen políticas claras y sostenidas de formación de formadores sobre el uso de las TIC/E. Alrededor del 58% señala una sola sesión de formación al año, frente a un 7,4% al mes y un 0,5% a la semana.
  Las estadísticas muestran que la densidad de la formación en informática varía de una región francófona a otra. Esto se debe a varias razones, las más importantes de las cuales están sin duda relacionadas con las instituciones académicas y sus gobiernos.

vii. Letonia:

- En 2020, el Ministerio de Educación y Ciencia de la República de Letonia ha establecido la mejora de la competencia digital de los educadores como un objetivo prioritario de la competencia profesional, asignando para ello una financiación adicional (0,5 millones de euros). La necesidad de concienciar a los alumnos y educadores sobre la seguridad de la información, la protección de la privacidad y el uso de servicios electrónicos fiables (Estrategia de Ciberseguridad 2019-2022, área de acciones "Concienciación pública, educación e investigación").

viii. Grecia:

- Aunque la adquisición de competencias digitales es un componente que no debería faltar en el conjunto de herramientas educativas de los educadores de EFP, se puede identificar una brecha importante al observar el sistema educativo actual en Grecia. A pesar de las numerosas reformas del currículo educativo, la evidencia sugiere que los educadores no están siendo suficientemente equipados con conocimientos de las TIC y, por lo tanto, carecen de

herramientas y técnicas pedagógicas orientadas a lo digital que podrían mejorar el proceso de enseñanza (Ministerio de Educación,2019).

Resultados

La investigación llevada a cabo para el proyecto CYBER.EU.VET reveló que hay una falta de datos e información sobre las competencias de ciberseguridad y los desafíos de los educadores de las instituciones educativas a nivel europeo, así como que hay un número limitado de iniciativas centradas en las cuestiones de ciberseguridad dentro de la EFP, lo que indica que el proyecto CYBER.EU.VET ha abordado el tema emergente en todos los Estados miembros. En la actualidad, la mayoría de las actividades y proyectos se centran en la concienciación sobre la ciberseguridad de la población en general y en la mejora de las competencias digitales generales de los educadores, en lo que ha influido la rápida adaptación al proceso de trabajo/aprendizaje a distancia.

El consorcio de socios es polifacético y una clara expresión de un grado diferente de competencias digitales en toda Europa. Sin embargo, independientemente de la clasificación DESI de los distintos países, este informe de investigación del consorcio puede utilizarse para extraer indicaciones significativas y válidas para todo el contexto europeo. El sentimiento de necesidad de formación es claro, incluso entre los profesores de FP que ya han recibido formación en TIC. No se rechaza la necesidad de formación, ni se cuestiona su utilidad. También se observa que cuanto más expuestos se sienten los profesores a los riesgos psicosociales, éticos, jurídicos, técnicos o sanitarios, más dicen sentir la necesidad de formarse. Según una encuesta nacional, más de la mitad de los profesores que se sienten vulnerables al ciberacoso consideran que la formación es necesaria. Para ellos, la formación inicial y continua es una oportunidad para compartir experiencias y analizar métodos de práctica profesional en este campo. Se sigue creyendo que el uso de las herramientas digitales en la educación es una forma de enseñar o un objeto que hay que enseñar a los alumnos, más que una parte integral de su cultura general. Hay que desarrollar una cultura de las fuentes de información y de las prácticas sobre los riesgos digitales (investigación y seguimiento). También debe reforzarse la formación sobre los retos de la tecnología digital y, en particular, sobre los problemas psicosociales, éticos, jurídicos y técnicos que pueden surgir en el uso de las herramientas digitales y que preocupan a los profesores hasta el punto de llevarles a renunciar a todo uso.

Así, el conocimiento de los riesgos digitales puede influir positivamente en las prácticas pedagógicas para educar a los alumnos en la alfabetización digital. Un profesor con una sólida cultura digital será

más proclive a utilizar la tecnología digital en el aula con sus alumnos y a hacer de la tecnología digital un objeto de enseñanza-aprendizaje.

La evidente influencia de la representación de los riesgos es imposible de cambiar positivamente sin una cultura digital general y plural, complementaria a una cultura de la información en sentido amplio, que evite la demonización del objeto técnico y permita aprovechar el potencial educativo.
No se trata de educar en el miedo, sino de emanciparse (y emanciparse, también como profesor) a través de una aprehensión crítica e ilustrada del mundo digital.

Volver al contenido ↑

c) Caja de herramientas CYBER.EU.VET

Según el Plan de Educación Digital 2021-2027, las competencias digitales y los retos de aprendizaje son también una prioridad en la agenda europea. La Comisión Europea está decidida a abordar la brecha de competencias digitales y a promover proyectos y estrategias para mejorar el nivel de competencias digitales en Europa. Todos los europeos necesitan competencias digitales para estudiar, trabajar, comunicarse, acceder a los servicios públicos en línea y encontrar información fiable. Sin embargo, muchos europeos no tienen las competencias digitales adecuadas. El Índice de Economía y Sociedad Digitales (DESI) muestra que 4 de cada 10 adultos y una de cada tres personas que trabajan en Europa carecen de competencias digitales básicas. También hay una baja representación de mujeres en profesiones y estudios relacionados con la tecnología, ya que sólo 1 de cada 6 especialistas en TIC y 1 de cada 3 licenciados en ciencias, tecnología, ingeniería y matemáticas (STEM) son mujeres.
La Comisión Europea ha fijado objetivos en la agenda europea de competencias y en el plan de acción de educación digital para garantizar que el 70% de los adultos tengan competencias digitales básicas de aquí a 2025. Estas iniciativas pretenden reducir el nivel de jóvenes de 13 a 14 años con un rendimiento inferior en informática y alfabetización digital del 30% (2019) al 15% en 2030. La Plataforma Europea de Competencias y Empleos Digitales es una nueva iniciativa puesta en marcha en el marco del programa Mecanismo "Conectar Europa". Ofrece información y recursos sobre competencias digitales, así como oportunidades de formación y financiación.

i. Marcos de competencia digital del CCI/CE

- Marco de competencia digital para los ciudadanos (DigComp)
- Marco de competencia digital para educadores (DigCompEdu)

- Marco de competencia digital para organizaciones educativas (DigCompOrg) y una herramienta de autorreflexión para centros escolares (SELFIE)

¿Por qué todos estos marcos?

- Creación de capacidades para la transformación digital de la educación y la formación y para abordar los retos de las competencias del siglo XXI.
- Marcos de referencia que proporcionan una comprensión global, completa y compartida: un lenguaje común.

¿Qué?

- Modelo conceptual, niveles de competencia y módulos de (auto)evaluación.
- La competencia se define como conocimientos, habilidades y actitudes.

ii. TheDigComp 2.2

Más de 250 nuevos ejemplos de conocimientos, habilidades y actitudes para ayudar a los proveedores de educación y formación a actualizar su plan de estudios y material de curso de DigComp para hacer frente a los desafíos actuales.

La lista de competencias y áreas de DigComp sigue siendo la misma:

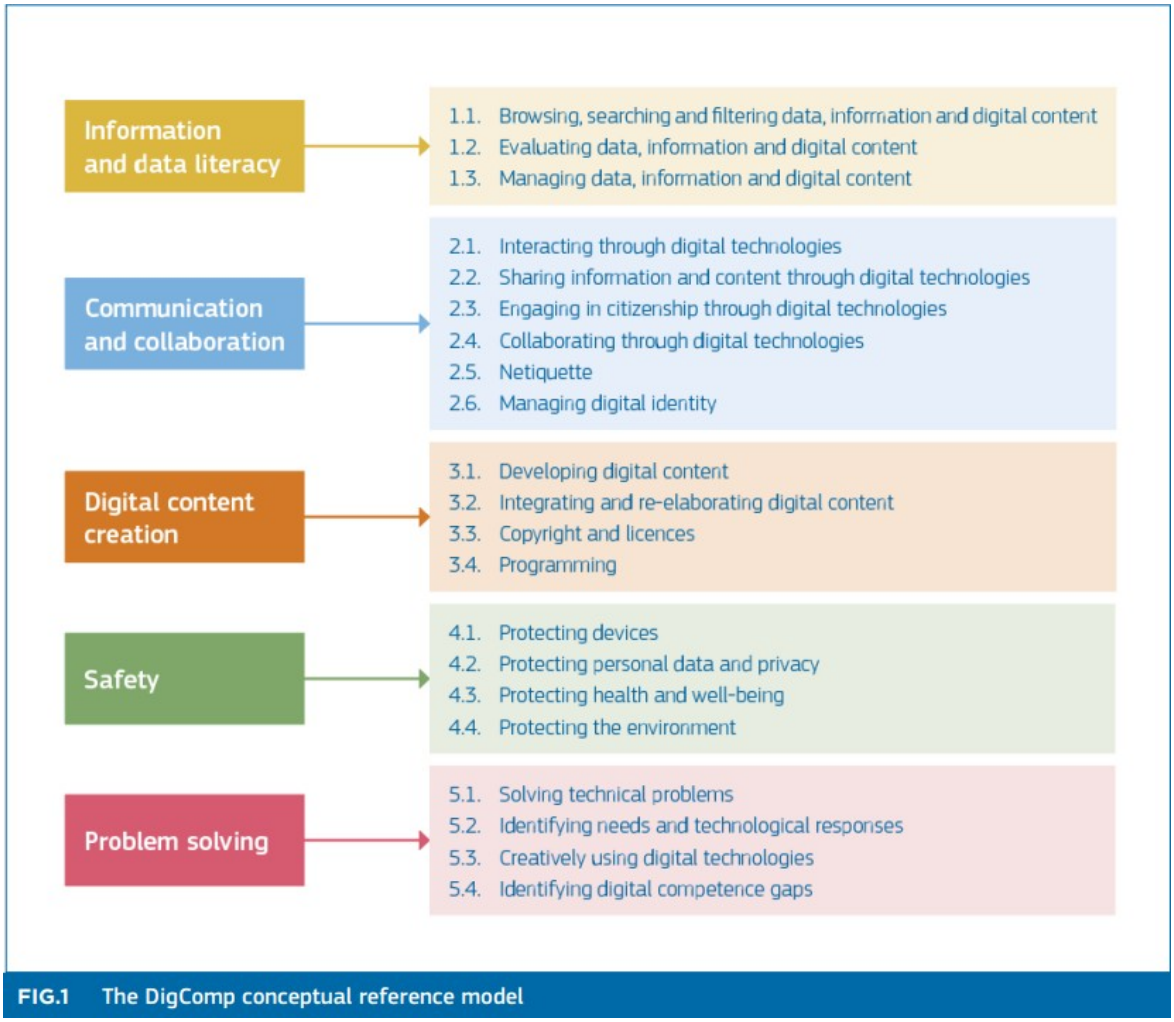


FIG.1 The DigComp conceptual reference model

[2]

Uno de los temas clave de la actualización de DigComp 2.2 es el bienestar y la seguridad. En cada área hay entre 10 y 15 enunciados por competencia para ilustrar temas contemporáneos oportunos. No representan una lista exhaustiva de lo que implica la competencia en sí y no están en los niveles de competencia, aunque algunos son más complejos que otros, pero son útiles para la planificación y

[2] Comisión Europea, Centro Común de Investigación, Vuorikari, R., Kluzer, S., Punie, Y., DigComp 2.2, The Digital Competence framework for citizens : with new examples of knowledge, skills and attitudes, Oficina de Publicaciones de la Unión Europea, 2022, https://data.europa.eu/doi/10.2760/115376

actualización del currículo y para el desarrollo del programa de formación de DigComp o del contenido del curso.

SEGURIDAD: "proteger los dispositivos y los contenidos digitales, y comprender los riesgos y amenazas en los entornos digitales. Conocer las medidas de seguridad y tener en cuenta la fiabilidad y la privacidad".[3]

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.

4

iii. The DigCompEdu

[3] Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2018 KE-01-18-834-ES-N.pdf
[4] Ibidem

El Marco Europeo para la Competencia Digital de los Educadores (DigCompEdu) es un marco científicamente sólido que describe lo que significa que los educadores sean digitalmente competentes. Proporciona un marco de referencia general para apoyar el desarrollo de las competencias digitales específicas de los educadores en Europa. DigCompEdu está dirigido a educadores de todos los niveles educativos, desde la educación infantil hasta la superior y la de adultos, pasando por la educación y la formación general y profesional, la educación para necesidades especiales y los contextos de aprendizaje no formal.

El marco DigCompEdu refleja los esfuerzos realizados a nivel internacional para captar y definir las competencias digitales específicas digitales de los profesores y formadores.

El objetivo es proporcionar un marco para quienes trabajan en el sector de la educación y la enseñanza superior y se encargan de desarrollar modelos de competencia digital, por ejemplo, los responsables políticos de los Estados miembros, las autoridades regionales/locales, las organizaciones educativas, las instituciones (públicas o privadas) que prestan servicios de formación y desarrollo profesional.

Así, el valor añadido del marco DigCompEdu es que proporciona:

- una base sólida que pueda orientar la política a todos los niveles
- una plantilla que permita a los interesados locales pasar rápidamente a desarrollar un instrumento concreto
- instrumento concreto, adaptado a sus necesidades, sin tener que desarrollar una base conceptual para este trabajo;
- un lenguaje y una lógica comunes que pueden ayudar al debate y al intercambio de las mejores prácticas
- un punto de referencia para que los Estados miembros y otras partes interesadas validen la integridad

– y el enfoque de sus propias herramientas y marcos existentes y futuros.[5]

iv. CREACIÓN DE LA CAPACIDAD DE HABILIDADES DIGITALES DEL EDUCADOR VETERINARIO

El uso o el desarrollo de marcos o herramientas de autoevaluación es una buena manera de determinar el nivel de referencia de la capacidad digital de un educador. A partir de ahí, se pueden diseñar actividades de desarrollo profesional específicas. Junto con la creciente necesidad de utilizar las tecnologías en la práctica docente, existe el requisito de cambiar la pedagogía para garantizar que las herramientas digitales se utilicen de forma eficaz no sólo en la enseñanza, sino también en el diseño y la evaluación de los cursos. El Marco Europeo para las Competencias Digitales de los Educadores (DigCompEdu) describe las áreas clave de competencia que necesitan los educadores a medida que profundizan en su compromiso con el aprendizaje digital y las pedagogías digitales. Las áreas de competencia clave se muestran en la siguiente figura (Redecker 2017

[5] Redecker, C. Marco europeo para la competencia digital de los educadores: DigCompEdu. Punie, Y. (ed). EUR 28775 ES. Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

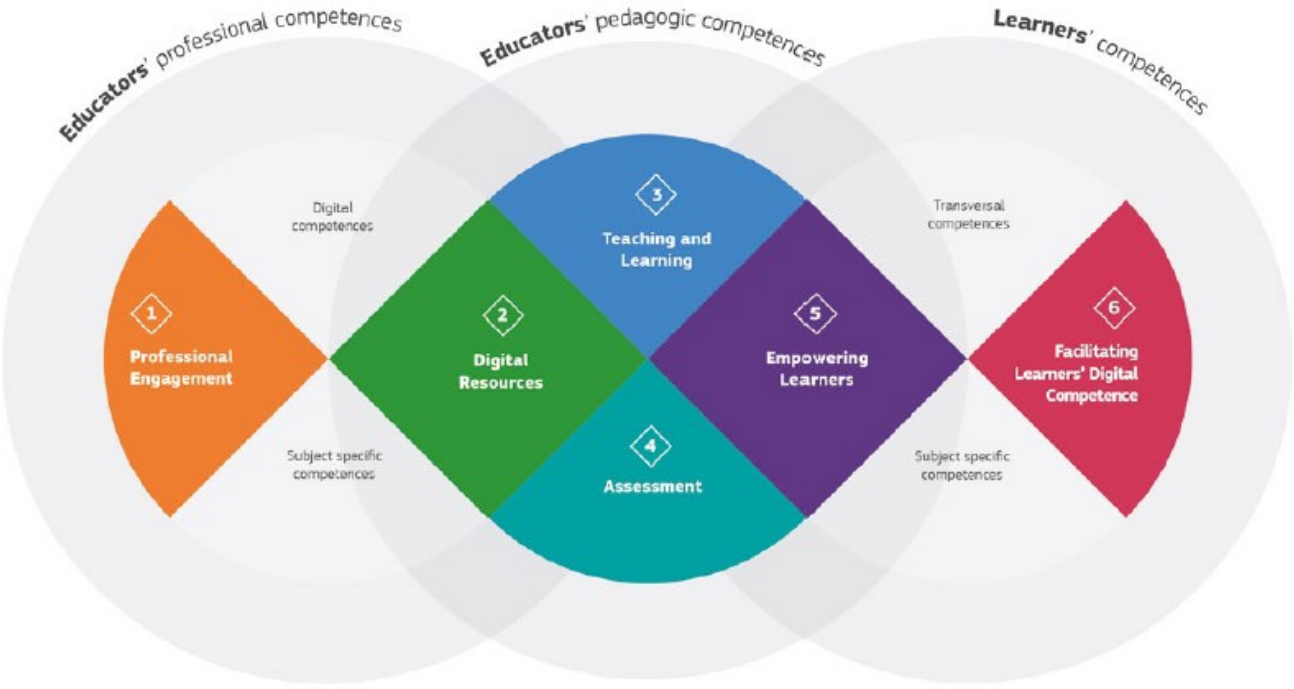


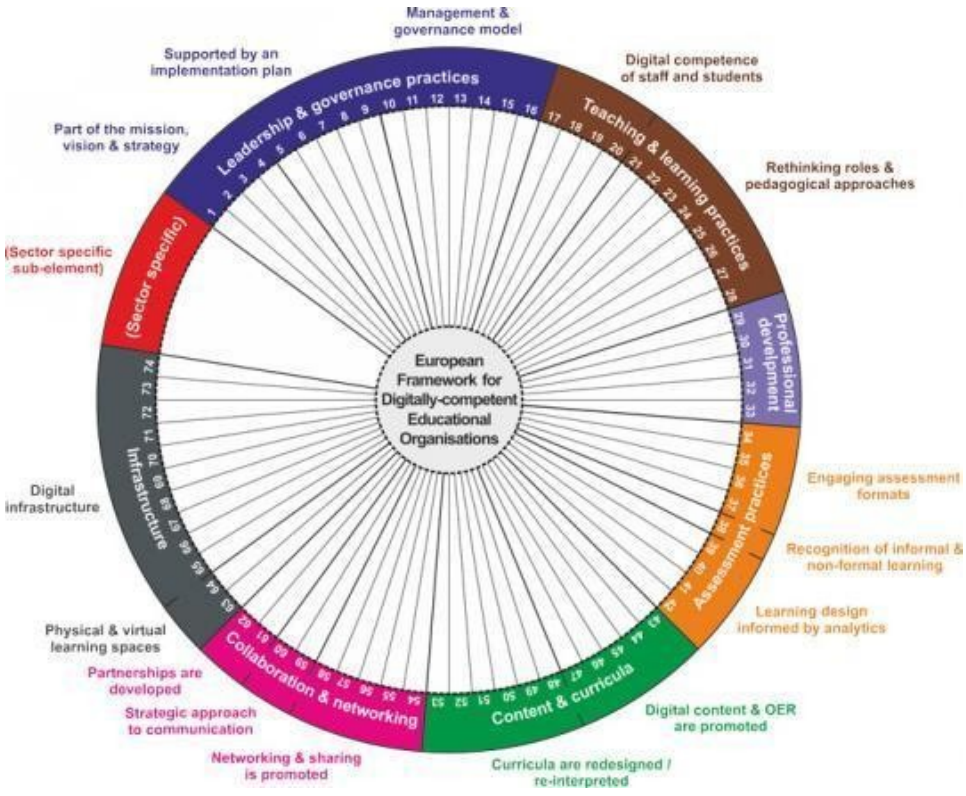
FIGURE 2: DIGCOMPEDU AREAS AND SCOPE

v. El marco DigCompOrg

En varios países europeos se utilizan varios marcos y herramientas de autoevaluación, pero hasta ahora no se ha intentado desarrollar un enfoque paneuropeo de la capacidad digital de las organizaciones. Un marco de referencia europeo que adopte un enfoque sistémico puede añadir valor al promover la transparencia, la comparabilidad y el aprendizaje entre iguales. El **marco DigCompOrg** puede ser utilizado por las organizaciones educativas (es decir, los centros de enseñanza primaria, secundaria y de FP, así como las instituciones de enseñanza superior) para guiar un proceso de

autorreflexión sobre su progreso hacia la integración global y el despliegue eficaz de las tecnologías digitales de aprendizaje.

Además, puede facilitar la transparencia y la comparabilidad entre las iniciativas relacionadas en toda Europa, y también puede desempeñar un papel en la lucha contra la fragmentación y el desarrollo desigual en los Estados miembros. El marco DigCompOrg también puede utilizarse como herramienta de planificación estratégica para que los responsables políticos promuevan políticas integrales para la adopción efectiva de las tecnologías digitales de aprendizaje por parte de las organizaciones educativas a nivel regional, nacional y europeo. También puede utilizarse como medio para concienciar sobre el enfoque sistémico necesario para el uso eficaz de las tecnologías digitales de aprendizaje.



Los objetivos principales de DigCompOrg son

- fomentar la autorreflexión y la autoevaluación dentro de las organizaciones educativas a medida que profundizan progresivamente en su compromiso con el aprendizaje y las pedagogías digitales;
- permitir a los responsables políticos (a nivel local, regional, nacional e internacional)
- diseñar, implementar y evaluar programas, proyectos e intervenciones políticas para la integración de las tecnologías de aprendizaje digital en los sistemas de educación y formación.

vi. SELFIE

SELFIE para el aprendizaje basado en el trabajo (WBL) es una herramienta en línea gratuita que ayuda a los centros de enseñanza y formación profesional (EFP) y a las empresas a aprovechar al máximo las tecnologías digitales para la enseñanza, el aprendizaje y la formación. SELFIE WBL ayuda a los centros educativos y a las empresas a adaptarse a la era digital. De este modo, apoya la transición digital, una de las principales prioridades políticas de la Comisión Europea. Esta adaptación de SELFIE a los requisitos específicos del aprendizaje en línea es un paso necesario para apoyar a los **centros de FP.**

En total, unos **35.000 participantes de unos 150 centros de formación profesional y 250 empresas de Francia, Alemania, Hungría, Polonia, Rumanía, Georgia, Montenegro y Turquía** participaron en el proyecto piloto. Los resultados de estos pilotos están disponibles para su descarga [LINK a los recursos].[6]

El Foro Europeo de Educación y Formación Técnica y Profesional (EfVET) y la Fundación Europea de Formación (ETF) prestaron un apoyo inestimable en todo momento.

[6] SELFIE resources | European Education Area (europa.eu)

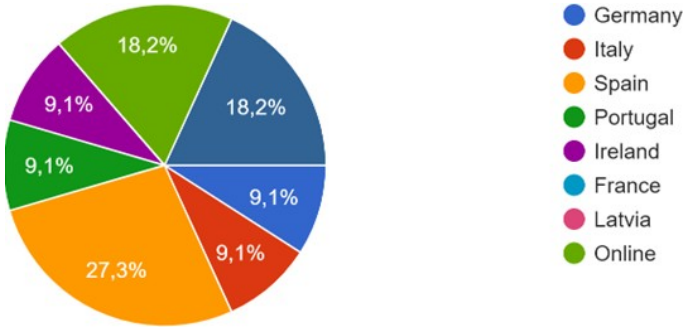
Volver al contenido ↑

d) Directrices CYBER.EU.VET

El proyecto CYBER.EU.VET pretendía contribuir a reforzar la capacidad de la EFP europea para reconocer y gestionar las amenazas de ciberseguridad (por ejemplo, ataques de phishing, botnets, fraudes financieros y bancarios, fraude de datos) en un contexto histórico en el que la formación en línea se utiliza cada vez más.

Para ello, se mejoraron las habilidades y competencias de los educadores de FP en la gestión de las amenazas de ciberseguridad, dado su papel central en la transferencia de conocimientos de buenas prácticas y habilidades a sus estudiantes, aumentando también la conciencia entre los profesores de FP, los estudiantes y sus familias sobre la importancia de reconocer estos riesgos diarios, que pueden tener un impacto tanto económico como social en todos los ciudadanos europeos. El proyecto se basó en una circulación conjunta de capacidades y conocimientos locales, nacionales y transnacionales, así como en un buen nivel de acceso y utilización de la información digital.

Se organizaron 8 sesiones de Gamejam con 54 estudiantes y 15 formaciones nacionales específicas para formadores para formadores para debatir los resultados de la investigación, las herramientas digitales compartidas y las nuevas creadas, intercambiando experiencias y consideraciones para desarrollar una especie de "narrativa colectiva temática" preparatoria para pasar de la exploración y el análisis a la gestión y la resolución de problemas digitales.



Estos eventos permitieron a los jóvenes trabajar juntos y demostrar que también las instituciones que se perciben como lejanas al ciudadano medio (por ejemplo, la Comisión de la UE) ofrecen oportunidades interesantes para la población juvenil.

Una **sesión de formación** se define en esta guía como una única sesión de formación que tiene lugar en el transcurso de un día o de una parte de un día. Puede durar 30 minutos, una hora o incluso un día entero. Una sesión de formación puede incluir pausas a lo largo del día y abarcar uno o más temas.

Una sesión puede celebrarse en un aula, en un pequeño grupo con una sola familia, o incluso individualmente. Un programa de formación, a efectos de esta guía, es un conjunto de sesiones de formación que completan un ciclo de formación. Por ejemplo, una agencia podría ofrecer un programa de formación de 8 semanas una vez a la semana. El programa de formación podría reiniciarse para un nuevo grupo de personas. (Talleres y cursos, 2021)

I. La base de un taller: Conocimientos, habilidades y actitudes

Esta guía sigue un marco para sensibilizar a los alumnos sobre las amenazas digitales, que se basa en los conocimientos, las habilidades y las competencias. Del mismo modo, los supervisores del programa y los profesores/formadores mejoran sus conocimientos, habilidades y actitudes para ser más eficaces. Esta sección analiza los conocimientos, las habilidades y las actitudes de los profesores y formadores.

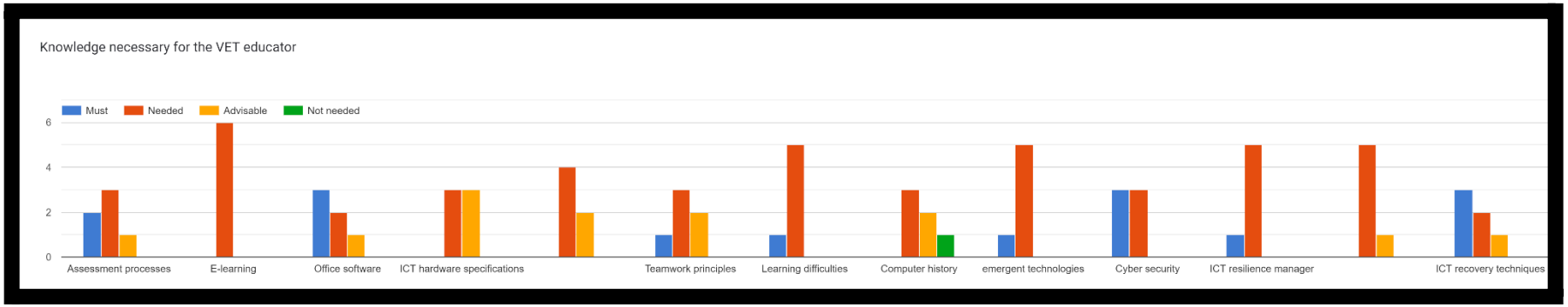
Los conocimientos, las habilidades y las actitudes son la base de una formación eficaz. Los formadores eficaces tienen conocimientos, habilidades y actitudes sobre la formación y los temas que imparten, y los programas y sesiones de formación que imparten deben incluir conocimientos, habilidades y actitudes para los participantes que se centran en el tema y el contenido.

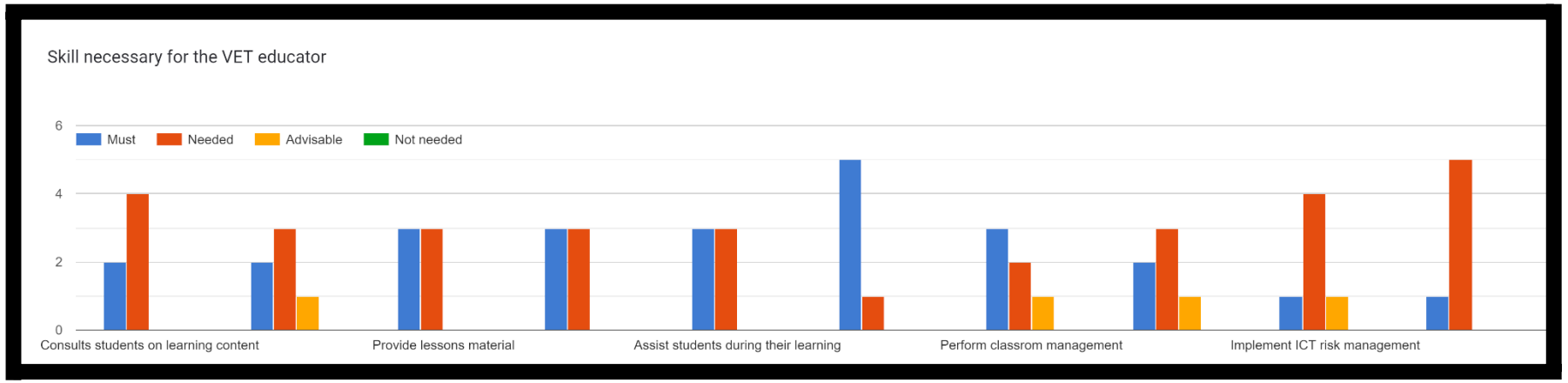
Pregúntese a sí mismo: ¿A quién puede dirigirse si tiene preguntas sobre las normas y el contenido del programa como nuevo profesional de la EFP?

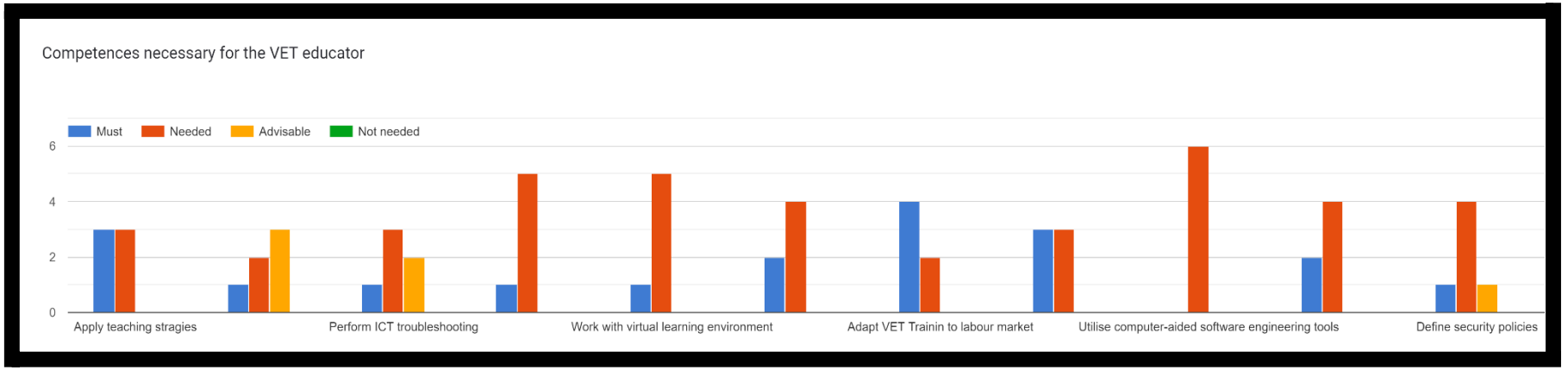
Los formadores deben tener un amplio conocimiento del contenido básico para poder responder a las preguntas que puedan surgir. Si un profesional no sabe la respuesta a una pregunta, es fundamental que declare que no la conoce pero que la investigará y le informará. Los profesionales no deben dar información falsa ni inventar respuestas en aras del bienestar y la comprensión de los participantes. Es responsabilidad del formador investigar, encontrar respuestas y hacer un seguimiento de los participantes para asegurarse de que reciben información precisa.

¿Quiere saber más sobre lo que puede hacer un profesor al tratar el tema?

A continuación se presentan ejemplos de los conocimientos, habilidades y actitudes adecuados que debe poseer un formador eficaz según los socios del consorcio.







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

Actividad: Como profesor/formador, ¿cuáles son algunos ejemplos de tus conocimientos, habilidades y actitudes? Rellena los espacios en blanco del cuadro. Se da un ejemplo.

Ejemplo de conocimiento	Ejemplo de habilidad	Ejemplo de actitud
Estoy familiarizado con la ciberseguridad y las tecnologías emergentes.	Puedo desarrollar materiales educativos digitales y adaptar la enseñanza al grupo objetivo.	Me apasiona hacer que las sesiones sean lo más eficaces posible para nuestros participantes, y me comprometo a hacerlo.

- **Conocimiento**: Resultado de la asimilación de información a través del aprendizaje. El conocimiento es el conjunto de hechos, principios, teorías y prácticas relacionados con un campo de estudio o trabajo.

- **habilidad**: Capacidad para aplicar los conocimientos y utilizar el saber hacer para completar tareas y resolver problemas.

- **Competencia**: Capacidad de aplicar adecuadamente los resultados del aprendizaje en un contexto definido (educación, trabajo, desarrollo personal o profesional. [7]

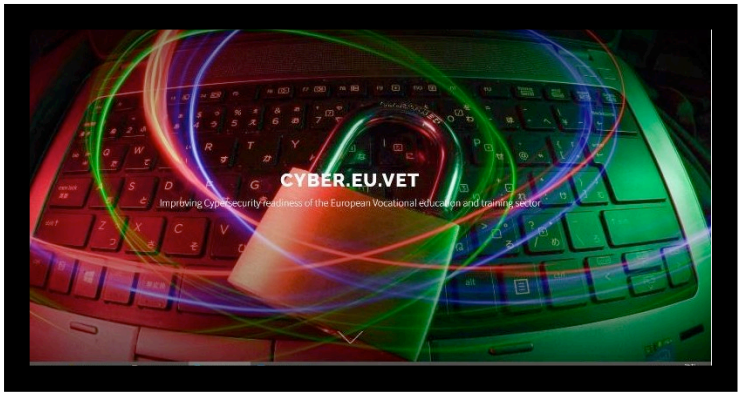
[7] El Marco Europeo de Cualificaciones para el Aprendizaje Permanente (MEC)

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

Volver al contenido

II. El sitio web CYBER.EU.VET

El consorcio del proyecto creó desde el primer paso del proyecto un sitio web dedicado desarrollado con tecnologías de código abierto (Wordpress) y un enfoque modular, que puede permitir a nuevos socios de diferentes países añadir y gestionar sus propios contenidos (una vez aceptados los términos de las condiciones establecidas por los socios del proyecto). Las plataformas digitales como CYBER.EU.VET one pueden abrirse de dos maneras para promover la innovación y la generación de valor (Boudreau 2010) .



Por supuesto, las plataformas digitales, y en este caso concreto la plataforma concebida como Recurso Educativo Abierto, pueden ser explotadas posteriormente para actividades de seguimiento. Este nuevo sistema permite relacionar el mundo físico tradicional con una interfaz digital capaz de conectar y organizar la demanda y la oferta de una herramienta o un servicio en un único espacio 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 crean redes que conectan personas y servicios a lo largo del tiempo.

La integridad de la red está vinculada no sólo a los factores de la infraestructura de información, su seguridad y el flujo de datos dentro de la red, sino también a los cambios sociales y ambientales que interfieren en los componentes humanos.

Por ello, se ha organizado una campaña de eventos multiplicadores para difundir y publicitar las herramientas tecnológicas y el manual CYBER.EUY.VET desarrollados.

Esta campaña tenía también el objetivo de aumentar la concienciación entre los profesores de FP, los estudiantes y sus familiares sobre la importancia de reconocer estos riesgos diarios, que pueden tener un impacto tanto económico como social en todos los ciudadanos europeos.

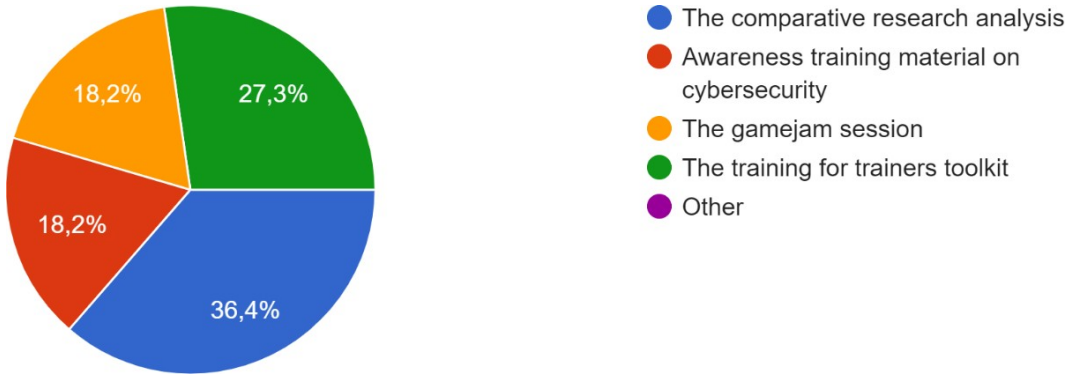
Los sistemas de TIC aprovechan el emergente "efecto red" combinando los medios sociales abiertos en línea, la creación de conocimiento distribuido y los datos de entornos reales **para crear conciencia de los problemas y las posibles soluciones solicitando esfuerzos colectivos, permitiendo nuevas formas de innovación social.**

III. "Una visión práctica"

Los socios y profesionales que han participado en el proyecto CYBER.EU.VET afirman haber beneficiado sus objetivos de investigación con una mejor comprensión de la percepción de los estudiantes de ciberseguridad en el contexto local y europeo. Los intercambios entre partes interesadas tan diferentes entre sí han sido una oportunidad para obtener diferentes perspectivas y enfoques de los problemas compartidos y para aprender a traducirlos a un lenguaje más común. En palabras de nuestro socio *"Ha sido muy beneficioso conocer el estado actual de la técnica en materia de ciberseguridad y las principales amenazas cibernéticas en los países socios. También es interesante conocer y poder seguir las tendencias en cuanto a ciberataques que parecen ser muy similares en cada país"*. El 81,8% de los socios declararon que tienen la intención de utilizar el material compartido o creado dentro del proyecto CYBER.VET.EU en el futuro, el 36,4% a nivel local, el 36,4% a nivel nacional y el 27,3% a nivel internacional, a través de sesiones de formación y talleres, foros y, por supuesto, medios de comunicación social.

El contexto de los países participantes en el proyecto es muy diferente entre sí, aunque como países europeos comparten ciertas similitudes. La ciberseguridad es muy cambiante ya que las amenazas son diferentes a lo largo del tiempo. Por ello, es interesante que los resultados obtenidos sean actualizados tanto por los formadores como por los investigadores para que sean válidos en el momento en que se utilicen.

Es significativo el gráfico que muestra qué herramientas compartidas fueron más útiles para los operadores de los diferentes servicios de los 8 socios del consorcio:



IV. A final note

El manual CYBER.EU.VET ha sido concebido para ayudar a los formadores de EFP y a los profesionales del sector digital a utilizar las herramientas de ciberseguridad, así como las instrucciones sobre cómo utilizar el material de CYBER.EU.VET que figura en el apéndice. Ofrece sugerencias sobre cómo organizar la formación, así como recomendaciones operativas para que los profesionales puedan proporcionar a los estudiantes los conocimientos y las herramientas que necesitan para reconocer las amenazas a la ciberseguridad. Este libro electrónico ha sido diseñado en beneficio de los profesores de EFP, los estudiantes de EFP, las familias de los estudiantes y las instituciones de EFP a nivel internacional o local. Pueden beneficiarse de él los profesionales (o trabajadores/gestores de casos) que imparten formación y orientación, los supervisores o los coordinadores de formación, y quienes imparten orientación, como los voluntarios, los becarios, otro personal de apoyo al reasentamiento, otros proveedores de servicios y los miembros de la comunidad. Una mayor concienciación sobre los riesgos causados por los fraudes de datos, el malware y otras amenazas a la seguridad en línea, a todos los niveles, desde la dirección del centro de FP hasta las familias del estudiante, son pasos fundamentales para defender a los ciudadanos de la UE de los daños causados por las amenazas a la ciberseguridad, en un momento ya caracterizado por una crisis de época.

Este libro electrónico contiene varias sugerencias que esperamos impulsen a los profesores y profesionales de la EFP a replantearse los objetivos de su formación y cómo podrían mejorar la calidad de la educación, desarrollando formas innovadoras de aprendizaje electrónico.

e) Anexos

I. Glosarios

II. Guía del usuario de CYBER.EU.VET - guía de orientación para futuras implementaciones

I. GLOSARIO

DATOS

Una secuencia de uno o más símbolos a los que se les da un significado mediante un acto o actos específicos de interpretación (los datos no tienen un significado intrínseco). Los datos pueden analizarse o utilizarse para obtener conocimientos o tomar decisiones. Los datos digitales se representan mediante el sistema numérico binario de unos (1) y ceros (0), a diferencia de su representación analógica. [8]

COMUNICACIÓN DIGITAL

Comunicación que utiliza la tecnología digital. Existen varios modos de comunicación, por ejemplo, la comunicación sincrónica (comunicación en tiempo real, por ejemplo, mediante skype o videochat o Bluetooth) y la asincrónica (comunicación no concurrente, por ejemplo, correo electrónico, sms) utilizando, por ejemplo, los modos uno-a-uno, uno-a-muchos o muchos-a-muchos.[9]

COMPETENCIA DIGITAL

La competencia digital puede definirse en términos generales como el uso seguro, crítico y creativo de las TIC para alcanzar objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el ocio, la inclusión y/o la participación en la sociedad.[10]

CONTENIDO DIGITAL

Cualquier tipo de contenido que exista en forma de datos digitales codificados en un formato legible por máquina y que pueda ser creado, visualizado, distribuido, modificado y almacenado utilizando tecnologías digitales. Algunos ejemplos de contenidos digitales son: páginas web y sitios web, redes sociales, datos y bases de datos, audio digital, como mp3, y libros electrónicos, imágenes digitales, vídeo digital, videojuegos, programas informáticos y software. En el marco de DigCompEdu, los contenidos digitales se dividen en recursos y datos digitales.[11]

ENTORNO DIGITAL

un contexto, o un "lugar", habilitado por la tecnología y los dispositivos digitales, que a menudo se transmite a través de Internet u otros medios digitales, por ejemplo, la red de telefonía móvil. Los registros y pruebas de la interacción de un individuo con un entorno digital constituyen su huella digital. En DigComp, el término entorno digital se utiliza como telón de fondo de las acciones digitales sin nombrar una tecnología o herramienta específica.

SERVICIO DIGITAL

permite a un usuario (ciudadano, consumidor) crear, procesar, almacenar o acceder a datos en forma digital y compartir o interactuar con datos en forma digital cargados o creados por el mismo u otros usuarios de ese servicio (Directiva (UE) 2019/770).

---

[8] Modificado de: es.wikipedia.org/wiki/Data_(computing)

[9] Fuente: Marco DigComp https://ec.europa.eu/jrc/digcomp

[10] *Ibidem*

[11] Redecker, C. Marco europeo para la competencia digital de los educadores: DigCompEdu. Punie, Y. (ed). EUR 28775 ES. Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2017, ISBN 978-92-79-73494-6, doi:10.2760/159770, JRC107466

TECNOLOGÍA DIGITAL

Cualquier producto que pueda utilizarse para crear, ver, distribuir, modificar, almacenar, recuperar, transmitir y recibir información de forma electrónica en formato digital. Por ejemplo, ordenadores y dispositivos personales (por ejemplo, un ordenador de sobremesa, un portátil, un netbook, una tableta, teléfonos inteligentes, PDA con funciones de telefonía móvil, consolas de juegos, reproductores multimedia, lectores de libros electrónicos), televisión digital, robots.[12]

HERRAMIENTAS DIGITALES

Tecnologías digitales utilizadas para un fin determinado o para llevar a cabo una función concreta de, por ejemplo, tratamiento de la información, comunicación, creación de contenidos, seguridad o resolución de problemas.[13]

CONTENIDO EDUCATIVO

Contenido (digital) relevante, de un modo u otro, para el contexto educativo. Este término es más amplio que el de "recurso educativo" en el sentido de que también comprende los contenidos marginales al proceso de enseñanza, por ejemplo, la comunicación con los alumnos, los padres, los colegas; los contenidos administrativos, etc.[14]

RECURSOS EDUCATIVOS

Recursos (digitales o no) diseñados y destinados a ser utilizados con fines educativos.[15]

ALFABETIZACIÓN MEDIÁTICA

se refiere a las habilidades, los conocimientos y la comprensión que permiten a los ciudadanos utilizar los medios de comunicación de forma eficaz y segura. Para que los ciudadanos puedan acceder a la información y utilizar, evaluar críticamente y crear contenidos de los medios de comunicación de forma responsable y segura, deben poseer competencias avanzadas en materia de alfabetización mediática. La alfabetización mediática no debe limitarse a aprender sobre las herramientas y las tecnologías, sino que debe tener como objetivo dotar a los ciudadanos de las habilidades de pensamiento crítico necesarias para ejercer el juicio, analizar realidades complejas y reconocer la diferencia entre la opinión y los hechos. [16]

RECURSOS EDUCATIVOS ABIERTOS

Materiales de enseñanza, aprendizaje e investigación en cualquier medio, digital o no, que son de dominio público o que han sido liberados bajo una licencia abierta que permite el acceso, uso, adaptación y redistribución sin costo por parte de otros sin restricciones o con restricciones limitadas. [17]

AUTOEVALUACIÓN

La autoevaluación implica la capacidad de juzgar de forma realista el propio rendimiento. Los defensores de la autoevaluación sugieren que tiene muchas ventajas, por ejemplo: proporciona una retroalimentación oportuna y eficaz y permite a los estudiantes evaluar su propio aprendizaje rápidamente; permite a los instructores entender y proporcionar una retroalimentación rápida sobre el aprendizaje; promueve la integridad académica a través de la autoinformación de los estudiantes sobre el progreso del aprendizaje; promueve las habilidades de la práctica reflexiva y el autocontrol; desarrolla el aprendizaje autorregulado; aumenta la motivación de los estudiantes; mejora la satisfacción de participar en un entorno de aprendizaje colaborativo; ayuda a los estudiantes a desarrollar una serie de habilidades personales y transferibles para satisfacer las expectativas de los futuros empleadores.[18]

---

[12] Modificado de la fuente: http://www.tutor2u.net/business/ict/intro_what_is_ict.htm

[13] *Ibidem*

[14] *Ibidem*

[15] *Ibidem*

[16] Fuente: la Directiva de Servicios de Medios Audiovisuales de la UE (2018)

[17] Fuente: Definición de la UNESCO http://www.unesco.org/new/en/communication-and-information/access-to-knowledge/open-educational-resources/what-are-open-educational-resources-oers/

[18] Fuente: Centro de Excelencia Docente de la Universidad de Cornell http://www.cte.cornell.edu/

INCLUSIÓN SOCIAL Proceso de mejora de las condiciones de participación en la sociedad de individuos y grupos (por el Banco Mundial). La inclusión social pretende capacitar a las personas pobres y marginadas para que aprovechen las florecientes oportunidades globales. Garantiza que las personas tengan voz en las decisiones que afectan a sus vidas y que disfruten de un acceso igualitario a los mercados, los servicios y los espacios políticos, sociales y físicos.[19]

ENTORNO ESTRUCTURADO
donde los datos residen en un campo fijo dentro de un registro o archivo, por ejemplo, bases de datos relacionales y hojas de cálculo. La respuesta/solución tecnológica se refiere al intento de utilizar la tecnología (y/o la ingeniería) para resolver un problema.

Referencias

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
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: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use. Publica-tions Office of the European Union. 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 (accessed on 3rd July, 2021).

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

European Commission. (2022). Translations of DigComp 2.0 in the European Skills, Competences and Occupa-tions classification (ESCO). Publications Office of the Eu-ropean Union. DOI:10.2767/316971

[19] Fuente: Marco DigComp https://ec.europa.eu/jrc/digcomp

European Union. (2018). Council Recommenda-tion of 22 May 2018 on key competences for lifelong learning (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 anal-ysis of frameworks. Publications Office of the European Union.

https://data.europa.eu/doi/10.2791/82116

Ferrari, A. (2013). DIGCOMP: A framework for developing and understanding digital competence in Europe. Publi-cations Office. 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). Understand-ing 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).

Government of Latvia, (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. Publications Office of the European Union. 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, Publications Office of the European Union, Luxembourg

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

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

OECD. (2014). Assessing problem-solving skills in PISA 2012. In PISA 2012 Results: Creative Problem Solv-ing (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 Conceptu-al Reference Model. Publications Office of the European Union. https://publications.jrc.ec.europa.eu/repository/handle/JRC101254

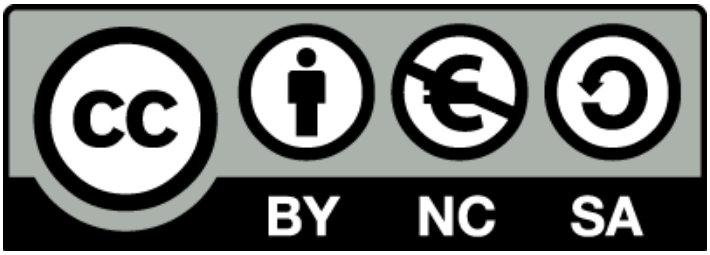
YBER.VET.EU

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

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.

Es posible seguir el documento a través del siguiente código QR :



Volver al contenido ↑