LINKS

Co-funded by the European Union

El marco de competencias de la soberanía digital

Co-funded by
the European Union

Este proyecto cuenta con el apoyo de la Comisión Europea a través del programa Erasmus+. Esta publicación refleja únicamente las opiniones del autor y la Comisión no se hace responsable del uso que pueda hacerse de la información aquí difundida.

Más información sobre

LINKS

Índice

Introducción

El proyecto LINKS tiene como objetivo apoyar a los trabajadores en el ámbito de la juventud europea para que logren su propia soberanía de datos y mejoren sus habilidades de seguridad digital a través de una nueva e innovadora forma de contenido formativo en apoyo de la creación de competencias digitales.

Durante las fases iniciales de planificación de este proyecto y aplicación, el análisis de las necesidades respaldó el hecho de que en la actualidad no existe un único marco de competencias de soberanía y seguridad digitales para Europa.

El DigComp (Marco de Competencia Digital) hace referencia a muchas de las habilidades y competencias básicas generales relacionadas con la seguridad digital en su conjunto, y este resultado hará referencia a este marco de competencia existente, pero está dirigido específicamente a la concienciación proactiva de los trabajadores en el ámbito de la juventud de toda Europa sobre las amenazas a la seguridad digital que existen actualmente.

El marco de competencias en materia de soberanía digital define los componentes clave de las competencias que necesitan los trabajadores en el ámbito de la juventud para integrar eficazmente la soberanía digital y los protocolos de seguridad en sus contextos localizados, así como para proporcionar y validar un marco de referencia de la UE para desarrollar y evaluar las competencias en materia de seguridad digital. Las competencias en seguridad digital están estrechamente vinculadas a las competencias digitales genéricas y no se consideran competencias por derecho propio.

El marco está dirigido a los trabajadores en el ámbito de la juventud, pero también es relevante y de interés para los profesores y formadores de TIC en activo y en formación, así como para los responsables de las políticas educativas y de aprendizaje permanente, en relación con la mejora de las competencias tecnológicas y el desarrollo de las capacidades de las personas.

Esperamos que las ONG de formación digital y las organizaciones de formación de toda Europa adopten este marco como parte de sus actividades educativas de evaluación y enseñanza, lo que, a largo plazo, aumentará la concienciación y fomentará la integración del marco en los organismos educativos digitales locales, regionales y nacionales de los países europeos.

Resultados de la encuesta y los grupos de discusión del proyecto

El Marco de Competencias de Soberanía Digital se basa en la metodología y los resultados de la encuesta y los grupos de discusión del proyecto. También pretende alinearse con el Marco DigComp, que apoya la explotación y la sostenibilidad a largo plazo como un marco de competencias adicional y específico del grupo destinatario.

La encuesta del proyecto ayudó a conocer el uso de la tecnología y la protección de datos en las prácticas de trabajo digital de los trabajadores en el ámbito de la juventud. Los trabajadores en el ámbito de la juventud necesitan una mayor concienciación combinada con una buena gestión de las identidades digitales, ya que puede ayudar a limitar los sucesos causados por la "falta de atención" del usuario o de la propia organización. Escribieron sobre la necesidad de establecer y comunicar políticas de seguridad en el trabajo a distancia, sobre la regulación del uso de dispositivos personales, la seguridad de los canales de comunicación y colaboración y la necesidad de proporcionar un soporte informático vigilante. Recomendaron poner cursos a disposición de más miembros del personal y de los jóvenes, utilizar ejemplos más pertinentes en relación con tareas específicas, mejorar la creación de redes y compartir buenas y malas experiencias en línea. Es importante mantenerse al día y, en particular, con los nuevos documentos de la UE.

La mayoría de los trabajadores en el ámbito de la juventud no han recibido formación específica, toman decisiones sobre la seguridad en línea basándose en sus propios conocimientos. Escriben que es necesario profundizar en estos aspectos para la seguridad de las organizaciones y de los usuarios privados y organizar una formación especial para los responsables de la protección de datos.

Necesidad del marco de competencias de soberanía digital

Cada vez preocupa más que los ciudadanos, las empresas y los Estados miembros de la Unión Europea estén perdiendo gradualmente el control sobre sus datos, su capacidad de innovación y su capacidad para configurar y aplicar la legislación en el entorno digital. En este contexto, ha ido creciendo el apoyo a un nuevo enfoque político destinado a reforzar la autonomía estratégica de Europa en el ámbito digital.

Las empresas tecnológicas están recopilando cantidades ingentes de datos personales, y en la UE ha crecido la preocupación por la forma en que los ciudadanos europeos pueden recuperar el control de sus datos digitales en un entorno en línea que ahora está dominado principalmente por empresas tecnológicas no pertenecientes a la UE.

A medida que el trabajo con jóvenes se adapta cada vez más al mundo digital, vemos que los trabajadores en este ámbito también adoptan nuevos enfoques. Aunque lo digital es nuevo y apasionante, y ofrece innumerables oportunidades, no obstante exige una mejor comprensión en el contexto del trabajo con jóvenes. Se requieren más acciones para trazar un mapa de las prácticas, plataformas, herramientas y marcos de aprendizaje existentes en el trabajo juvenil digital en lo que respecta a las competencias de soberanía digital.

La soberanía digital es un concepto nuevo en la era digital, entendido comúnmente como "la capacidad de los individuos de poseer sus datos privados y controlar su uso".

La pandemia de COVID-19 ha tenido enormes efectos en la vida cotidiana de la mayoría de las personas. En respuesta, la tecnología se ha adaptado para intentar mitigar estos efectos, ofreciendo a los individuos alternativas digitales a muchas de las actividades cotidianas que ya no pueden realizarse normalmente. La socialización virtual y los eventos en línea se han convertido en algo habitual y han contribuido en gran medida a que las personas no estén completamente aisladas mientras permanecen encerradas.

La educación en línea también se ha convertido en la nueva normalidad en muchos lugares, ya que las escuelas y universidades recurren a las clases en línea para mantener la educación de los estudiantes en el buen camino. Además, como las personas tienen horarios más flexibles, o más tiempo libre durante el encierro, se ha producido un aumento significativo del número de personas que hacen uso de herramientas personales de aprendizaje y desarrollo, como las aplicaciones de aprendizaje de idiomas. La sanidad también se ha volcado en las soluciones digitales, y cada vez es más habitual que la atención sanitaria física y mental esté disponible en línea, lo que ha contribuido con bastante éxito a mitigar los efectos negativos de la reducción

Marcos pertinentes existentes

Se han desarrollado varios marcos de competencias pedagógicas digitales para apoyar el desarrollo profesional efectivo y significativo, basado en criterios, de las competencias pedagógicas digitales de los profesores profesionales.

Los marcos europeos publicados en los últimos años describen cómo debería ser una organización educativa digitalmente competente DigCompOrg y un profesorado digitalmente competente DigCompEdu, animando a las organizaciones a garantizar las competencias de su personal y a desarrollar soluciones nacionales para garantizar la competencia digital.

DigCompEdu es un marco de competencia digital y sus principales destinatarios son los profesores universitarios y los miembros del personal.
El marco DigComp identifica los componentes clave de la competencia digital en cinco áreas:

1. Conocimientos básicos de información y datos: Articular las necesidades de información, localizar y recuperar datos, información y contenidos digitales. Juzgar la pertinencia de la fuente y su contenido. Almacenar, gestionar y organizar datos, información y contenidos digitales.
2. Comunicación y colaboración: Interactuar, comunicarse y colaborar a través de las tecnologías digitales siendo conscientes de la diversidad cultural y generacional. Participar en la sociedad a través de los servicios digitales públicos y privados y la ciudadanía participativa. Gestionar la propia presencia, identidad y reputación digitales.
3. Creación de contenidos digitales:Crear y editar contenidos digitales, Mejorar e integrar la información y los contenidos en un corpus de conocimientos existente, comprendiendo al mismo tiempo cómo deben aplicarse los derechos de autor y las licencias. Saber dar instrucciones comprensibles para un sistema informático.
4. Seguridad: Proteger los dispositivos, los contenidos, los datos personales y la intimidad en los entornos digitales. Proteger la salud física y psicológica, y ser conscientes de las tecnologías digitales para el bienestar social y la inclusión social. Ser conscientes del impacto medioambiental de las tecnologías digitales y de su uso.
5. Solución de problemas: Identificar necesidades y problemas, y resolver problemas conceptuales y situaciones problemáticas en entornos digitales. Utilizar herramientas digitales para innovar procesos y productos. Mantenerse al día de la evolución digital.

Existe un modelo de referencia conceptual DigComp en el que 21 competencias son pertinentes para estas áreas. Otras dimensiones describen niveles de competencia, conocimientos, habilidades y actitudes, así como casos de uso.

El Marco de Competencias de Soberanía Digital para trabajadores en el ámbito de la juventud

Basándose en el estudio y análisis de los marcos existentes, los socios de este proyecto decidieron centrarse en cuatro temas de seguridad de DigiComp y añadir también competencias necesarias especialmente para los trabajadores en el ámbito de la juventud. Estas son las competencias del marco DigiComp:

4.1 Protección de dispositivos

Proteger los dispositivos y contenidos digitales, y comprender los riesgos y amenazas en los entornos digitales. Conocer las medidas de seguridad y protección y tener debidamente en cuenta la fiabilidad y la privacidad.

4.2 Protección de los datos personales y la intimidad

Proteger los datos personales y la intimidad en entornos digitales. Comprender cómo utilizar y compartir la información personal identificable, protegiéndose a sí mismo y a los demás de posibles daños. Comprender que los servicios digitales utilizan una "política de privacidad" para informar sobre cómo se utilizan los datos personales.

4.3 Proteger la salud y el bienestar

Ser capaz de evitar los riesgos para la salud y las amenazas para el bienestar físico y psicológico durante el uso de las tecnologías digitales. Ser capaz de protegerse a sí mismo y a los demás de posibles peligros en entornos digitales (por ejemplo, el ciberacoso). Conocer las tecnologías digitales para el bienestar social y la inclusión social..

4.4 Proteger el medio ambiente

Ser conscientes del impacto medioambiental de las tecnologías digitales y de su uso.

https://joint-research-centre.ec.europa.eu/digcomp/digital-competence-framework_en#ref-4-safety_

A la hora de definir las competencias digitales básicas para los trabajadores en el ámbito de la juventud, resulta útil pensar tanto en las características universales (competencias DigComp para los ciudadanos) como en las específicas (actividades cotidianas en el trabajo con jóvenes) del aprendizaje práctico resultante.

Competencias para la protección de los datos personales y la intimidad

*competencias técnicas en tecnologías digitales,
* la capacidad de utilizar las tecnologías digitales de forma significativa para trabajar, estudiar y otras actividades cotidianas,
* la capacidad de evaluar críticamente las tecnologías digitales;
* conocer las normas básicas relativas a la seguridad en línea;
* Comprender cómo funciona Internet;
* comprender qué es el marketing electrónico y cómo funciona;
* comprender la privacidad y ser consciente de los derechos de propiedad intelectual;
* saber cómo aplicar las medidas de seguridad;
* desarrollar la autoeficacia en el uso de las tecnologías digitales.

Competencias para los dispositivos que deben protegerse

Proteger el ordenador y el smartphone con programas de seguridad potentes y actualizados. Si el ordenador o el teléfono están infectados con software malicioso, las demás medidas de protección no sirven de mucho, porque los delincuentes pueden poseer ya la clave de todas las acciones en línea. También es importante asegurarse de que las actualizaciones del sistema operativo están instaladas. Los trabajadores en el ámbito de la juventud deben cuidar todos sus dispositivos. Deben estar actualizados, con un software antivirus eficaz. Varios fabricantes lanzan actualizaciones que no sólo mejoran las funciones, sino que también corrigen cualquier fallo de seguridad que pueda poner los dispositivos
en peligro. Como norma general de seguridad, es aconsejable no utilizar ningún otro ordenador o dispositivo para actividades que requieran "iniciar sesión" en alguno de los servicios que se utilizan.

Aprender a detectar el spam y las estafas

Aunque algunos son fáciles de identificar, otros intentos de phishing en un correo electrónico, en las redes sociales o en sitios web pueden parecer muy legítimos. La única forma de no caer nunca en una estafa de phishing es no hacer nunca clic en un enlace enviado. Si el correo electrónico dice que es de un banco y tiene todos los logotipos correctos y conoce el nombre, puede que sea del banco real o puede que no. En lugar de utilizar el enlace proporcionado, encontrar el sitio web y utilizar un motor de búsqueda puede ayudar a prevenir la estafa. De este modo, el usuario sabrá si ha aterrizado en el sitio legítimo y no en un sitio falso simulado.

Utilizar sitios web fiables para comprar

Si un usuario no conoce la reputación de una empresa a la que quiere comprar, es importante que estudie el sitio antes de hacerlo. Pregunte: "¿Qué opinión tienen de otros usuarios?".¿Utilizan una conexión segura y encriptada para la información personal y financiera?".

Mantenerse alerta

Desconfiar del WiFi público y pensárselo dos veces antes de entrar en una red no segura. Existen herramientas que pueden ayudar a un usuario a tener más privacidad y blindar durante la navegación la actividad de otros usuarios y de los propios sitios web en redes WiFi públicas.

Seguridad en la red

El mundo en línea se ha convertido en un entorno que cambia tan rápidamente que los consejos de hoy pueden quedar obsoletos mañana. Los trabajadores en el ámbito de la juventud deben ser conscientes de que el contenido que consumen (y a veces puede ser realmente mucho) debe filtrarse. Es importante desconfiar un poco. Es relativamente fácil falsificar cosas en Internet. Es muy fácil poner en Internet algo que no es del todo cierto, o simplemente un montón de mentiras. Debemos tener mucho cuidado de no creer en todo lo que vemos y leemos en Internet. Como buen consejo, deberíamos indagar más para distinguir qué es verdad y qué no lo es en caso de que tengamos la más mínima duda sobre algo. Intentemos ser críticos con las cosas online y así minimizaremos el riesgo que conlleva cualquier actividad online.

Compartir información en las redes sociales

“Compartir información describe el intercambio de datos entre varias organizaciones, personas y tecnologías" (Techopedia). Hay varios tipos de intercambio de información:

- Información compartida por particulares (como un vídeo compartido en Facebook o YouTube);
- Información compartida por organizaciones (como el canal RSS de un informe meteorológico en línea);
- Información compartida entre firmware/software (como las direcciones IP de los nodos de red disponibles o la disponibilidad de espacio en disco).

Todas las redes sociales (o la mayoría de ellas) permiten a los usuarios crear perfiles tan detallados como deseen. En algunos casos, este procedimiento ayuda a los usuarios a encontrar a otros usuarios con intereses comunes, etc. En redes sociales como Facebook, es posible cambiar la configuración de privacidad para controlar qué información es pública y qué información se guarda sólo para los "amigos". Sin embargo, es importante saber que la propia red social dispone de esta información independientemente de la configuración de privacidad.

Normalmente la gente comparte edad, sexo, familia, otros intereses, formación académica y detalles relacionados con el propio empleo. Publicar fotos o "estados" es una forma rápida de mostrar sentimientos, situaciones y compartir información. La mayoría de las redes sociales están diseñadas para conseguirlo de la forma más rápida posible. Ser consciente de qué cosas comparte un usuario es realmente importante. Compartir expone la información que permite a los anunciantes rastrear las preferencias y gustos de los consumidores potenciales.

GDPR

El GDPR se aplicó a todos los miembros de la UE y del EEE a partir del 25 de mayo de 2018. Ha sustituido a la legislación actual en materia de privacidad en los países miembros actualmente sujetos a la Directiva 95/46 de la UE. El GDPR es más detallado y preciso en determinados ámbitos, y tiene en cuenta los retos que plantea un mundo digital en rápida evolución, lo que da lugar a riesgos para la privacidad de los interesados.

Referencias

Protección de datos y privacidad en línea
https://europa.eu/youreurope/citizens/consumers/internet-telecoms/dataprotection-online-privacy/i ndex_en.htm
Techopedia https://www.techopedia.com/definition/24839/information-sharing
Instrucciones paso a paso para configurar el ordenador y crear un usuario
https://www.wikihow.com/Use-a-Computer
Protección de datos
https://www.privacyrights.org/consumer-guides/social-networking-privacy-how-be-safe-secure-and -social