Aumentar la resiliencia digital
Manual y metodología

Aumentar la resiliencia digital haciendo accesibles a todos el bienestar y la seguridad digitales

2022-2-SK01-KA220-ADU-000096888

Co-funded by the European Union

Erasmus+ proyecto KA220 Asociaciones de cooperación en educación de adultos

Aumentar la resiliencia digital haciendo accesibles a todos el bienestar y la seguridad digitales

2022-2-SK01-KA220-ADU-000096888

DigiWELL

Aumentar la resiliencia digital
Manual y metodología

Septiembre, 2023

Esta publicación fue preparada como resultado del Proyecto “Aumentar la resiliencia digital haciendo accesibles a todos el bienestar y la seguridad digitales” (Proyecto No: 2022-2-SK01-KA220-ADU-000096888), que se implementa en el marco de la Erasmus+ KA220 Asociaciones de cooperación en educación de adultos.

DigiWELL Consorcio

Slovak University of Agriculture in Nitra, Slovakia

Muğla Sıtkı Koçman University, Turkey

Czech technical university in Prague, Czech

Innovation, Training, and Employment Association for Sustainable Development (AIFED), Spain

European Institute for Innovation – Technology (EIfI-Tech), Germany

Foundation Maker's Place Private Company (Found.ation), Greece

Syzigia Skopje Foundation (SYZYGY), Macedonia

Faculty of Economics and Management
Slovak University of Agriculture in Nitra |
Tr. Andreja Hlinku 2 | 949 76 Nitra | Slovakia | email: digiwell@uniag.sk

Website: www.digiwell.sk

Descargo de responsabilidad:

"Cofinanciado por el Programa Erasmus+ de la Unión Europea. Esta publicación refleja únicamente las opiniones de los contribuyentes, y la Comisión Europea y la Asociación Académica Eslovaca para la Cooperación Internacional no se hacen responsables del uso que pueda hacerse de la información contenida en ella."

Paquete de trabajo 2: **Aumentar la resiliencia digital Manual y metodología**

Lista de colaboradores: *Murat Sümer, Czech Technical University,*

David Vaneček, Czech Technical University,

Martina Hanová, Slovak University of Agriculture in Nitra, Slovakia

Marcela Hallová, Slovak University of Agriculture in Nitra, Slovakia

Eva Oláhová, Slovak University of Agriculture in Nitra, Slovakia

Eyüp Şen, Muğla Sıtkı Koçman University, Turkey

İlker Yorulmaz, Muğla Sıtkı Koçman University, Turkey

Maria Martinez, AIFED, Spain

Jesus de Haro Martinez, AIFED, Spain

Chris Ashe, Elfl-Tech, Germany

Mattia Ferrari, Elfl-Tech, Germany

Maria Kandilioti, Found.ation, Greece

Roula Mourmouri, Found.ation, Greece

Suzana Trajkovska, SYZYGY, Macedonia

Aleksandar Kochankovski, SYZYGY, Macedonia

Contenido

Resumen

Tras la pandemia del COVID-19, algunas necesidades se han vuelto vitales debido al uso de las tecnologías digitales e internet, que están muy presentes en nuestras vidas. La más importante de ellas es poder realizar transacciones seguras en el mundo digital sin sufrir daños. Especialmente los adultos necesitan medidas de seguridad digital y algunas competencias para protegerse de las ciberamenazas. Además, internet y las tecnologías digitales no sólo facilitan la vida, sino que también crean algunos problemas psicológicos negativos. Por ejemplo, el ciberacoso se ha convertido en un problema difícil de abordar. En consecuencia, garantizar el bienestar en el mundo digital se ha convertido en una necesidad en las condiciones actuales. De nuevo, en relación con esta cuestión, el creciente uso de la tecnología digital y el punto alcanzado por la transformación digital han traído a la agenda de la gente algunos problemas como la fatiga digital.

En este sentido, el proyecto DigiWELL pretende incorporar los principios del bienestar digital a la educación de adultos. Sus iniciativas pretenden contribuir a las prácticas generales de las organizaciones, redes e iniciativas de educación de adultos. El proyecto entiende lo crucial que es abordar cómo la tecnología está afectando a la salud mental, la productividad y el bienestar general de los adultos en la era digital. El principal objetivo de DigiWELL es proporcionar a los estudiantes adultos la información, las habilidades y los recursos necesarios para navegar ética y conscientemente por el mundo digital. El proyecto DigiWELL también implica la creación y ejecución de otras iniciativas de capacitación de estudiantes adultos. El objetivo de estas actividades es proporcionar un entorno de apoyo en el que los adultos puedan compartir sus experiencias, dificultades y triunfos en la promoción del bienestar digital. Con esto en mente, el proyecto DigiWELL presenta muchas oportunidades para que los individuos y las organizaciones de adultos tomen conciencia e ilustren sobre la importancia del bienestar digital y sobre cómo promover el bienestar digital de los individuos adultos y de los educadores y formadores de adultos. Facilitar el bienestar digital con un enfoque holístico es mucho más posible si todas las partes relevantes toman medidas para apoyar las necesidades de bienestar digital de los individuos. En consecuencia, la información, los consejos y las buenas prácticas que se presentan en este manual invitan a las personas y a las organizaciones interesadas a tomar iniciativas para que más de nosotros tengamos un mejor bienestar digital y también vidas digitales más fuertes.

1 Introducción

1.1 Objetivo del método y Manuel

- Contribuir a que el bienestar digital y la seguridad digital sean accesibles para todos fomentando e informando a los adultos sobre el bienestar digital y la seguridad digital y las competencias necesarias para ello.
- Introducir la resiliencia digital, el bienestar digital y la seguridad digital, el marco terminológico y las mejores prácticas de bienestar digital y seguridad digital entre todas las personas.
- Garantizar la multiculturalidad, adaptando los resultados desarrollados a las organizaciones pertinentes de los países socios.

1.2 Marco DigComp de la UE

En DigComp, la competencia digital implica el "uso seguro, crítico y responsable de las tecnologías digitales y la participación en ellas para el aprendizaje, el trabajo y la participación en la sociedad. Se define como una combinación de conocimientos, habilidades y actitudes". (Recomendación del Consejo sobre las competencias clave para el aprendizaje permanente, 2018).

El marco DigComp identifica los componentes clave de la competencia digital en 5 áreas. Las áreas se resumen a continuación:

Alfabetización informacional y de 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.

Comunicación y colaboración: Interactuar, comunicarse y colaborar a través de las tecnologías digitales teniendo en cuenta 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.

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.

Seguridad: Proteger los dispositivos, los contenidos, los datos personales y la privacidad 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.

Resolver 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.

Una de las competencias clave en el ámbito de la seguridad es la protección de la salud y el bienestar. Proteger la salud y el bienestar significa: (a) 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, (b) ser capaz de protegerse a uno mismo y a los demás de los posibles peligros en los entornos digitales (por ejemplo, el ciberacoso) y (c) ser consciente de las tecnologías digitales para el bienestar social y la inclusión social.

1.3 Por qué M&M es un buen recurso para los adultos

Como ya se ha mencionado, tras la pandemia del COVID-19, algunas necesidades se han vuelto vitales debido al uso de las tecnologías digitales e internet, que están muy presentes en nuestras vidas. La más importante de ellas es poder realizar transacciones seguras en el mundo digital sin sufrir daños. Especialmente los adultos necesitan medidas de seguridad digital y algunas competencias para protegerse de las ciberamenazas. Además, internet y las tecnologías digitales no sólo facilitan la vida, sino que también crean algunos problemas psicológicos negativos. Por ejemplo, el ciberacoso se ha convertido en un problema difícil de abordar. En consecuencia, garantizar el bienestar en el mundo digital se ha convertido en una necesidad en las condiciones actuales. De nuevo, en relación con este tema, el creciente uso de la

tecnología digital y el punto alcanzado por la transformación digital han traído a la agenda de las personas algunos problemas como la fatiga digital.

Este manual utiliza tantos ejemplos del mundo real como es posible y deja que los alumnos adultos descubran algunos conceptos por sí mismos para apoyar el aprendizaje de adultos basado en Knowles (1968).

1.4 Por qué M&M es un buen recurso para los formadores de adultos

La formación y la educación desempeñan un papel crucial en la concienciación sobre la seguridad digital, al dotar a las personas de los conocimientos, las capacidades y las mejores prácticas necesarias para protegerse a sí mismas y a sus organizaciones contra las ciberamenazas. Además, la formación y la educación para la seguridad digital son componentes esenciales de la creación de una sólida cultura de ciberseguridad. Mediante el diseño de programas de formación adaptados a las necesidades y funciones específicas se dota a los adultos de los conocimientos y habilidades necesarios para identificar y responder a las ciberamenazas con eficacia.

La formación ayuda a las personas a comprender los distintos tipos de ciberamenazas, como el phishing, el malware, la ingeniería social y el ransomware. Al reconocer estas amenazas, las personas pueden ser más vigilantes y precavidas al utilizar las plataformas digitales. La educación puede enseñar a las personas a identificar correos electrónicos, mensajes o sitios web de phishing. Aprenden a detectar elementos sospechosos y a evitar hacer clic en enlaces maliciosos o facilitar información sensible. Al mismo tiempo, la formación incluye directrices sobre la seguridad de los dispositivos móviles, su protección mediante contraseñas, el uso del cifrado y la precaución con las descargas de aplicaciones, al tiempo que garantiza que las personas conozcan las normativas de ciberseguridad pertinentes y los requisitos de cumplimiento, lo que ayuda a mantener las prácticas legales y éticas. Por último, a través de la educación, las personas comprenden que la ciberseguridad es una responsabilidad compartida y que la participación activa de todos es necesaria para mantener un entorno seguro, mientras que inculca buenos hábitos de ciberseguridad, animando a las personas a aplicar medidas de seguridad tanto en el trabajo como en su vida personal.

El proyecto DigiWELL pretende responder a las necesidades de seguridad digital y bienestar de los adultos que no han nacido en la era de Internet. Para ello, creará y desarrollará oportunidades de aprendizaje flexibles que respondan a las necesidades específicas de aprendizaje de los adultos. El proyecto se centrará en mejorar la resiliencia digital a través de un enfoque de aprendizaje combinado. Especialmente este manual contribuye al objetivo anterior, ya que crea una cultura consciente de la seguridad que defiende activamente contra las amenazas cibernéticas y protege los activos digitales y la información sensible.

En otras palabras, un manual con una sesión dedicada a la seguridad digital puede desempeñar un papel importante a la hora de dotar a los adultos de las capacidades y los conocimientos necesarios para protegerse en la era digital, fomentando una experiencia en línea más segura tanto para las personas como para las comunidades. DigiWELL es un recurso valioso para los adultos, ya que les informa sobre los riesgos potenciales, les ayuda a comprender la importancia de la ciberseguridad y cómo protegerse en línea. Por último, ofrece orientación práctica sobre la aplicación de medidas de seguridad digital y capacita a los adultos para navegar por el mundo digital con confianza, además de servir como guía de referencia que los

adultos pueden volver a consultar cada vez que se enfrenten a nuevos retos de seguridad digital o necesiten refrescar ciertos temas.

1.5 Diccionario del proyecto DigiWELL y cómo utilizarlo

El objetivo del diccionario es familiarizar a los usuarios adultos de tecnologías digitales con términos y definiciones básicos relacionados con el bienestar digital, la seguridad digital y la resiliencia digital.

Clasificación de términos

En cuanto al contenido, el diccionario contiene 3 categorías básicas de términos;

1. Términos y definiciones del ámbito de las tecnologías de la información y la comunicación (tecnologías digitales según el proyecto).
2. Términos y definiciones del ámbito de la seguridad informática, cibernética y digital (seguridad digital según el proyecto).
3. Términos y definiciones definidos por los objetivos del proyecto: bienestar digital y resiliencia digital. Estos términos son relativamente nuevos y forman parte de la investigación documental de los equipos del proyecto. Cabe destacar que no existe una definición uniforme de estos términos. Esta categoría también incluye términos del campo de la salud mental y física, por ejemplo, adicción digital, fatiga/agotamiento digital, desintoxicación digital, etc.

Nota: En la base de datos de texto de un diccionario, un término puede tener más de una definición por muchas razones: la definición original ha evolucionado con el tiempo, la definición amplia se adapta a un área específica, las definiciones de términos son similares pero con diferencias sutiles, etc.

Términos y definiciones

Resiliencia digital: 1. La resiliencia digital significa tener la conciencia, las habilidades, la agilidad y la confianza necesarias para utilizar las nuevas tecnologías y adaptarse a los cambiantes requisitos de las competencias digitales. La resiliencia digital mejora la capacidad para resolver problemas y mejorar las competencias, así como la capacidad para navegar por las transformaciones digitales. 2. La resiliencia digital es la capacidad de los jóvenes para desarrollar una mentalidad crítica cuando acceden a la información digital para reducir su vulnerabilidad a la información potencialmente dañina. 3. Por resiliencia digital se entiende "el proceso de adaptarse bien a las fuentes digitales de estrés y desarrollar habilidades para gestionar el impacto de entornos y aplicaciones digitales en constante cambio".

Seguridad digital: La seguridad digital es la protección de la identidad digital, ya que representa una identidad física en la red o en los servicios de Internet. La seguridad digital es un conjunto de buenas prácticas y herramientas utilizadas para proteger los datos personales y la identidad en línea en el mundo online. Ejemplos de herramientas son: servicios web, software antivirus, tarjetas SIM de teléfonos inteligentes, dispositivos personales biométricos y seguros, gestores de contraseñas, control parental, etc.

Bienestar digital: 1. El bienestar digital describe la capacidad de una persona para gestionar eficazmente los efectos negativos de la tecnología en su vida profesional y personal. El objetivo del bienestar digital es promover el uso saludable de los dispositivos tecnológicos y los servicios digitales. 2. Un estado de bienestar personal experimentado a través del uso saludable de la tecnología digital. 3. El bienestar digital abarca las formas en que la tecnología de la información -incluidas las comunicaciones y los sensores- puede ayudar a las personas a vivir una vida larga y saludable.

Competencia digital: Uso confiado, crítico y responsable de las tecnologías digitales y compromiso con ellas para el aprendizaje, el trabajo y la participación en la sociedad. Se define como una combinación de conocimientos, habilidades y actitudes.

Adicción digital: La adicción digital es una adicción nociva a los medios digitales, los dispositivos e internet caracterizada por su uso excesivo de forma que repercute negativamente en la vida del usuario.

Competencias digitales: Las competencias digitales son un conjunto de capacidades para utilizar dispositivos digitales, aplicaciones de comunicación y redes para acceder a la información y gestionarla. Permiten a las personas crear y compartir contenidos digitales, comunicarse y colaborar, y resolver problemas para una autorrealización eficaz y creativa en la vida, el aprendizaje, el trabajo y las actividades sociales.

Ciberamenaza: Cualquier circunstancia o evento con el potencial de afectar negativamente a organizaciones/individuos mediante el acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio. El objetivo es robar/dañar datos o perturbar el bienestar digital.

Ciberacoso: Término para diversas formas de acoso en el espacio en línea en el que uno o más individuos utilizan la tecnología digital para dañar intencionada y repetidamente a otra persona (por ejemplo, enviando correos electrónicos o mensajes instantáneos, publicando comentarios en redes sociales o foros públicos).

Ciberseguridad: La ciberseguridad es un subconjunto de la seguridad de la información, su objetivo es proteger el ciberespacio (es decir, redes, intranets, servidores, sistemas de información e informáticos e infraestructuras) de accesos no autorizados, ciberataques o daños. La ciberseguridad se centra en la protección de la información en forma electrónica/digital ubicada en ordenadores, almacenamiento y redes (en el ciberespacio).

Privacidad digital: La privacidad digital es la capacidad de una persona para controlar y proteger el acceso y el uso de su información personal cuando accede a Internet. La privacidad digital ayuda a las personas a permanecer en el anonimato en línea salvaguardando la información personal identificable, como nombres, direcciones, números de identificación social, datos de tarjetas de crédito, etc.

Seguridad digital frente a ciberseguridad frente a seguridad de la información: Seguridad de la información: protege la información (en cualquier formato y forma) y los sistemas de información del acceso y uso no autorizados para asegurar y preservar la privacidad de los datos importantes. Ciberseguridad: protege redes y sistemas de comunicación completos, sistemas informáticos y otros componentes digitales, así como los datos digitales almacenados en ellos. Seguridad digital: protege la presencia en línea (identidad e información sensible asociada, activos.

Mejor práctica: Método o procedimiento probado que ofrece la solución más eficaz en un ámbito determinado, que se ha demostrado que conduce a resultados óptimos y que se establece (sugiere) como norma apropiada para su adopción generalizada. En seguridad digital, se trata de procedimientos definidos para garantizar la protección de un individuo/organización en el espacio digital (por ejemplo, técnicas, programas, instrucciones, manuales recomendados).

2 Bienestar digital

2.1 ¿Qué es el bienestar?

El término "**bienestar**" describe la condición de estar contento, alegre y saludable. Incluye el bienestar físico, mental y emocional de una persona, entre otras áreas de su existencia. Más allá de estar libre de enfermedades o molestias, el bienestar se centra en la felicidad general y la calidad de vida.

El **bienestar físico** es el estado del propio cuerpo, teniendo en cuenta aspectos como la forma física, la dieta y la ausencia de enfermedades. Implica mantener un estilo de vida saludable mediante el ejercicio constante, una alimentación nutritiva, suficientes horas de sueño y la gestión del estrés.

La salud cognitiva y emocional de una persona está relacionada con su bienestar mental. Implica tener una buena perspectiva, sentirse realizado y ser capaz de manejar el estrés y las dificultades de la vida. Actividades como practicar la atención plena, dedicarse a un hobby, pedir apoyo a los seres queridos y obtener ayuda profesional cuando sea necesario pueden ayudar a alimentar el bienestar mental.

El **bienestar emocional** es la capacidad de comprender y controlar las emociones. Implica cultivar la resiliencia, mantener buenas relaciones y tener un sentido positivo de uno mismo. El autoconocimiento, el control emocional, la comunicación eficaz y el desarrollo de relaciones de apoyo contribuyen al bienestar emocional.

La **calidad de las conexiones** de una persona y su sentido de pertenencia a la comunidad forman parte del bienestar social. Implica fomentar vínculos duraderos con los seres queridos, los amigos íntimos y una red social más amplia. Participar en actividades sociales, retribuir a la comunidad y mantener un sentimiento de conexión y pertenencia pueden mejorar el bienestar social.

En general, **el bienestar es una idea global** que considera cómo se interrelacionan las distintas facetas de la vida de una persona. Implica buscar activamente una existencia equilibrada y satisfactoria, cuidar la salud física y mental, cultivar relaciones sanas y encontrar sentido a la propia vida.

2.2 Bienestar y digitalización

Al permitir la comunicación, aumentar la eficiencia y mejorar el acceso a la información, la tecnología y la digitalización tienen el potencial de mejorar el bienestar. Para gestionar el uso digital, salvaguardar la privacidad y la seguridad y lograr un buen equilibrio entre la tecnología y otras facetas de la vida, es crucial ser consciente de los posibles inconvenientes y tomar las precauciones necesarias.

La tecnología y la digitalización han mejorado enormemente el acceso a la información y los servicios, lo que repercute positivamente en el bienestar. Las personas tienen ahora fácil acceso a herramientas digitales para su desarrollo personal, información sanitaria, grupos de apoyo en línea y recursos educativos. Gracias a la comunicación y conexión a distancia, la tecnología fomenta las conexiones sociales y reduce el sentimiento de soledad. Las personas pueden mantenerse en contacto con amigos, familiares y comunidades gracias a las plataformas digitales, los medios sociales y las aplicaciones de mensajería, que mejoran el bienestar social. Muchas facetas de la vida se han vuelto más eficientes y cómodas gracias a la digitalización. Mediante el uso de herramientas y servicios digitales, las tareas que antes requerían mucho tiempo y esfuerzo ahora pueden completarse rápidamente y sin esfuerzo. Esto puede contribuir al bienestar general al liberar tiempo y reducir el estrés. Además, las habilidades digitales son cada vez más cruciales en el mercado laboral a medida que se desarrolla la tecnología. La empleabilidad y el bienestar socioeconómico de una persona pueden mejorar adquiriendo y utilizando estos talentos. La brecha digital, que se produce cuando algunas personas o grupos carecen de acceso a la tecnología o de alfabetización digital, puede, no obstante, agravar las disparidades ya existentes.

Aunque el uso inadecuado o excesivo de la tecnología puede tener efectos perjudiciales para la salud mental, también puede tener efectos positivos. La ansiedad, la desesperación y la baja autoestima pueden verse influidas por el exceso de tiempo frente a la pantalla, la comparación con las redes sociales y el abuso en línea. Para salvaguardar la salud mental, es crucial mantener un equilibrio saludable y practicar un uso consciente de la tecnología. Además, el entorno digital presenta algunos problemas de privacidad y seguridad. Las amenazas cibernéticas, las violaciones de datos y el fraude en línea pueden poner en peligro la seguridad financiera y la información personal de las personas. Mantener el bienestar general en la era digital exige proteger la seguridad y la privacidad digitales.

2.3 ¿Qué es el bienestar digital?

El desarrollo de la resiliencia digital y la adopción de procedimientos de seguridad conducen a una condición de salud óptima y bienestar general en la esfera digital, lo que se denomina bienestar digital. El bienestar digital tiene su origen en el concepto de wellbeing y tiene que ver con la vida digital de los individuos. La capacidad de las personas para adaptarse, gestionar y prosperar en el mundo digital gestionando con éxito tanto su bienestar como su seguridad se denomina resiliencia digital, que es una mezcla de bienestar y seguridad digitales. La piedra angular de la resiliencia digital es el bienestar digital, que hace hincapié en preservar una conexión positiva y sensata con la tecnología. Implica limitar el tiempo frente a la pantalla, dar prioridad a la salud mental y emocional, crear comunidades en línea de apoyo y aprender alfabetización digital. En el contexto del bienestar, la resiliencia digital ayuda a las personas a hacer frente a dificultades en línea como el ciberacoso, el hostigamiento en línea o la exposición a contenidos peligrosos, preservando al mismo tiempo su bienestar general. Las personas pueden desarrollar una sólida resiliencia digital que les permita moverse por el mundo digital con seguridad y responsabilidad integrando el bienestar digital con la seguridad digital. Son más capaces de gestionar los retos del mundo digital, adaptarse a los peligros cambiantes, tomar decisiones acertadas, salvaguardar su información

personal y mantener su salud mental, emocional y física mientras utilizan Internet. En última instancia, la resiliencia digital fomenta una experiencia en línea más segura, saludable y satisfactoria para las personas.

2.3.1 Salud mental, bienestar y bienestar digital

Toda nuestra calidad de vida está influida por las profundas conexiones entre nuestra salud mental y el bienestar general. Nuestro bienestar psicológico y emocional, que incluye aspectos como nuestros pensamientos, sentimientos y comportamientos, se denomina salud mental. Es fundamental para nuestra salud total, tan importante como el bienestar físico. Por el contrario, el bienestar es un estado integral de equilibrio, plenitud y satisfacción en la vida. La relación entre ambos se basa en cómo la salud mental de una persona repercute significativamente en su salud física y viceversa. Nuestro bienestar total aumenta cuando cultivamos una salud mental positiva controlando el estrés, superando obstáculos y estableciendo relaciones sanas, lo que se traduce en una vida más plena y significativa. Por otra parte, la sensación de bienestar puede mejorar enormemente la salud mental al fomentar la resiliencia, la estabilidad emocional y una mayor capacidad para afrontar los retos de la vida. Podemos crear una vida feliz y próspera centrándonos en la relación entre nuestra salud mental y el bienestar.

Debido a las rápidas mejoras de la tecnología y a su omnipresente integración en nuestra vida cotidiana, la salud mental asume una naturaleza compleja y dinámica en la era digital. En el contexto de la era digital, el bienestar mental y emocional de una persona se denomina "salud mental digital". Incluye las redes sociales, las interacciones en línea, los efectos psicológicos de las tecnologías digitales y la conexión continua que define la vida moderna. Aunque la tecnología ha creado muchas ventajas y oportunidades, también ha creado importantes dificultades para la salud mental. A pesar del continuo contacto virtual, la era digital puede dar lugar a problemas como la adicción a Internet, el ciberacoso, la sobrecarga de información, la comparación social y la sensación de aislamiento. Sin embargo, también ofrece enfoques de vanguardia para gestionar la salud mental, como aplicaciones de salud mental, terapia en línea y grupos de apoyo virtuales. Mantener un equilibrio saludable entre nuestra vida en línea y fuera de ella, ser conscientes de la cantidad de medios digitales que consumimos y buscar activamente herramientas digitales que puedan mejorar nuestro bienestar mental, al tiempo que nos protegemos de posibles trampas, es esencial a medida que nos adentramos en los entresijos de la era digital.

En la actualidad, existe una compleja relación entre la salud mental y el bienestar digital. El bienestar psicológico y emocional de las personas, que incluye factores como el estado de ánimo, los pensamientos, los sentimientos y el comportamiento, se denomina salud mental. Por otro lado, el bienestar digital describe el equilibrio y la armonía que uno siente cuando utiliza la tecnología y entabla relaciones digitales. La era digital tiene muchos beneficios, ya que permite la conectividad, el acceso a la información y las posibilidades de desarrollo personal. Sin embargo, el uso excesivo de la tecnología, las notificaciones continuas, la presión de las redes sociales y la sobrecarga de información pueden tener un impacto negativo en la salud mental al causar tensión, preocupación y una sensación de separación de la realidad. Por otro lado, puede tener un impacto beneficioso en la salud mental cuando se prioriza el bienestar digital estableciendo límites, tomando descansos regulares de las pantallas y estando atentos al consumo digital. Para fomentar tanto la salud mental como el bienestar digital y garantizar una coexistencia armoniosa entre nuestras vidas virtuales y reales, es esencial encontrar un equilibrio saludable entre la participación digital y las actividades fuera de línea. Una vida más significativa y equilibrada en la era digital puede lograrse adoptando deliberadamente la tecnología y utilizando las herramientas digitales para mejorar la salud mental.

2.3.2 ¿Por qué necesitamos el bienestar digital?

Los factores clave del bienestar digital son la calidad de vida, la comunicación, la productividad y el éxito, y la salud mental y física. El bienestar digital es importante porque incluye el estado general de salud, felicidad y satisfacción. Se refiere a la salud general de las personas y las comunidades, teniendo en cuenta sus aspectos sociales, psicológicos y físicos. El uso de teléfonos móviles, redes sociales y videojuegos en exceso o de forma poco saludable puede ser perjudicial para la salud mental. La ansiedad, la desesperación, la soledad y la baja autoestima pueden verse exacerbadas por el exceso de tiempo frente a la pantalla, las comparaciones frecuentes con otros en las redes sociales o el ciberacoso. En este sentido, el bienestar digital es la forma de tener el control sobre nuestra propia vida. Es crucial tener una conexión sana con la tecnología para favorecer una buena salud mental y el bienestar digital. Poner límites al uso de gadgets, realizar desintoxicaciones digitales, participar en actividades offline y dar prioridad al autocuidado y a las interacciones cara a cara pueden formar parte de ello. Debemos ser conscientes del impacto que la tecnología digital tiene en nuestra salud mental y tomar medidas proactivas para garantizar un uso sensato.

El bienestar digital se ha convertido en una necesidad humana esencial en la era digital, sobre todo a raíz de la pandemia de Covid-19. Nuestra dependencia de las plataformas digitales ha aumentado a medida que la tecnología sigue invadiendo todos los aspectos de nuestra vida cotidiana, desde la comunicación y la educación hasta el empleo y el entretenimiento. La epidemia ha hecho que la digitalización avance a un ritmo sin precedentes, exigiendo trabajo a distancia, escolarización en línea y más relaciones virtuales. En consecuencia, mantener nuestro bienestar digital es crucial para llevar una vida plena y saludable. Podemos utilizar la tecnología de forma consciente y responsable para asegurarnos de que mejora nuestras vidas en lugar de suponer una amenaza para nuestro bienestar general en este entorno digital en rápida evolución, reconociendo el bienestar digital como una necesidad humana fundamental.

2.3.3 Bienestar digital bueno y malo

El bienestar digital es un término amplio que abarca diversos aspectos del mundo digital. Se refiere tanto a la salud física, psicológica y social de los individuos como a su sensación de conciencia digital, equilibrio, seguridad, satisfacción y salud. Como se ha visto, el significado atribuido al término "bienestar digital" se orienta sobre todo hacia el lado favorable de la digitalización, que se refiere a un buen bienestar digital. A la inversa, los individuos que experimentan una falta de bienestar digital se refieren a un bienestar digital pobre. Teniendo esto en cuenta, se podría afirmar que los siguientes aspectos se encuentran entre los principales indicadores de un buen bienestar digital:

- Seguridad digital: Garantizar la seguridad digital contribuye notablemente al bienestar digital. Abarca la protección de su presencia en línea, incluida su identidad, datos y activos.
- Seguridad digital: Incluye que las personas sean conscientes de los riesgos potenciales en el mundo digital y tiene que ver con la capacidad de las personas para identificar y gestionar de forma crítica diversas amenazas en el entorno digital.
- Equilibrio digital: Se refiere al aprovechamiento intencionado de la tecnología y el mundo digital. El equilibrio digital tiene que ver con el uso del mundo digital, las herramientas y los equipos digitales para ámbitos de la vida, no para todo. Un equilibrio regular y coherente entre la vida en línea y fuera de ella y evitar una dependencia excesiva de la tecnología son signos de un buen equilibrio digital.

- Independencia digital: Es la capacidad de controlar el tiempo que se pasa en línea y evitar centrar el mundo digital en la vida cotidiana. Pasar demasiado tiempo en línea y planificar menos actividades sociales debido a un uso excesivo de Internet son algunos signos de dependencia digital.
- Satisfacción digital: Se refiere a alcanzar la satisfacción y sentir placer mientras se emplean herramientas y equipos digitales y se interactúa con la tecnología.
- Oportunidad digital: Se refiere a beneficiarse de la tecnología y la digitalización para abrir nuevas posibilidades relacionadas con la difusión de las tecnologías digitales y adquirir nuevas competencias para crear nuevas oportunidades.
- Uso crítico y responsable de la tecnología: Junto con sus oportunidades, la tecnología exige que los usuarios actúen de forma responsable protegiendo los derechos propios y respetando los derechos de los demás, que actúen de forma responsable y prudente, y que piensen de forma crítica ante cualquier contenido del mundo digital.

Estos aspectos también podrían considerarse entre las dimensiones del bienestar digital. Si una persona tiene o garantiza un nivel relativamente alto de seguridad digital, protección, equilibrio, independencia, satisfacción, oportunidad y/o uso crítico y responsable de la tecnología al utilizar herramientas y equipos digitales, se podría considerar que tiene un buen bienestar digital. Por el contrario, si una persona carece de algunos de los componentes anteriores, significa que tiene un bienestar digital deficiente. Cabe recordar que estar sano física, psicológica y socialmente también se refiere a un buen bienestar digital y que otros aspectos pueden contribuir al bienestar digital y al bienestar general de las personas.

2.3.4 Fomentar el bienestar digital de las personas: Beneficios potenciales para todos y para la educación de adultos

Promover el bienestar digital en la educación de adultos o potenciar el bienestar de los adultos y el bienestar digital ofrece muchas oportunidades. Ante todo, el bienestar es una necesidad humana básica. Especialmente después de COVID-19, la mayoría de las personas pasan mucho más tiempo en línea y están más expuestas a la tecnología junto con sus riesgos y amenazas. Tanto si lo desean intencionadamente como si no, las personas aportan todo su ser al trabajo, es decir, existe una clara conexión entre el propio bienestar de las personas y el ambiente en el entorno laboral. Así pues, las posibles acciones para fomentar el bienestar y el bienestar digital de los individuos contribuyen tanto a ellos como seres humanos como a las organizaciones para las que trabajan. Desde una perspectiva organizativa, fomentar el bienestar digital de los trabajadores contribuye, aunque no exclusivamente, al rendimiento, el compromiso, la innovación y la satisfacción del equipo. El bienestar digital permite a los individuos estar más centrados, comprometidos y ser más productivos, lo que contribuye a una vida más saludable tanto dentro como fuera del entorno laboral. La adopción de prácticas de bienestar digital por parte de los empleados les permite estar menos agotados y distraídos. Promover acciones de apoyo al bienestar digital favorece el equilibrio entre la vida laboral y personal de las personas. Además, elimina los efectos negativos de la sobreexposición a la digitalización, lo que permite experimentar menos ansiedad, desesperación, estrés, etc.

La idea de bienestar en el contexto de la educación de adultos va más allá de las ideas convencionales de logros académicos e incluye la salud y la realización generales de los estudiantes. El concepto de "bienestar digital" ha cobrado importancia con la llegada de la era digital, especialmente para los nómadas

digitales que dependen en gran medida de la tecnología para llevar un estilo de vida móvil. En la educación de adultos, el término "bienestar digital" se refiere a proporcionar a los estudiantes las habilidades y la información que necesitan para utilizar Internet con sensatez y ética. Promover el bienestar digital es crucial para crear un entorno de aprendizaje satisfactorio, ya que los nómadas digitales a menudo se enfrentan a dificultades particulares, como compaginar su vida personal y profesional y superar emociones de soledad. Integrar el bienestar digital en la educación de adultos implica enseñar a los estudiantes a controlar adecuadamente el tiempo que pasan frente a la pantalla, a crear comunidades en línea positivas y a ser conscientes de su uso digital. También abarca temas como la ciberseguridad, el cansancio digital y la privacidad de los datos. En el mundo digital actual, los educadores pueden garantizar una experiencia de aprendizaje positiva y enriquecedora abordando la evidente necesidad de potenciar el bienestar digital en la educación de adultos y proporcionando a los nómadas digitales y a otros alumnos las herramientas necesarias para mantener un equilibrio saludable entre sus interacciones digitales y su bienestar general.

Se necesita una estrategia cuidadosa y minuciosa para integrar con éxito el bienestar digital en la educación de adultos, porque es un proceso complicado y continuo. El primer paso, y el más importante, es formar a los alumnos adultos para que sean conscientes del valor del bienestar digital y de cómo afecta a su salud general y a su productividad. Gracias a esta instrucción, adquieren las habilidades prácticas necesarias para navegar por el mundo digital con sensatez y seguridad. La segunda etapa consiste en modificar el material del curso para que el plan de estudios refleje los conceptos del bienestar digital. Esto implica incorporar ideas como el control de las distracciones digitales, la privacidad en línea, la etiqueta digital y la alfabetización digital. Los estudiantes adultos pueden tener un mayor conocimiento de las ventajas y desventajas de la tecnología y aprender a utilizarla eficazmente incorporando estas características a los cursos. Se crea un entorno de apoyo en el que los alumnos pueden compartir experiencias, intercambiar técnicas y reafirmar su compromiso con el bienestar digital mediante el diseño de eventos de capacitación adicionales, como seminarios y conversaciones. Para ser pertinente y eficaz en el fomento del bienestar en la era digital, la educación de adultos debe evolucionar continuamente a fin de mantenerse al día con la rápida evolución del panorama digital.

3 Seguridad digital

3.1 Seguridad digital y ciberseguridad

Según la Organización de Cooperación y Desarrollo Económicos (OCDE), la seguridad digital es esencial para la confianza en la era digital. La OCDE ha estado facilitando la cooperación internacional y desarrollando análisis de políticas y recomendaciones en materia de seguridad digital desde principios de los años noventa. El trabajo en esta área tiene como objetivo desarrollar y promover políticas que fortalezcan la confianza sin inhibir el potencial de las tecnologías de la información y la comunicación (TIC) para apoyar la innovación, la competitividad y el crecimiento. La seguridad digital se refiere a los aspectos económicos y sociales de la ciberseguridad, a diferencia de los aspectos puramente técnicos y los relacionados con la aplicación de la ley penal o la seguridad nacional e internacional. El término "digital" es coherente con expresiones como la economía digital, la transformación digital y las tecnologías digitales.

Constituye una base para un diálogo internacional constructivo entre las partes interesadas que buscan fomentar la confianza y maximizar las oportunidades de las TIC[1].

La seguridad digital y la ciberseguridad están relacionadas pero no son lo mismo. Ambos implican la protección de los activos digitales y la información contra el acceso no autorizado, el uso o los daños, pero difieren en su alcance y enfoque.

La seguridad digital se refiere a la práctica de salvaguardar los datos, la información y los activos digitales del acceso no autorizado, el robo o el daño. Abarca una gama más amplia de medidas de seguridad que protegen los datos y la información en diversas plataformas y dispositivos digitales, incluidas computadoras, teléfonos inteligentes, tabletas y otras tecnologías digitales.

Las medidas de seguridad digital pueden incluir:

- Protección con contraseña: Creación de contraseñas seguras y únicas para cuentas y dispositivos en línea.
- Cifrado de datos: Codificación de datos para evitar accesos no autorizados o filtraciones de datos.
- Comunicaciones seguras: Uso de protocolos de cifrado para la transmisión segura de datos.
- Controles de acceso: Implementación de permisos y restricciones para limitar el acceso a datos sensibles.
- Seguridad del dispositivo: Utilizando características como bloqueos de pantalla y limpieza remota para dispositivos perdidos o robados.

La ciberseguridad es un subconjunto de la seguridad digital y se centra específicamente en la protección de los activos digitales contra amenazas y ataques cibernéticos. Implica la defensa contra el acceso no autorizado, daños o interrupciones de sistemas, redes e infraestructuras digitales.

Las medidas de ciberseguridad pueden incluir:

- Protección contra cortafuegos: Establecer barreras para evitar el acceso no autorizado a una red.
- Sistemas de detección de intrusos: Monitoreo de redes para actividades sospechosas y amenazas potenciales.
- Protección contra malware: Uso de software antivirus para detectar y eliminar software malicioso.
- Planificación de la respuesta a incidentes: Desarrollo de protocolos para responder eficazmente a los incidentes de ciberseguridad.
- Inteligencia de amenazas cibernéticas: Recopilación y análisis de información para anticipar y prevenir las amenazas cibernéticas.

[1] HTTPS://WWW.OECD.ORG/DIGITAL/DIGITAL-SECURITY/

La seguridad digital abarca una gama más amplia de prácticas que protegen los datos y la información en el ámbito digital, mientras que la ciberseguridad es un área especializada centrada en la defensa contra amenazas cibernéticas y ataques en sistemas y redes digitales. Ambos son componentes cruciales para garantizar la seguridad y la protección generales de los activos digitales y la información.

3.2 Amenazas a la ciberseguridad que enfrentan los adultos

Los adultos se enfrentan a una amplia gama de amenazas de ciberseguridad en el mundo digital de hoy. Aquí hay algunas amenazas de ciberseguridad comunes que los adultos a menudo encuentran:

- ***Ataques de phishing:*** El phishing es una técnica utilizada por los ciberdelincuentes para engañar a las personas para que proporcionen información confidencial, como credenciales de inicio de sesión, números de tarjetas de crédito o datos personales. Los correos electrónicos, mensajes o sitios web de phishing pueden parecer de fuentes confiables, pero su objetivo es engañar a los usuarios para que divulguen su información.
- ***Malware:*** El malware es un software malicioso diseñado para infiltrarse, dañar o obtener acceso no autorizado a los sistemas informáticos. Los tipos de malware incluyen virus, ransomware, spyware y troyanos. El malware puede propagarse a través de archivos adjuntos de correo electrónico malicioso, sitios web infectados o software comprometido.
- ***Robo de identidad:*** Los ciberdelincuentes pueden robar información personal, como números de Seguro Social, fechas de nacimiento o datos financieros, para cometer robo de identidad. Esta información se obtiene a menudo a través de violaciones de datos o intentos de phishing.
- ***Estafas en línea:*** Hay numerosas estafas en línea dirigidas a adultos, como estafas de lotería, estafas románticas, estafas de soporte técnico falso y esquemas de inversión fraudulentos. Los estafadores utilizan varias tácticas para manipular a las personas para enviar dinero o proporcionar información personal.
- ***Violaciones de datos:*** Las violaciones de datos se producen cuando la información confidencial en poder de las empresas u organizaciones es expuesta o robada. Como adulto, puede verse afectado por violaciones de datos si su información personal es almacenada por las entidades afectadas.
- ***Ingeniería Social:*** La ingeniería social implica la manipulación de individuos para revelar información confidencial o realizar ciertas acciones. Los ciberdelincuentes pueden utilizar técnicas de ingeniería social para obtener acceso no autorizado a sistemas o cuentas.
- ***Ataques de contraseña:*** Las contraseñas débiles o la reutilización de contraseñas pueden conducir a ataques de contraseña, como ataques de fuerza bruta o ataques de diccionario, donde los ciberdelincuentes intentan adivinar o descifrar contraseñas para obtener acceso no autorizado.
- ***Riesgos de Wi-Fi Público:*** El uso de redes Wi-Fi públicas puede exponer a los adultos a riesgos de seguridad, ya que estas redes pueden carecer de cifrado adecuado y son susceptibles de escuchar a escondidas por los atacantes.
- ***Amenazas internas:*** Las amenazas internas involucran a empleados o personas con acceso autorizado a sistemas o datos que intencionalmente o involuntariamente causan daños o filtran información confidencial.

- ***Vulnerabilidades de IoT:*** La creciente adopción de dispositivos de Internet de las cosas (IoT) puede crear riesgos de ciberseguridad, ya que muchos de estos dispositivos pueden tener medidas de seguridad inadecuadas y pueden ser explotados por los ciberdelincuentes.

Para protegerse contra estas amenazas, los adultos deben practicar una buena higiene de la ciberseguridad, incluyendo el uso de contraseñas fuertes y únicas, permitiendo la autenticación de múltiples factores, manteniendo el software y los dispositivos actualizados, siendo cautelosos con los correos electrónicos y enlaces sospechosos, y ser conscientes de la información que comparten en línea. La capacitación periódica sobre ciberseguridad también puede ayudar a las personas a mantenerse informadas sobre las amenazas emergentes y las mejores prácticas para mantenerse seguras en línea. La siguiente sección presenta en detalle algunas de las prácticas de seguridad digital más esenciales para los adultos para reducir el riesgo de ser víctima de amenazas de ciberseguridad y proteger sus identidades y activos digitales.

3.3 Prácticas de seguridad digital para adultos

Las prácticas de seguridad digital son esenciales para que los adultos protejan su información personal, datos y cuentas en línea de las amenazas de ciberseguridad. Estas son algunas prácticas importantes de seguridad digital que los adultos deben seguir:

- ***Utilice contraseñas fuertes y únicas:*** Los adultos deben crear contraseñas fuertes y únicas para sus cuentas en línea. Evite el uso de contraseñas fácilmente adivinables como "123456" o "contraseña." Considera usar un administrador de contraseñas para generar y almacenar contraseñas complejas de forma segura.
- ***Habilitar autenticación multifactor (MFA):*** Siempre que sea posible, habilite la autenticación multifactorial en sus cuentas en línea. MFA añade una capa adicional de seguridad al requerir una segunda forma de verificación, como un código de una sola vez enviado a su dispositivo móvil, además de su contraseña.
- ***Mantenga el software y los dispositivos actualizados:*** Actualice regularmente su sistema operativo, navegadores web y aplicaciones de software. Las actualizaciones a menudo incluyen parches de seguridad que abordan vulnerabilidades conocidas.
- ***Sea cauteloso con los correos electrónicos y enlaces:*** Tenga cuidado al abrir correos electrónicos de remitentes desconocidos o hacer clic en enlaces sospechosos. Ten especial cuidado con los correos electrónicos que piden información confidencial o te indican que inicies sesión en un sitio web falso.
- ***Proteja su red doméstica:*** cambie la contraseña predeterminada en su enrutador Wi-Fi doméstico y habilite el cifrado WPA2 o WPA3 para proteger su red inalámbrica. Evite el uso de redes Wi-Fi públicas para actividades sensibles a menos que use una red privada virtual (VPN).
- ***Realice copias de seguridad de datos regularmente:*** realice copias de seguridad de sus archivos y datos importantes en un disco duro externo, almacenamiento en la nube o un servicio de copia de seguridad seguro. En caso de pérdida de datos o ataques de ransomware, tener copias de seguridad asegura que puede recuperar sus archivos.
- ***Utilice Secure Wi-Fi y HTTPS:*** Al acceder a sitios web sensibles, asegúrese de que utilizan el cifrado HTTPS. Busque el símbolo de candado en la barra de direcciones del navegador para verificar la seguridad del sitio web.

- ***Ten cuidado con las redes sociales:*** Ten cuidado con la información que compartes en las plataformas de redes sociales. Evite publicar datos personales como su dirección, número de teléfono o planes de viaje, ya que esta información se puede usar para ataques de ingeniería social.
- ***Instalar antivirus y software de seguridad:*** Utilice antivirus y software de seguridad de buena reputación en sus dispositivos para proteger contra el malware y otras amenazas. Mantenga el software actualizado para garantizar una protección óptima.
- ***Infórmese sobre la ciberseguridad:*** Manténgase informado sobre las últimas amenazas y mejores prácticas de ciberseguridad leyendo fuentes confiables, asistiendo a seminarios web o participando en programas de concientización de ciberseguridad (Consulte los recursos de seguridad digital disponibles para adultos).

Al incorporar estas prácticas de seguridad digital en sus rutinas diarias, los adultos pueden reducir significativamente el riesgo de ser víctimas de amenazas a la ciberseguridad y proteger sus identidades y activos digitales.

3.4 Recursos de seguridad digital disponibles para adultos

El Cybersecurity Education Hub[2] (CEH) de la Universidad Estatal de California en San Marcos ofrece recursos y dirección para los esfuerzos del campus y la comunidad para aumentar la educación y la conciencia de seguridad digital. El CEH es un esfuerzo de colaboración de la Oficina de Seguridad de la Información del campus, las Facultades de Ciencias y Matemáticas y Administración de Empresas.

El CEH trabaja para asegurar que los programas educativos de seguridad digital del campus aborden temas amplios relacionados con los acontecimientos actuales en el campo de la seguridad digital, y proporciona oportunidades para que los temas de seguridad digital se incorporen en los cursos impartidos en toda la universidad. La CEH también ofrece recursos a estudiantes, organizaciones estudiantiles y al público en general. Promueve y facilita la comunicación y la colaboración con la educación en seguridad digital en toda la comunidad. Proporcionaron materiales de aprendizaje sobre temas como la privacidad y las redes sociales, la seguridad cibernética para los estudiantes, la ciberseguridad actual y los conceptos de ciberseguridad.

Además, en 2008 se introdujeron materiales de capacitación sobre seguridad cibernética de la ENISA[3]. Desde entonces se ha ampliado con nuevas secciones que contienen información crítica para el éxito en el campo de la seguridad cibernética. La ENISA contiene materiales de capacitación, como manuales para profesores, juegos de herramientas para estudiantes e imágenes virtuales, que complementan las sesiones de capacitación práctica.

[2] https://www.csusm.edu/cybersec-hub/index.html

[3] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

4 Mejores prácticas de creación de seguridad digital para adultos

La seguridad digital es cada vez más importante en nuestra sociedad conectada, y las personas mayores son uno de los grupos más vulnerables en línea. A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas. Por lo tanto, es importante establecer medidas y directrices para proteger a los adultos mayores en el entorno digital. A continuación se presentan algunas buenas prácticas y acciones exitosas implementadas en varios países que pueden servir de referencia para otros.

La estrategia de ciberseguridad de la Unión Europea, representada en los informes que están disponibles en el sitio web oficial de la Comisión Europea, proporciona información valiosa sobre las mejores prácticas para mejorar la seguridad digital en Europa.

4.1 Cuestiones clave para construir seguridad digital

Esta sección puede parecer una repetición de la sección 3.3. Prácticas de seguridad digital para adultos, pero contiene más escenarios y ejemplos del mundo real.

Contraseñas fuertes: Ayúdales a crear contraseñas fuertes y únicas para cada cuenta. Las contraseñas deben ser largas y contener letras mayúsculas y minúsculas, números y caracteres especiales. Las contraseñas deben ser largas (al menos 8 caracteres), contener letras mayúsculas y minúsculas, números y caracteres especiales. Evite usar información personal predecible, como nombres o fechas de nacimiento. Recuérdales que no compartan sus contraseñas con nadie y que las cambien regularmente.

Por ejemplo, una contraseña fuerte podría ser "P@ssw 0rd2023!" que combina letras mayúsculas, minúsculas, números y caracteres especiales. Evite el uso de información personal predecible como nombres o fechas de nacimiento, como "John1980" o "MarySmith123."

Educación y concienciación: Infórmeles sobre los riesgos y amenazas en línea, como el phishing, el malware y el robo de identidad. Ayúdelos a entender cómo reconocer y evitar estas situaciones. Es importante educarlos sobre los riesgos en línea, como el phishing (intentos de obtener información confidencial fraudulentamente), el malware (malware) y el robo de identidad. Aprenda a reconocer estas señales de advertencia y evite caer en estas trampas. Explique los posibles efectos negativos y cómo protegerse.

Por ejemplo, explique que los correos electrónicos de phishing pueden parecer de fuentes legítimas, pidiéndoles que hagan clic en enlaces e ingresen información confidencial. Muéstreles ejemplos de correos electrónicos sospechosos y cómo identificarlos. Proporcione información sobre tipos comunes de malware, como software antivirus falso o ventanas emergentes, y cómo evitarlos.

Autenticación de dos factores (2FA): Ayúdelos a implementar la autenticación de dos factores siempre que sea posible. Esto añade una capa adicional de seguridad a sus cuentas. La autenticación de dos factores añade una capa adicional de seguridad. Ayúdelos a habilitar esta función en sus cuentas si es posible. 2FA requiere otro método de autenticación además de una contraseña estándar, como un código de mensaje de texto, autenticador o huella digital.

Por ejemplo, después de introducir su contraseña, recibirán un mensaje de texto con un código de verificación que deben ingresar para acceder a su cuenta. Esto añade una capa adicional de seguridad y hace que sea más difícil para los usuarios no autorizados acceder a sus cuentas.

Uso seguro de dispositivos móviles: Ayúdelos a configurar bloqueos de pantalla, reconocimiento facial o huellas dactilares para proteger sus dispositivos móviles. Recuérdales que no compartan sus dispositivos con personas que no conocen y que tengan cuidado al descargar aplicaciones de fuentes poco fiables.

Por ejemplo, muéstreles cómo habilitar un PIN o usar su huella digital para desbloquear su teléfono inteligente. Recuérdales que no compartan sus dispositivos con personas que no conocen y que sean cautelosos al descargar aplicaciones de fuentes poco fiables.

Actualizaciones de software: Asegúrese de que sus dispositivos (computadoras, tabletas, teléfonos inteligentes) tienen los últimos parches de seguridad y actualizaciones instaladas. Las actualizaciones a menudo incluyen soluciones para vulnerabilidades conocidas, por lo que mantener sus dispositivos actualizados ayuda a protegerlos.

Compras en línea: Recuérdeles comprar solo en sitios web confiables y seguros y usar métodos de pago seguros. Enséñeles a buscar un candado en la barra de direcciones y a usar métodos de pago seguros, como tarjetas de crédito con medidas de seguridad adicionales.

Uso seguro del correo electrónico: Advertirles sobre el phishing y aconsejarles que eviten hacer clic en enlaces o descargar archivos adjuntos de remitentes desconocidos. Adviértales sobre el phishing por correo electrónico, donde los estafadores tratan de obtener información confidencial haciéndose pasar por remitentes legítimos. Esto resalta la importancia de no hacer clic en enlaces o descargar archivos adjuntos de correos electrónicos sospechosos o remitentes desconocidos. Le insta a verificar la legitimidad de los correos electrónicos con el remitente antes de enviar información confidencial.

Redes sociales: Ayúdales a ajustar la configuración de privacidad en sus redes sociales para controlar quién ve sus publicaciones y evitar compartir información personal confidencial. Enséñeles a evitar compartir información confidencial, como números de teléfono, direcciones o información financiera públicamente en las redes sociales.

Por ejemplo, guíalos a través de la configuración de privacidad en Facebook para restringir quién puede ver sus publicaciones solo a amigos. Enfatiza la importancia de ser cauteloso al compartir información como números de teléfono, direcciones o detalles financieros en plataformas de redes sociales.

Navegación segura: Aprenda a reconocer estos sitios web seguros ("https" y "lock") y evite hacer clic en enlaces sospechosos o descargar archivos desconocidos. Enséñeles a distinguir entre sitios web seguros comprobando su barra de direcciones para un bloqueo y si se inician. "http" en lugar de "https". Explica la importancia de evitar hacer clic en enlaces sospechosos o descargar archivos de fuentes desconocidas, ya que pueden contener malware o redirigirte a sitios web fraudulentos.

Seguridad Wi-Fi: Asegúrese de que utilicen contraseñas seguras en su red Wi-Fi doméstica y evite conectarse a redes Wi-Fi públicas o desconocidas. Explique la importancia de usar contraseñas seguras en su red Wi-Fi doméstica y evite conectarse a redes Wi-Fi públicas o desconocidas. Las redes Wi-Fi no seguras pueden ser atacadas o interceptadas por espionaje de datos.

Cuentas inactivas: Ayúdeles a cerrar o eliminar cuentas en línea que ya no utilizan para reducir el riesgo de seguridad. Las cuentas inactivas pueden ser vulnerables a ataques, especialmente si contienen información personal.

Cuidado con las llamadas y mensajes sospechosos: Enséñeles a no revelar información personal o financiera a llamadas o mensajes inesperados. Enséñeles a tener cuidado al revelar información personal o financiera a llamadas inesperadas o mensajes de texto. Anime al remitente a verificar su identidad antes de compartir información confidencial. Por ejemplo, proporcione ejemplos de estafas comunes, como llamadas de soporte técnico falsas o notificaciones de premios de lotería.

Supervisión y soporte: Ofrézcase para ayudar con controles regulares de sus cuentas en línea y ayudarles si sospechan actividades sospechosas o tienen problemas de seguridad. Manténgase al día con las últimas amenazas en línea y proporcione orientación y soporte continuo. Por ejemplo, muéstreles cómo revisar la actividad de su cuenta reciente e iniciar sesión en varias plataformas.

Información personal: Enséñeles a tener cuidado al compartir información personal en línea y a limitar la cantidad de información que publican. Limite la cantidad de información que publican, como direcciones, números de teléfono o información escolar. Fomenta la privacidad y la importancia de proteger su identidad en línea.

Copia de seguridad de datos importantes: Copia de seguridad de datos importantes con regularidad para evitar la pérdida en caso de una violación de seguridad o fallo del dispositivo.

4.2 Mejores prácticas en el mundo

4.2.1 Cibereuropa

ENISA ha estado organizando Cyber Europe[4] desde 2010, una serie de ejercicios de gestión de incidentes cibernéticos y crisis con escenarios interesantes inspirados en eventos de la vida real y desarrollados por expertos en ciberseguridad europeos. Cada dos años, los sectores público y privado de los países de la UE y del EEE, así como las instituciones, organismos y agencias europeos, colaboran para reforzar sus capacidades técnicas y operativas existentes.

[4] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

El ejercicio Cibereuropa dura dos días y simula incidentes de ciberseguridad a gran escala que se convierten en crisis cibernéticas que afectan a toda la UE. Los participantes en este ejercicio podrán analizar incidentes técnicos avanzados de ciberseguridad, abordar situaciones complejas de continuidad empresarial y gestión de crisis que requieran coordinación y cooperación desde el nivel local hasta el de la UE.

La serie de ejercicios Cyber Europe tiene como objetivo mejorar la preparación de Europa para hacer frente a incidentes y crisis de ciberseguridad a gran escala, permitiendo a los participantes probar y mejorar su preparación en toda la UE, fomentar la confianza en el ecosistema de ciberseguridad de la UE, y proporcionar oportunidades de capacitación.

Participar en Cyber Europe ofrece una excelente oportunidad para:

- Sensibilización cibernética
- Crear y/o poner a prueba procedimientos de gestión de crisis cibernéticas
- Mejorar la comunicación dentro de la cadena de respuesta cibernética
- Crear un lenguaje común y mejorar la comprensión mutua
- Desarrollar una variedad de habilidades y habilidades de resiliencia individual y colectiva
- Analice incidentes técnicos complejos de ciberseguridad; maneje situaciones complejas de continuidad de negocios y gestión de crisis.

4.2.2 Adaptación de la interfaz y la tecnología

Japón ha sido pionero en adaptar la tecnología y los dispositivos para hacerlos más accesibles a las personas mayores. Por ejemplo, algunos teléfonos inteligentes y tabletas japoneses tienen interfaces de usuario más simples y características de accesibilidad mejoradas, lo que los hace más fáciles de usar para personas con habilidades digitales limitadas. Otros países y fabricantes de tecnología pueden adoptar tales políticas para asegurar que los adultos mayores puedan usar los dispositivos digitales de manera segura y efectiva. La adopción de estas prácticas por otros países y fabricantes de tecnología puede garantizar que los adultos mayores tengan acceso a dispositivos digitales más fáciles de usar, ayudando a mejorar su seguridad y participación en línea.

Existen varios cursos en el territorio europeo destinados a sensibilizar a las personas mayores sobre el uso de estas herramientas. Por ejemplo, la asociación ACDA de París ofrece cursos de bajo coste para introducir a las personas mayores en el mundo de la tecnología. Los cursos de esta asociación ofrecen la oportunidad de aprender desde lo básico cómo operar una computadora. El descubrimiento de unidades informáticas, aplicaciones, formatos de archivo. Después de eso, los participantes pueden adquirir habilidades más avanzadas, como administrar y organizar el buzón de correo y aprender el uso de la palabra sobre cómo procesar un documento escrito[5].

[5] http://www.aucoursdesages.fr/cours.php

4.2.3 Líneas de ayuda y apoyo especializado

Singapur ha establecido su propia línea telefónica de ayuda para las personas mayores que se enfrentan a problemas de seguridad digital. Esta línea de ayuda ofrece asesoramiento y asistencia técnica para resolver problemas de ciberseguridad. Otros países pueden considerar la introducción de servicios similares para proporcionar un canal de comunicación directo y seguro para las personas mayores que necesitan ayuda en línea. Estos servicios proporcionan a las personas mayores un canal de comunicación directo y seguro para obtener ayuda con problemas de ciberseguridad, como fraude en línea o malware. La introducción de servicios similares en otros países puede ser una importante red de apoyo para proteger a las personas mayores en el mundo digital.

Por ejemplo, en el territorio europeo, la asociación AGE UK[6] prioriza el apoyo a las personas mayores más vulnerables a la exclusión digital.

Además de prestar servicios a la población anciana, los cursos se centrarán específicamente en ayudar a un grupo de alto riesgo a acceder al mundo digital. Aunque los componentes básicos del programa permanecerán en gran medida sin cambios mientras se trabaja con estos grupos de alto riesgo, es probable que sean necesarios algunos ajustes para garantizar que el programa siga siendo accesible y eficaz para aquellos que más lo necesitan.

Los servicios de alto riesgo del Programa Digital Champion estarán dirigidos a personas mayores que:

- Tener demencia y/o pérdida de memoria
- Tener un ingreso bajo
- Vivir solo
- Tienen problemas de movilidad
- Están confinados en casa.

4.2.4 Campañas de sensibilización y educación

Países como Australia y Canadá han implementado campañas de ciberseguridad y programas de educación en seguridad digital para adultos mayores. Estas campañas proporcionan información sobre amenazas cibernéticas comunes, consejos sobre cómo protegerse del fraude en línea y la importancia de mantener sus dispositivos actualizados. Los gobiernos pueden asociarse con organizaciones locales, centros comunitarios y grupos de voluntarios para llegar a la población mayor y proporcionar capacitación en habilidades digitales. Estas campañas de información y educación tienen como objetivo empoderar a las personas mayores a través de la educación en seguridad digital. Se les enseña cómo identificar y evitar el fraude en línea, proteger su información personal y utilizar herramientas de seguridad como antivirus y contraseñas seguras. También están informados sobre los riesgos asociados con el uso de las redes sociales y la importancia de una configuración de privacidad en línea adecuada. La asociación mencionada anteriormente ACDA en París también ofrece cursos de Seguridad Digital.

[6] https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/

Otra asociación que se centra en la conciencia digital es la Fundación Orange, que informa a los grupos frágiles sobre lo último en tecnología y los dirige a un uso digital más seguro[7].

Además, la Fundación Orange ha organizado una serie de cursos gratuitos de formación digital en toda Francia para jóvenes y mujeres que a menudo están desempleados, carecen de cualificaciones y, a veces, en situaciones precarias. Al capacitar a estas personas en habilidades digitales, les ayudan a re-socializar, buscar un trabajo, adoptar los usos profesionales de la tecnología digital, desarrollar un negocio o incluso hacer digital su profesión.

4.2.5 Programas de Protección Financiera

Países como el Reino Unido[8] y Estados Unidos han introducido políticas para proteger a los jubilados de las estafas financieras en línea. Estas políticas incluyen límites de responsabilidad para las víctimas de fraude y recursos para recuperar fondos robados. Otros países pueden explorar estas iniciativas y adaptarlas a sus sistemas financieros para proteger a las personas mayores contra posibles pérdidas financieras. La protección financiera para los adultos mayores es una parte importante de la seguridad digital. Los programas diseñados específicamente para prevenir y mitigar el fraude financiero en línea pueden proporcionar a esta población un mayor nivel de seguridad. El establecimiento de límites a la responsabilidad de las víctimas del fraude y la creación de mecanismos para recuperar el dinero robado son medidas que pueden adoptarse. Estas políticas no solo protegen el bienestar financiero de los adultos mayores, sino que también envían un mensaje claro de que su bienestar y seguridad financiera se toman en serio.

En Europa, el establecimiento de límites a la responsabilidad de las víctimas del fraude es un aspecto vital para salvaguardar el bienestar financiero de los adultos mayores. Cuando se responsabiliza a las víctimas de fraude por las pérdidas financieras que sufren, puede tener graves consecuencias, como la ruina financiera y la angustia emocional. Mediante la aplicación de políticas que establecen límites razonables a la responsabilidad, la sociedad reconoce las vulnerabilidades singulares que enfrentan los adultos mayores y trata de aliviar la carga que se les impone. Esta medida proporciona una red de seguridad que garantiza que los adultos mayores no se vean sobrecargados injustamente con las repercusiones de las actividades fraudulentas. El establecimiento de límites a la responsabilidad de las víctimas de fraude es un aspecto clave para salvaguardar el bienestar financiero de las personas de edad. En suelo europeo, muchas asociaciones se dedican a proteger a las personas mayores que a menudo son víctimas de fraude en línea, que carecen de conciencia y pueden sufrir pérdidas financieras. Una de estas asociaciones es Marketing Management IO (MMIO), una agencia certificada en España y Francia[9].

Cuando se responsabiliza a las víctimas de fraude por sus pérdidas financieras, esto puede tener graves consecuencias. De ahí la importancia de la sensibilización. Al aplicar políticas que establecen límites razonables a la responsabilidad, la sociedad reconoce las vulnerabilidades singulares de las personas de edad y trata de aliviar la carga que soportan. Esta medida proporciona una red de seguridad que garantiza que las personas mayores no se vean injustamente agobiadas por las repercusiones de las actividades fraudulentas.

---

[7] https://fondationorange.com/en/digital-solidarity

[8] https://www.bankofamerica.com/signature-services/elder-financial-services/

[9] https://www.marketing-management.io/blog/formation-digital-marketing

Marketing Management IO (MMIO) incluye temas como oportunidades de Internet, referencias naturales, visibilidad en línea, marketing de contenidos y aumento de las ventas. Los conceptos se simplifican y las acciones son gratuitas. También hay disponibles recursos adicionales.

El curso incluye 5 lecciones con videos. Facebook ofrece una plataforma con acceso gratuito a más de 70 cursos en línea. Estos cursos se centran específicamente en el uso de Facebook para mejorar su presencia en línea y las ventas de negocios, la seguridad y la conciencia.

4.2.6 Colaboración con la industria tecnológica

Algunos países, como los Estados Unidos, se han asociado con empresas de tecnología para abordar los problemas de seguridad digital asociados con el envejecimiento de la población. Esta colaboración puede incluir la mejora del software de seguridad, la mejora de la detección de fraudes y la implementación de funciones de seguridad en productos y servicios digitales. La colaboración con la industria de la tecnología puede ser una forma eficaz de mantenerse al día de las últimas amenazas y soluciones de seguridad, como la implementación de tecnologías de seguridad avanzadas, la mejora de la detección de fraude, y promover prácticas de seguridad para productos y servicios digitales destinados a las personas mayores. La colaboración con la industria tecnológica garantiza una respuesta más rápida y actualizada a las amenazas digitales.

Otros países como Francia e Inglaterra tienen cursos de seguridad digital para ayudar a las personas mayores a entender las tecnologías de defensa; los cursos ofrecidos les permiten construir una base en la digitalización y entender cómo navegar de forma segura por Internet.

Por ejemplo, Konexio ofrece formación en habilidades digitales - desde las más básicas hasta las más avanzadas - para promover la integración social y profesional. Innovadores, basados en casos prácticos y con un fuerte énfasis en las habilidades transversales y relacionales o en las habilidades interpersonales, nuestros cursos de formación tienen como objetivo permitir que todos se incluyan en la digitalización de la sociedad. Ofrecen diversas formaciones: habilidades digitales, diseñador web, técnico de sistemas y redes, ayudantes digitales. El programa se centra en el aprendizaje de las habilidades blandas y los códigos sociales del mundo profesional a través de talleres. También ofrece oportunidades de conexión directa con el mundo profesional a través de nuestra red. Ofrece seguimiento regular y apoyo personalizado para ayudar a nuestros alumnos a progresar y resolver cualquier dificultad que puedan encontrar.

4.2.7 Recursos, informes e iniciativas internacionales

Estos recursos proporcionan una valiosa orientación y buenas prácticas para mejorar la seguridad digital en la educación de adultos en la UE.

Un ciberespacio abierto, seguro y protegido: Este informe ofrece una visión general de la estrategia de ciberseguridad de la UE, cuyo objetivo es promover un ciberespacio abierto, seguro y seguro en Europa. El informe incluye las mejores prácticas para mejorar la ciberseguridad, incluida la gestión de riesgos, la respuesta a incidentes y las asociaciones público-privadas.

Informe sobre el panorama de amenazas de la ENISA: Este informe de la Agencia de Ciberseguridad de la Unión Europea (ENISA) ofrece una visión general del panorama actual de amenazas a la ciberseguridad en Europa, incluidos los tipos más comunes de ciberataques y los sectores de mayor riesgo. El informe incluye las mejores prácticas para prevenir y mitigar los ataques cibernéticos, incluida la capacitación en

materia de concienciación sobre la seguridad, la gestión de la vulnerabilidad y la planificación de la respuesta a incidentes.

Directiva NIS y Ley de Ciberseguridad de la UE: Este informe proporciona una visión general del marco legal de la UE para la ciberseguridad, incluyendo la Directiva de Redes y Sistemas de Información (NIS) y la Ley de Ciberseguridad de la UE. El informe incluye las mejores prácticas para cumplir con los requisitos legales, como la notificación de incidentes y la gestión de riesgos.

Marco de certificación de ciberseguridad de la UE: Este informe ofrece una visión general del marco de certificación de ciberseguridad de la UE, cuyo objetivo es mejorar la seguridad y la fiabilidad de los productos y servicios digitales. El informe incluye las mejores prácticas para obtener y mantener certificaciones de ciberseguridad, incluida la seguridad mediante el diseño, las pruebas y la evaluación, y el seguimiento y la evaluación permanentes.

Ciberseguridad para las PYME: Este informe proporciona orientación y mejores prácticas para las pequeñas y medianas empresas (PYME) sobre cómo mejorar su postura en materia de ciberseguridad. El informe incluye asesoramiento sobre gestión de riesgos, capacitación en materia de conciencia de seguridad, desarrollo de software seguro y planificación de la respuesta a incidentes.

Competencias digitales en la población adulta: Este informe de la Comisión Europea ofrece una visión general de las competencias digitales de la población adulta en la UE. Incluye una sección sobre seguridad digital, que destaca la necesidad de que los adultos tengan conocimientos y habilidades básicas para protegerse de las amenazas cibernéticas.

Competencias digitales para el aprendizaje permanente: Este informe de la Comisión Europea proporciona orientación y mejores prácticas para desarrollar competencias digitales entre los adultos. Incluye una sección sobre seguridad digital, que proporciona asesoramiento sobre gestión de riesgos, navegación segura, gestión de contraseñas y protección de datos.

El proyecto Ciberseguridad para la educación digital: este proyecto de la European Schoolnet proporciona recursos y formación sobre ciberseguridad para profesores y alumnos en Europa. El proyecto incluye una serie de materiales, incluidos cursos en línea, planes de lecciones y herramientas de evaluación, todos centrados en mejorar la seguridad digital en la educación.

El Proyecto de Seguridad Digital para la Tercera Edad: Este proyecto de la Agencia de Ciberseguridad de la Unión Europea (ENISA) proporciona recursos y formación sobre ciberseguridad para las personas mayores. El proyecto incluye una variedad de materiales, incluyendo cursos en línea, guías y videos, todos centrados en mejorar la seguridad digital entre los adultos mayores.

Digital Skills and Jobs Coalition: Esta iniciativa de la Comisión Europea tiene como objetivo mejorar las competencias digitales de los europeos para que puedan participar plenamente en la economía digital. Incluye una serie de recursos y oportunidades de formación, incluida la seguridad digital.

4.3 Mejores prácticas de la educación de adultos en materia de seguridad digital

ENISA Programa de formación de formadores

Todos los materiales de formación en línea y los cursos de formación en la sección 'Cursos de formación para especialistas en seguridad cibernética' se basan en la filosofía 'Formar al formador'. El

programa y la filosofía 'Formar al Formador' tienen como objetivo ampliar la red de formadores y promover un mejor intercambio de información. Esto servirá para varios propósitos, incluyendo:

- Compartir materiales de capacitación para ahorrar tiempo y dinero en la capacitación,
- Creación de actividades regionales de capacitación,
- Fomentar la cooperación entre los diferentes proveedores de formación;
- Promover buenas prácticas de formación,
- Reducir la competencia y la duplicación.

Los materiales de formación en línea de la ENISA incluirán un manual para formadores, un conjunto de herramientas para estudiantes y máquinas virtuales para descargar. Esto permite a los posibles instructores preparar el curso, y el Manual les ayudará a guiar a los estudiantes a través del curso. Contendrá hojas de trucos, pequeñas pruebas potenciales para ver si los estudiantes han comprendido las lecciones importantes de los cursos, e información adicional o ejercicios que el entrenador puede usar para hacer el curso más interesante o desafiante.

Aprender de los éxitos y fracasos de los demás permite que tanto los entrenadores novatos como los experimentados diseñen y entreguen entrenamientos mejores, haciéndolos más exitosos, más "divertidos" y con resultados mejores y más duraderos.

TiK - Tecnología en breve

El proyecto de alta tecnología sigue un enfoque intergeneracional a través de la formación ofrecida por jóvenes voluntarios (de 16 a 30 años) como los llamados "Tablet-Entrenadores", que son educados a lo largo de un plan de estudios especial tableta-educación. Los cursos tienen la distinción de una multitud de métodos y preguntas flexibles y un compromiso especial de los jóvenes formadores. Ofrecen cursos de bajo umbral voluntariamente por solo una pequeña asignación de gastos. El desarrollo ulterior de los cursos está garantizado por los comentarios de los participantes y los instructores, que también elaboraron materiales especiales y folletos para las personas de edad. Los cursos son de fácil acceso para los interesados y se presta mucha atención a una amplia distribución geográfica de los "módulos TiK" y de la información sobre www.digitaleseniorinneen. Los participantes en los cursos son personas y especialmente mujeres económicamente desfavorecidas de bajo nivel educativo. Hasta finales de 2018 más de 2000 personas aprendieron con los módulos y otras 1000 personas participaron en el curso-programa. El participante más viejo que acaba de tomar parte en un curso es 97 años de edad, él recibe su educación por un joven en una guardería. El proyecto fue adjudicado varias veces a nivel federal y provincial.

5 Formación de adultos: cómo desarrollar la resiliencia digital

La andragogía como estudio del aprendizaje de adultos se originó en Europa en la década de 1950, pero no fue hasta la década de 1970 que fue pionera como teoría y modelo del aprendizaje de adultos por Malcolm Knowles, un practicante y teórico estadounidense de la educación de adultos, que definió la andragogía como "el arte y la ciencia de ayudar a los adultos a aprender" (Fidishun 2000). Fidishun (2000) sugirió que los principios andragógicos se utilicen en el diseño de clases en línea para facilitar "la flexibilidad y la capacidad de los estudiantes para moverse a través de las lecciones cuando, donde y a su propio ritmo."

5.1 Cuatro principios de la andragogía

Teniendo en cuenta que los adultos tienen su propia forma única de aprender, hay 4 principios centrales que explican cómo desarrollar mejor la formación para ellos.

- Cuando se trata de aprender, los adultos quieren o necesitan involucrarse en cómo se planifica, imparte y ejecuta su entrenamiento. Quieren controlar qué, cuándo y cómo aprenden.
- Los adultos ganan más cuando pueden llevar experiencias pasadas al proceso de aprendizaje. Pueden recurrir a lo que conocían anteriormente para añadir mayor contexto a su aprendizaje.
- Memorizar datos e información no es la forma correcta de que los adultos aprendan. Necesitan resolver problemas y usar el razonamiento para comprender mejor la información que se les presenta.
- Los adultos quieren saber "¿Cómo puedo usar esta información ahora?". Lo que están aprendiendo necesita ser aplicable a sus vidas y ser implementado inmediatamente.

5.2 Cómo los entrenadores adultos implementarán la andragogía

Habilitar el aprendizaje autónomo

En el pasado, el aprendizaje ha sido a menudo una actividad obligatoria realizada en un momento determinado. Ahora, con tecnologías como un sistema de gestión del aprendizaje, podemos crear un entorno de aprendizaje mucho más autónomo e independiente para los estudiantes adultos. Podemos permitirles entrenar cuando y donde quieran, ofrecerles una selección de cursos que pueden elegir para inscribirse y permitirles tener sus propios objetivos de aprendizaje.

Usando ejemplos de aprendizaje en el mundo real

Como afirma la teoría, a los adultos les gusta saber cómo el entrenamiento tendrá una aplicación inmediata y un beneficio para ellos. Por lo tanto, al crear el contenido del curso, debemos inyectarlo con tantos ejemplos del mundo real como sea posible.

Cuando entrene a estudiantes adultos en bienestar digital y/o seguridad digital, guíelos paso a paso a través de un flujo de trabajo que realmente usarán y explícitamente indicará cómo y por qué lo usarían. Indique cómo ayudará la capacitación y luego use ejemplos genuinos para entrenar.

Dejar que los estudiantes adultos lo resuelvan por sí mismos

Dado que los adultos prefieren resolver problemas antes que solo los hechos, al crear contenido es una buena idea no solo presentar todas las respuestas de inmediato. ¿Por qué no ser creativo en su lugar y construir cursos que pongan en marcha el cerebro de tus alumnos?

Podemos hacer esto de algunas maneras simples, incluyendo la adición de evaluaciones y simulaciones que esbozan problemas específicos que un alumno podría realmente encontrar, y luego conseguir que los estudiantes adultos usen sus habilidades para superarlo.

6 Conclusión

La seguridad digital de las personas mayores es una cuestión clave que requiere la atención y la acción de los gobiernos y la sociedad en general. Mediante la aplicación de las buenas prácticas mencionadas, los países pueden mejorar la protección digital y el bienestar de su población que envejece. La sensibilización, la educación, el apoyo dedicado, la adaptación tecnológica y la colaboración de la industria son pilares clave para garantizar una experiencia en línea segura y positiva para los adultos mayores.

El proyecto DigiWELL tiene como objetivo incorporar los principios del bienestar digital en la educación de adultos. Sus iniciativas están encaminadas a contribuir a las prácticas generales de las organizaciones, redes e iniciativas de educación de adultos. El proyecto entiende lo crucial que es abordar cómo la tecnología está afectando la salud mental, la productividad y el bienestar general de los adultos en la era digital. El objetivo principal de DigiWELL es proporcionar a los estudiantes adultos la información, las habilidades y los recursos necesarios para navegar ética y concienzudamente por el mundo digital. El proyecto DigiWELL también incluye la creación y ejecución de nuevas iniciativas de empoderamiento de los alumnos adultos. El objetivo de estas actividades es proporcionar un entorno de apoyo donde los adultos puedan compartir sus experiencias, dificultades y triunfos en la promoción del bienestar digital. Con esto en mente, el proyecto DigiWELL presenta muchas oportunidades para que las personas y las organizaciones de adultos sean conscientes e iluminadas sobre la importancia del bienestar digital y sobre cómo promover el bienestar digital de las personas adultas y los educadores y formadores de adultos. Permitir el bienestar digital con un enfoque holístico es mucho más posible si todas las partes relevantes toman medidas para apoyar las necesidades de bienestar digital de las personas. En consecuencia, la información, consejos y buenas prácticas presentadas en este manual invitan a las personas y organizaciones interesadas a tomar iniciativas para que más de nosotros tengamos un mejor bienestar digital y también vidas digitales más fuertes.

7 References

En la elaboración del diccionario se utilizaron recursos en línea disponibles de forma gratuita: diccionarios en línea, artículos científicos y literatura en el campo de la seguridad de la información, tecnologías y servicios digitales, bienestar digital y resiliencia digital, así como términos y definiciones del tema Información. seguridad. Todas las fuentes están enumeradas en la base de datos de texto de la versión funcional del diccionario.

1 BAI. Committee on National Security Systems (CNSS) Glossary (2015). In *BAI Information Security Consulting & Training [online]*. Retrieved from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Capterra Glossary*. Capterra. (n.d.). https://www.capterra.com/glossary/

3 CSRC. (n.d.). *Glossary*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

4 *Cybersecurity glossary of terms*. Global Knowledge. (n.d.). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Glossary*. DigitalHealthEurope. (n.d.). https://digitalhealtheurope.eu/glossary/

6 *Glossary*. The Digital Wellness Lab. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (n.d.). *ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security*. Online browsing platform (OBP) - ISO. https://www.iso.org/obp/ui/iso

8 Jirásek, P., Novák, L., Požár, J., & Vavruška, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Cyber security glossary*. *Fifth edition.* Praha: Česká pobočka AFCEA, 2022. p. 352, ISBN 978-80-908388-4-0

9 Kissel, R. L. (2019, July 16). *Glossary of key information security terms*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-1

10 MF SR. (n.d.). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK*. CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, R. D. (2021). *Glossary of key information security terms*. NIST. Retrieved from: https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, L. V. (2015). *Computer security: Principles and practice*. *Third edition.* Boston, MA: Pearson, 2015. p.838. ISBN 978-0-13-377392-7. Pearson.

13 *TVETipedia Glossary*. UNSECO-UNEVOC. (n.d.) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Fidishun, D. (2000). Teaching adult students to use computerized resources: Utilizing Lawler's keys to adult learning to make instruction more effective. *Information technology and libraries*, *19*(3), 157-157.

15 European Commission, Directorate-General for Education, Youth, Sport and Culture, Key competences for lifelong learning, Publications Office, 2019, https://data.europa.eu/doi/10.2766/569540