

KA210-ADU Small-Scale Partnership in Adult Education

Empoderamiento de los adultos: seguridad digital y prevención del fraude en la era de la tecnología |



digisAFE

Project Number:

2025-1-IT02-KA210-ADU-000359787

Informe transnacional



Open License Notice

This document is licensed under the Creative Commons Attribution 4.0 International (CC BY 4.0).

Acrónimo del proyecto	digiSAFE
Título del proyecto	Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology (Empoderamiento de los adultos: seguridad digital y prevención del fraude en la era de la tecnología)
Número del proyecto	2025-1-IT02-KA210-ADU-000359787
Duración	Fecha de inicio: 01-09-2025 Fecha de finalización: 31-08-2027
Subprograma	Asociación a pequeña escala en educación de adultos
Página web del proyecto	www.digisafeproject.eu
Fecha de entrega	
Estado	Versión 1.0
Autor	UNO
Autor responsable	

Índice

Índice.....	3
1. Introducción.....	4
2. Metodología.....	5
3. Contexto nacional.....	7
4. Buenas prácticas.....	17
5. Análisis de los Resultados de la Encuesta.....	49
6. Análisis Transnacional.....	59
7. Conclusiones principales.....	63
8. Deficiencias detectadas y necesidades de formación.....	64
9. Recomendaciones para el desarrollo curricular.....	66
10. Conclusión.....	70
Bibliografía / Referencias.....	71

1. Introducción

El proyecto digiSAFE —«Empoderamiento de los adultos: seguridad digital y prevención del fraude en la era de la tecnología»— es una asociación a pequeña escala de Erasmus+ en el ámbito de la educación de adultos (KA210-ADU, acuerdo de subvención n.º 2025-1-IT02-KA210-ADU-000359787) ejecutado por un consorcio transnacional formado por tres organizaciones asociadas: Associazione Italiana Socio-Educatori per la Cooperazione – AISEC APS (Italia, coordinadora del proyecto), Asociación UNO (España) e IKREON (Eslovaquia). El proyecto se desarrolla entre el 1 de septiembre de 2025 y el 31 de agosto de 2027.

La transformación digital está cambiando prácticamente todos los aspectos de la vida cotidiana en toda Europa, desde la forma en que los ciudadanos acceden a los servicios públicos y gestionan sus finanzas personales hasta cómo se comunican y consumen información. Si bien la digitalización ofrece oportunidades innegables, también genera riesgos nuevos y en rápida evolución, en particular el fraude en línea, la ciberdelincuencia, la desinformación y la violación de datos. Los adultos de más de 45 años se ven afectados de manera desproporcionada por estos riesgos, ya que a menudo combinan un alto nivel de participación digital con una conciencia limitada sobre la ciberseguridad y un acceso insuficiente a formación específica en seguridad digital.

El proyecto digiSAFE se concibió para abordar directamente esta brecha. Sus principales resultados son un plan de estudios de educación no formal (ENF) centrado en la seguridad digital y la prevención del fraude, y un kit de herramientas práctico para la prevención del fraude digital, ambos diseñados específicamente para adultos mayores de 45 años. Para fundamentar estos resultados en datos empíricos, la primera fase del proyecto incluyó una investigación nacional exhaustiva en los tres países socios. Este informe transnacional sintetiza y compara los resultados de esa investigación nacional y constituye el principal resultado de la Actividad A1 (fase de evaluación de necesidades), proporcionando la base empírica para el desarrollo del plan de estudios y el conjunto de herramientas.

El presente documento tiene por objeto consolidar y analizar los resultados de las investigaciones nacionales de Italia, España y Eslovaquia, y comparar las conclusiones de los tres países con el fin de identificar tendencias comunes, diferencias significativas y patrones transnacionales. Además, pretende identificar las lagunas de aprendizaje específicas y las necesidades de formación de los adultos mayores de 45 años en relación con la seguridad digital, la prevención del fraude en línea y la concienciación sobre la ciberseguridad, al tiempo que ofrece recomendaciones basadas en datos empíricos para orientar el diseño del plan de estudios de educación no formal (NFE) de digiSAFE y del kit de herramientas para la prevención del fraude digital.

El público objetivo al que se dirige este informe está formado por adultos de 45 años o más, con especial atención a las personas con niveles bajos o medios de competencias digitales que son más vulnerables a los riesgos en línea. Este grupo es cada vez más activo en los entornos digitales, pero a menudo carece de las competencias, la confianza y la concienciación necesarias para desenvolverse en ellos de forma segura y autónoma.

En este contexto, el informe se alinea con las prioridades clave de Erasmus+ y de la Unión Europea en general, concretamente con las relacionadas con la transformación digital, la inclusión social y el aprendizaje permanente, al apoyar el desarrollo de enfoques educativos inclusivos y accesibles para los estudiantes adultos.

2. Metodología

La investigación en la que se basa este informe transnacional se llevó a cabo simultáneamente en los tres países socios durante la primera fase del proyecto digiSAFE (finales de 2025 – principios de 2026). Se adoptó una metodología compartida y armonizada para garantizar la comparabilidad de los datos y los resultados entre los distintos contextos nacionales. Esta metodología se basó en un marco de investigación común desarrollado a nivel del proyecto, siendo el socio principal de la Actividad A1 (Asociación UNO) el responsable de preparar las directrices de investigación, que fueron aplicadas de manera coherente por todos los socios en los tres países. La investigación combinó dos enfoques complementarios: la investigación documental y una encuesta cuantitativa de autoevaluación.

2.1 Investigación documental

Cada socio nacional llevó a cabo una revisión exhaustiva de fuentes secundarias, incluyendo datos estadísticos oficiales, documentos de política nacional, instrumentos legislativos, informes de la Comisión Europea y literatura académica y gris, seleccionados en función de su relevancia y fiabilidad de acuerdo con las directrices de la investigación. Además de trazar un mapa del contexto nacional a nivel macro, los socios también identificaron un conjunto de buenas prácticas nacionales para orientar el desarrollo de los resultados del proyecto. La investigación documental tenía por objeto ofrecer una visión general completa de cada país, incluyendo el estado actual de la alfabetización digital entre los adultos mayores de 45 años, los marcos normativos existentes que regulan la protección de datos y la ciberseguridad, y los programas o iniciativas activos que promueven la educación digital para adultos y la seguridad en línea. Las fuentes utilizadas se documentan en los informes nacionales y se recogen en la sección de bibliografía del presente documento.

2.2 Cuestionario de autoevaluación

Se distribuyó un cuestionario cuantitativo estandarizado de autoevaluación entre adultos de más de 45 años en cada país socio. Se utilizó el mismo cuestionario en todos los países para garantizar la comparabilidad de los resultados. El instrumento utilizaba una combinación de escalas de 5 puntos y preguntas de opción múltiple para evaluar los hábitos digitales cotidianos de los participantes, la confianza que ellos mismos percibían en los entornos en línea, habilidades específicas de seguridad digital, el conocimiento de diversos tipos de amenazas en línea, la experiencia directa con el fraude digital y las necesidades de formación percibidas. El objetivo principal de la encuesta era identificar las competencias digitales, los niveles de concienciación sobre los riesgos y las necesidades de formación entre los adultos mayores de 45 años.

La encuesta se difundió en línea a través de las redes de cada socio mediante canales de comunicación adaptados para llegar al grupo demográfico objetivo. La recopilación de datos se llevó a cabo de forma voluntaria y totalmente anónima, de conformidad con el Reglamento General de Protección de Datos (RGPD). Se estableció un objetivo mínimo de al menos 50 respuestas válidas por país, tal y como se definió en la propuesta del proyecto, para garantizar la fiabilidad de los datos y la comparabilidad de los resultados en los tres contextos nacionales.

2.3 Participantes

Los datos de la encuesta se recopilaban en los tres países socios, y cada país aportó un tamaño de la muestra comparable, lo que garantizó una base equilibrada para el análisis transnacional. En las tres muestras, las mujeres constituían la mayoría de los encuestados. La distribución por edades se concentró en los grupos de 45 a 54 y de 55 a 64 años, con una representación menor de encuestados mayores de 65 años. Los participantes procedían de una mezcla de contextos urbanos, semiurbanos y rurales, y presentaban diversas trayectorias educativas y laborales, incluyendo adultos empleados, autónomos y jubilados. En general, la muestra refleja un grupo diverso de adultos mayores de 45 años, lo que refuerza la relevancia y la representatividad de los resultados.

2.4 Análisis de datos

Cada socio analizó de forma independiente los conjuntos de datos nacionales utilizando métodos estadísticos descriptivos. El análisis se centró en la frecuencia, la distribución de las respuestas y la identificación de patrones recurrentes dentro de cada muestra nacional. En particular, los socios examinaron variables clave como los niveles de uso digital, la confianza en uno mismo, la conciencia de los riesgos en línea, las experiencias con el fraude digital y las necesidades de formación expresadas.

Para garantizar la coherencia, se siguió un enfoque analítico común en todos los países, lo que permitió una comparación estructurada de los resultados. A continuación, los resultados se examinaron a nivel transnacional mediante comparaciones entre países, destacando tanto las similitudes como las diferencias en los comportamientos, las percepciones y las vulnerabilidades de los participantes. Se prestó especial atención a la identificación de patrones relevantes para el diseño de intervenciones educativas, incluyendo áreas de necesidad compartida y retos específicos de cada país.

El presente informe sintetiza estos análisis y extrae conclusiones transnacionales basadas en la evidencia combinada, proporcionando una base coherente para el desarrollo del plan de estudios y el kit de herramientas de digiSAFE.

3. Contexto nacional

Este apartado ofrece una visión general comparativa del panorama digital para adultos mayores de 45 años en cada país socio. Para cada país, el análisis abarca el estado actual de la alfabetización digital, los principales retos a los que se enfrenta el grupo destinatario, las normativas y políticas nacionales pertinentes, y los programas e iniciativas existentes.

3.1 Italia

Alfabetización digital y principales retos

Italia presenta una paradoja llamativa: aunque se han logrado avances significativos en la infraestructura digital y la implantación de los servicios públicos digitales, persisten las brechas estructurales en las competencias digitales de los ciudadanos, especialmente entre los adultos mayores. Según el informe nacional sobre el estado de la Década Digital 2025 de la Comisión Europea, Italia ha avanzado en conectividad y administración electrónica; sin embargo, siguen existiendo retos críticos en la capacidad de los ciudadanos para utilizar las tecnologías digitales de forma eficaz y segura.

Los datos del ISTAT confirman esta doble tendencia. En 2024, el 86,2 % de los hogares italianos tenía acceso a Internet, pero esta cifra se reduce al 60,6 % entre los hogares compuestos exclusivamente por personas mayores. El uso de Internet varía significativamente según la edad: mientras que el 81,9 % de la población total de 6 años o más utilizó Internet en los tres meses anteriores, solo lo hizo el 68,1 % de las personas de entre 65 y 74 años. Las disparidades regionales agravan aún más este panorama, ya que las regiones del sur se quedan rezagadas con respecto al centro y el norte de Italia tanto en acceso como en uso.

Los niveles de competencias digitales entre las personas mayores siguen siendo una preocupación fundamental. En 2023, solo el 45,9 % de las personas de entre 16 y 74 años que utilizaban Internet poseía al menos competencias digitales básicas. La proporción se sitúa en un 48,7 % entre las personas de 45 a 54 años, en un 38,5 % entre aquellos de 55 a 64 años y en un mero 19,3 % entre los mayores de 65 a 74 años. Como resultado, muchos adultos del grupo de más de 45 años tienen dificultades para acceder de forma autónoma a los servicios digitales, evaluar la información en línea y protegerse de los riesgos en Internet.

El fraude en línea y la ciberdelincuencia representan una preocupación creciente y concreta. El ISTAT estima que aproximadamente 1,7 millones de personas —lo que corresponde al 3,3 % de los usuarios de Internet— sufrieron fraudes o estafas en línea en los 12 meses anteriores a la encuesta de 2022-2023. Los casos de fraude financiero a través de la banca en línea aumentaron un 74 % en comparación con 2015-2016. En 2024, la plataforma Commissariato di PS Online registró alrededor de 3 millones de visitas, más de 82 000 denuncias y aproximadamente 23 000 solicitudes de asistencia relacionadas con el phishing y las estafas en línea.

Estos datos indican que, para los adultos mayores de 45 años, el problema ya no es solo el acceso, sino la calidad y la autonomía del uso digital.

Normativa y políticas nacionales

Italia ha desarrollado un marco normativo y político integral en materia de seguridad digital. La protección de datos se rige por el Reglamento (UE) 2016/679, que se aplica a nivel nacional mediante el Decreto Legislativo italiano n.º 196/2003 en su versión modificada, bajo la supervisión de la Autoridad Italiana de Protección de Datos (Garante per la protezione dei dati personali). El Código de Administración Electrónica establece los derechos digitales de los ciudadanos en sus interacciones con las administraciones públicas, mientras que la Agencia para la Italia Digital (AgID) promueve la ciudadanía digital y la denuncia de infracciones. La ciberseguridad se coordina a través de la Estrategia Nacional de Ciberseguridad 2022-2026, gestionada por la Agencia Nacional de Ciberseguridad (ACN). Italia también ha transpuesto la Directiva NIS2 mediante el Decreto Legislativo n.º 138/2024 y ha aplicado el Reglamento de Resiliencia Operativa Digital (DORA) en el sector financiero.

Programas e iniciativas existentes

Además de las medidas normativas, Italia ha desarrollado una amplia gama de programas e iniciativas para apoyar la inclusión y la educación digital de los adultos. Repubblica Digitale, una iniciativa nacional liderada por el Departamento de Transformación Digital, desempeña un papel central, ya que coordina la Estrategia

Nacional de Competencias Digitales y promueve la colaboración entre instituciones públicas, actores del sector privado y organizaciones de la sociedad civil. En este marco, la Red de Facilitación Digital tiene como objetivo llegar a dos millones de ciudadanos para 2026 a través de 4000 puntos de acceso físicos (Punti Digitale Facile), proporcionando apoyo para acceder a los servicios digitales y mejorando la seguridad en línea.

Otras iniciativas incluyen el Servizio Civile Digitale y programas de financiación específicos como Dritti al Punto, que apoyan actividades de formación centradas en la concienciación sobre la ciberseguridad, el uso crítico de la información y el acceso seguro a los servicios digitales públicos. Paralelamente, las políticas del mercado laboral, como el Programa GOL (Garanzia di Occupabilità dei Lavoratori), pretenden involucrar a tres millones de beneficiarios, con un fuerte énfasis en el desarrollo de las competencias digitales.

La formación de adultos cuenta además con el apoyo de los Centros Provinciales de Educación de Adultos (CPIA), que actúan como centros territoriales clave para el aprendizaje permanente. Estos centros ofrecen oportunidades de educación tanto formal como no formal y desempeñan un papel crucial a la hora de llegar a los grupos vulnerables, incluidos los adultos mayores con bajos niveles de educación o competencias digitales. Su función se inscribe en políticas más amplias que promueven el aprendizaje permanente y el desarrollo de competencias en toda la población.

Por último, una amplia gama de actores institucionales y sectoriales contribuye a la sensibilización y a la promoción de un comportamiento seguro en línea. La Agencia para la Italia Digital (AgID) y la Agencia Nacional de Ciberseguridad (ACN) apoyan la difusión de competencias digitales y de ciberseguridad, mientras que la Policía Postal presta servicios de prevención y asistencia. La Agencia de Protección de Datos promueve la sensibilización sobre los derechos de privacidad, y las instituciones financieras, como el Banco de Italia, junto con iniciativas como I Navigati, contribuyen a educar a los ciudadanos sobre el fraude en línea y los riesgos de ciberseguridad financiera.

En general, el contexto italiano pone de manifiesto una brecha significativa entre la rápida digitalización de los servicios y la capacidad real de los adultos (especialmente los mayores de 45 años) para utilizar estas herramientas de forma segura y eficaz. Si bien el marco normativo e institucional está bien desarrollado, el principal reto sigue siendo garantizar que todos los ciudadanos, especialmente las personas mayores, adquieran las competencias necesarias para participar de forma plena y segura en la sociedad digital.

3.2 España

Alfabetización digital y principales retos

España ha experimentado una rápida transformación digital durante la última década, lo que ha redefinido las formas en que los ciudadanos interactúan con los servicios públicos, las instituciones financieras, los sistemas de salud y las plataformas de comunicación. La adopción generalizada de la banca en línea, las plataformas de administración electrónica, los servicios de salud digitales y las redes sociales ha aumentado significativamente la conectividad digital entre la población, mejorando tanto la accesibilidad como la eficiencia administrativa.

Sin embargo, a pesar de este progreso general, en España persiste una brecha digital. Esta brecha está estrechamente relacionada con la edad, el nivel educativo y las condiciones socioeconómicas. Los adultos de más de 45 años, y en particular los mayores de 55, tienden a manifestar menores niveles de confianza digital y un conocimiento más limitado de las prácticas de seguridad digital. Muchas personas de este grupo de edad no adquirieron competencias digitales durante su educación formal o su trayectoria profesional, lo que hace que la adaptación a entornos digitales en rápida evolución sea más compleja y, a menudo, más lenta.

Esta brecha generacional se refleja además en los patrones de uso digital y la exposición a los riesgos en línea. El fraude en línea y la ciberdelincuencia representan una preocupación cada vez más importante en el contexto español. Entre las amenazas más comunes se incluyen los correos electrónicos de phishing, los mensajes SMS fraudulentos, el robo de identidad, los servicios en línea falsos y las estafas financieras. Los adultos mayores de 45 años son especialmente vulnerables, ya que a menudo combinan el uso habitual de servicios digitales (como la banca en línea, las aplicaciones de mensajería y el comercio electrónico) con un menor conocimiento de los riesgos de ciberseguridad y las prácticas preventivas. Además, la creciente sofisticación de las técnicas de ingeniería social, incluido el uso de mecanismos de fraude basados en la inteligencia artificial, está intensificando aún más estas vulnerabilidades y dificultando su detección para los usuarios menos experimentados.

A nivel institucional, España ha desarrollado una serie de estrategias nacionales que abordan la transformación digital, la ciberseguridad y la inclusión digital. Estos marcos normativos tienen por objeto reforzar las competencias digitales de los ciudadanos, mejorar los mecanismos de protección de datos y promover un uso más seguro y responsable de las tecnologías digitales. Paralelamente a estas estrategias nacionales, las instituciones públicas, los gobiernos autonómicos y las organizaciones de la sociedad civil han puesto en marcha diversos programas de formación e iniciativas de sensibilización centrados en la alfabetización digital de los adultos y la seguridad en línea.

No obstante, las iniciativas existentes siguen estando fragmentadas y distribuidas de forma desigual entre las regiones. Además, muchos programas tienden a dar prioridad a la adquisición de competencias digitales básicas, mientras que prestan menos atención a

la seguridad digital, la prevención del fraude y la conciencia crítica sobre los riesgos en línea. Esta brecha pone de manifiesto la necesidad de intervenciones educativas más estructuradas, accesibles y específicas, diseñadas específicamente para mejorar la resiliencia digital entre los adultos de más de 45 años.

En este contexto, el proyecto digiSAFE responde directamente a estos retos combinando investigación, educación no formal y herramientas prácticas destinadas a reforzar las competencias en materia de seguridad en línea y a apoyar una participación más segura en la sociedad digital.

Normativa y políticas nacionales

La respuesta de España a la seguridad digital y la prevención del fraude se enmarca en un sistema de gobierno multinivel que combina la legislación nacional con marcos estratégicos más amplios destinados a fomentar la transformación e inclusión digitales. En los últimos años, el Gobierno español ha complementado cada vez más los enfoques normativos con estrategias nacionales integrales diseñadas para reducir las desigualdades digitales y reforzar las capacidades digitales de los ciudadanos, especialmente entre los grupos vulnerables, como los adultos mayores de 45 años.

Un pilar clave de este enfoque es la estrategia nacional «España Digital 2026», que actúa como hoja de ruta principal para la transformación digital del país. Esta estrategia promueve el crecimiento económico, la cohesión social y la inclusión territorial a través de la digitalización, al tiempo que aborda explícitamente las brechas digitales existentes relacionadas con la edad, el género y la geografía. Entre sus prioridades se encuentran la expansión de la infraestructura digital, la promoción de las tecnologías emergentes y el fortalecimiento de las competencias digitales de los ciudadanos como medio para garantizar que ningún grupo se quede atrás en la transición digital.

En este contexto, el Plan Nacional de Competencias Digitales desempeña un papel central en la promoción de la inclusión digital. Su objetivo es dotar a los ciudadanos, los trabajadores y las administraciones públicas de las competencias necesarias para desenvolverse en una sociedad cada vez más digital. El plan aborda específicamente las brechas estructurales en materia de alfabetización digital, que aún afectan a una parte significativa de la población, en particular a las personas mayores y otros grupos vulnerables. Sus medidas incluyen programas de formación a gran escala, iniciativas de reciclaje profesional y acciones para reducir las desigualdades de género y territoriales en el acceso a las competencias digitales.

Además, programas como la iniciativa UNICO Banda Ancha tienen como objetivo ampliar el acceso a Internet de alta velocidad en zonas rurales y desatendidas, reduciendo las disparidades territoriales y garantizando un acceso más equitativo a los servicios digitales

en todo el país. Estas iniciativas destacan la importancia de abordar no solo las competencias individuales, sino también las condiciones estructurales de acceso, como la conectividad.

Estas iniciativas estratégicas se inscriben en el marco más amplio del Plan de Recuperación, Transformación y Resiliencia, que integra la digitalización como pilar fundamental del desarrollo económico y social. A través de inversiones y reformas coordinadas, España busca no solo modernizar su economía, sino también garantizar un acceso inclusivo a las tecnologías y servicios digitales para toda la población.

Junto con estos marcos estratégicos, España ha desarrollado una sólida estructura jurídica en materia de seguridad digital. El marco jurídico básico lo establece la Ley Orgánica 3/2018, de Protección de Datos Personales y de Garantía de los Derechos Digitales (LOPD-GDD), que incorpora el Reglamento General de Protección de Datos (RGPD) al ordenamiento jurídico español. Estos instrumentos regulan el tratamiento y la protección de los datos personales, al tiempo que reconocen los derechos digitales como derechos fundamentales. Sin embargo, el conocimiento y la comprensión efectiva de estos derechos siguen siendo desiguales, especialmente entre los usuarios de más edad, que dependen cada vez más de los servicios digitales.

En el ámbito de la ciberseguridad, el Real Decreto-Ley 12/2018 y el Real Decreto 43/2021 transponen los requisitos europeos de ciberseguridad al ordenamiento jurídico nacional, reforzando la capacidad institucional de España para gestionar los riesgos digitales. Del mismo modo, el fraude en línea se aborda a través del Código Penal español (Ley Orgánica 10/1995), que tipifica como delito una amplia gama de delitos cibernéticos, incluidos el phishing y el robo de identidad. No obstante, la creciente sofisticación del fraude digital destapa la necesidad de medidas complementarias centradas en la prevención y la sensibilización de los usuarios.

La protección del consumidor y la regulación de las plataformas refuerzan aún más este contexto a través de instrumentos como el Real Decreto Legislativo 1/2007 y la Ley 34/2002 (LSSI), alineados con iniciativas europeas como la Ley de Servicios Digitales. Estas normativas mejoran la transparencia, la rendición de cuentas y la protección de los usuarios en los entornos digitales.

Por último, la rápida expansión de los servicios públicos digitales ha ido acompañada de iniciativas como el Plan de Digitalización de las Administraciones Públicas, cuyo objetivo es mejorar la accesibilidad, la eficiencia y la experiencia del usuario en las interacciones con las instituciones públicas. Sin embargo, aunque estos avances representan un progreso significativo, también pueden reforzar involuntariamente las desigualdades existentes si no van acompañados de medidas adecuadas de alfabetización digital. En particular, las personas mayores con competencias digitales limitadas pueden

enfrentarse a barreras adicionales a la hora de acceder a servicios esenciales que están cada vez más disponibles principalmente en línea.

En general, España combina un marco jurídico completo con un conjunto cada vez más sólido de estrategias nacionales orientadas a la transformación e inclusión digitales. Sin embargo, sigue existiendo una brecha significativa entre la existencia de estas políticas y su impacto efectivo en las prácticas digitales cotidianas de los ciudadanos. En particular, los adultos mayores de 45 años suelen carecer de los conocimientos y habilidades necesarios para beneficiarse plenamente de estas medidas. Esta brecha destaca la importancia de iniciativas educativas y de sensibilización como digiSAFE, que traducen los contextos normativos y estratégicos en conocimientos prácticos y competencias cotidianas.

Programas e iniciativas existentes

En España, varias iniciativas abordan la inclusión digital entre las personas mayores, especialmente en el marco de programas nacionales destinados a mejorar las competencias digitales de toda la población. Las iniciativas públicas promovidas por el Gobierno de España, así como los programas locales puestos en marcha por los ayuntamientos, las ONG y los centros de educación para adultos, ofrecen formación básica en alfabetización digital a las personas mayores, centrándose en el uso de los teléfonos inteligentes, la navegación por Internet y el acceso a los servicios públicos digitales. Por ejemplo, programas como los talleres de formación digital que se ofrecen en bibliotecas públicas y centros comunitarios proporcionan apoyo práctico a las personas mayores para que aprendan a utilizar aplicaciones móviles y a acceder a plataformas de administración electrónica. Además, las iniciativas promovidas en el marco del Plan Nacional de Competencias Digitales incluyen cursos básicos destinados a mejorar la autonomía digital de las personas mayores. Del mismo modo, las organizaciones no gubernamentales suelen organizar sesiones introductorias centradas en tareas digitales cotidianas, como la banca en línea o la reserva de citas médicas, lo que refuerza el uso práctico de las herramientas digitales.

Sin embargo, estas iniciativas tienden a dar prioridad a la inclusión digital general en lugar de a la seguridad digital. Las actividades de formación suelen centrarse en cómo utilizar las herramientas digitales, prestando poca atención a los riesgos asociados a los entornos en línea, como el fraude, el phishing o las estafas emergentes basadas en la inteligencia artificial. En España, el Instituto Nacional de Ciberseguridad (INCIBE) desempeña un papel clave, ya que actúa como punto de referencia nacional en materia de ciberseguridad. Esta institución pública ofrece campañas de sensibilización, recursos educativos y servicios de apoyo destinados a prevenir las ciberamenazas y a ayudar a los ciudadanos a hacer frente a los riesgos digitales. Sin embargo, a pesar del importante papel que desempeña el INCIBE, estas iniciativas suelen estar diseñadas para la

población en general y no se dirigen específicamente a los adultos mayores de 45 años a través de itinerarios de aprendizaje estructurados y continuos.

En general, aunque España ha desarrollado un marco nacional integral para la inclusión digital y la ciberseguridad, tal y como se describe en la sección 1.2, su aplicación práctica sigue siendo desigual. Las diferencias en el acceso a la formación, los niveles de alfabetización digital y la falta de programas dirigidos a grupos de edad específicos limitan la eficacia de estas políticas. Esta brecha entre los marcos normativos y los resultados prácticos deja en evidencia la necesidad de enfoques más inclusivos y personalizados. Como resultado, persiste una brecha significativa entre los esfuerzos de inclusión digital y el desarrollo de habilidades prácticas para la prevención del fraude entre las personas mayores. Esto remarca la necesidad de enfoques educativos específicos que combinen la alfabetización digital con la formación práctica en el reconocimiento y la respuesta a las amenazas en línea. En este contexto, digiSAFE aborda directamente esta brecha ofreciendo un modelo de aprendizaje personalizado y basado en escenarios, diseñado específicamente para adultos de más de 45 años.

3.3 Eslovaquia

Alfabetización digital y principales retos

La República Eslovaca se enfrenta a un reto particular: aunque la infraestructura digital y la conectividad han mejorado considerablemente, el capital humano necesario para desenvolverse con seguridad en los entornos digitales sigue estando muy poco desarrollado, especialmente entre la población de más edad. Según el informe nacional sobre el estado de la Década Digital 2024 de la Comisión Europea, Eslovaquia ha alcanzado una cobertura de competencias digitales básicas del 51,3 %, lo que supone un ligero descenso con respecto a mediciones anteriores y se sitúa por debajo de la media de la UE, que es del 55,6 %.

Las disparidades son especialmente graves entre los grupos demográficos de mayor edad. Entre las personas mayores eslovacas de entre 65 y 74 años, solo el 11 % posee competencias digitales básicas o superiores a estas, menos de la mitad de la media de la UE, que es del 24 % para el mismo grupo de edad. Además, el 27 % de las personas mayores de este grupo de edad nunca ha utilizado Internet, y solo el 39 % ha utilizado un ordenador en los últimos doce meses. En el caso de los adultos de entre 45 y 64 años, las competencias digitales se limitan con frecuencia a operaciones rutinarias, careciendo de la profundidad crítica y los marcos analíticos necesarios para hacer frente a las amenazas de ciberseguridad en constante evolución.

Eslovaquia se enfrenta a tipologías de fraude específicas y graves. Una táctica muy extendida consiste en que los estafadores se hacen pasar por agentes de policía,

empleados de seguridad bancaria o representantes del Banco Nacional de Eslovaquia, aprovechando la tecnología de suplantación de números para manipular la identificación de llamadas y empleando tácticas basadas en el miedo para obtener credenciales bancarias o coaccionar a las víctimas para que transfieran fondos a cuentas fraudulentas. Además, el espacio digital eslovaco está muy expuesto a campañas de desinformación vinculadas al posicionamiento geopolítico y a la polarización política interna.

Normativa y políticas nacionales

Para proteger los derechos digitales de los ciudadanos y contrarrestar las amenazas cibernéticas, la República Eslovaca ha desarrollado un marco normativo estrictamente alineado con las directivas de la Unión Europea. La base de la protección de datos en Eslovaquia es el Reglamento General de Protección de Datos (RGPD), incorporado a la legislación nacional mediante la Ley n.º 18/2018 Coll. sobre la Protección de Datos Personales. En vigor desde mayo de 2018, esta legislación establece directrices claras para el tratamiento lícito de los datos personales, exigiendo transparencia, minimización de datos y limitación de la finalidad. Garantiza a los ciudadanos el derecho de acceso, rectificación y supresión de sus datos, además de protección frente a la toma de decisiones automatizadas no autorizadas.

La Oficina de Protección de Datos Personales de la República Eslovaca (ÚOÚ) supervisa estas normas. Como autoridad de control independiente, la ÚOÚ garantiza el cumplimiento en los sectores público y privado además de ofrecer orientación vinculante sobre cuestiones complejas de protección de datos, como la realización de evaluaciones de impacto relativas a la misma. Cabe destacar que la legislación eslovaca regula estrictamente el uso del número de nacimiento (rodné číslo). La divulgación pública de este identificador está prohibida, salvo que la persona lo autorice explícitamente o lo exija una legislación específica, lo que constituye una medida fundamental para prevenir el robo de identidad.

En materia de ciberseguridad, la principal herramienta legislativa es la Ley n.º 69/2018 Coll. sobre ciberseguridad, que transponía originalmente la Directiva NIS europea. Esta ley estableció las bases para la gobernanza nacional de la ciberseguridad, definiendo las obligaciones legales de los operadores de servicios esenciales, los requisitos de notificación de incidentes y los procedimientos de auditoría. Para hacer frente a las amenazas en constante desarrollo, Eslovaquia actualizó este marco para cumplir los requisitos avanzados de la NIS2, Directiva (UE) 2022/2555. Mediante la Ley n.º 366/2024 Coll., en vigor desde el 1 de enero de 2025, Eslovaquia amplió significativamente el alcance de su normativa en materia de ciberseguridad. La enmienda introduce un mecanismo preciso para identificar a las entidades obligadas, abarca una gama más amplia de sectores críticos y aplica medidas de seguridad más estrictas.

La Autoridad Nacional de Seguridad (NBÚ) coordina estas iniciativas legislativas a través de la Estrategia Nacional de Ciberseguridad 2021-2025. La estrategia establece prioridades que incluyen garantizar la preparación del Estado, detectar la ciberdelincuencia, construir un sector privado resiliente, integrar la ciberseguridad en la administración pública y promover las competencias digitales tanto de los profesionales como del público en general. Este énfasis en la educación pública destaca que las defensas técnicas deben estar respaldadas directamente por la concienciación de los ciudadanos y la resiliencia digital individual.

Programas e iniciativas existentes

La implementación de la estrategia digital de Eslovaquia se basa en la colaboración entre instituciones públicas, ONG, fuerzas del orden y el sector privado para reducir la brecha digital y mejorar la seguridad en línea de los adultos.

El Ministerio de Inversiones, Desarrollo Regional e Informatización (MIRRI) lidera estos esfuerzos, gestionando componentes clave del Plan Nacional de Recuperación y Resiliencia. Su iniciativa insignia, «Digitálni seniori» (Mayores digitales), tiene como objetivo proporcionar formación en competencias digitales a más de 100 000 personas mayores (de más de 65 años) y personas desfavorecidas para 2026. El programa ofrece sesiones de formación adaptadas a las necesidades locales y proporciona a los graduados una tableta configurada y un paquete de datos móviles, abordando directamente tanto las barreras educativas como las relacionadas con el hardware.

En el ámbito de la seguridad, la Autoridad Nacional de Seguridad (NBÚ) y el Centro Nacional de Ciberseguridad (SK-CERT) gestionan la ciberseguridad técnica y la respuesta nacional ante incidentes, al tiempo que contribuyen a las campañas de sensibilización pública. Además, la Policía de la República Eslovaca combate activamente el fraude digital y la desinformación. A través de su canal de comunicación público específico, «Hoaxy a podvody – Polícia SR» (Bulos y estafas), la policía supervisa el espacio digital, desmiente los bulos virales, alerta a los ciudadanos sobre las estafas financieras emergentes y educa al público para que identifique las comunicaciones fraudulentas.

La colaboración intersectorial se formaliza a través de la Coalición Digital (Digitálna koalícia), una asociación que une al Gobierno, el sector de las tecnologías de la información, el mundo académico y la sociedad civil. Esta plataforma lleva a cabo evaluaciones nacionales, como la Prueba de Aptitud en Tecnologías de la Información, para evaluar las competencias digitales de la población e identificar los grupos demográficos que requieren intervención educativa. La coalición también colabora con MIRRI para diseñar formación a medida para personas mayores y empleados de la administración pública de edad avanzada.

Las ONG y el sector privado proporcionan un apoyo especializado esencial. Iniciativas independientes como Konšpirátori.sk ofrecen al público bases de datos transparentes de sitios web conocidos por difundir desinformación o contenido fraudulento, lo que las convierte en herramientas prácticas para la verificación de fuentes. En el sector financiero, la Asociación Bancaria Eslovaca y los distintos bancos llevan a cabo regularmente campañas de sensibilización específicas para prevenir el fraude en la banca electrónica. Estas campañas enseñan a los clientes a reconocer los intentos de phishing, a utilizar la autenticación multifactorial y a navegar de forma segura.

Aunque Eslovaquia ha establecido una base institucional sólida, lograr una resiliencia digital generalizada entre los adultos mayores de 45 años requiere un esfuerzo sostenido. El éxito depende de la expansión continua de programas de educación no formal accesibles y de la difusión eficaz de herramientas prácticas de ciberseguridad.

4. Buenas prácticas

La investigación documental nacional identificó un total de quince buenas prácticas en los tres países socios —cinco por país— que representan una amplia gama de actores, metodologías y enfoques específicos. Estas iniciativas demuestran cómo se abordan los retos de la seguridad digital mediante la prevención, la educación y el empoderamiento en diferentes niveles de gobierno y de la sociedad civil. A continuación se presentan las prácticas por país mediante un formato coherente.

4.1 Italia

Durante la investigación documental se identificaron cinco buenas prácticas nacionales relevantes que reflejan un ecosistema diverso de iniciativas destinadas a reforzar la alfabetización digital, la seguridad en línea y la prevención del fraude entre los adultos. Entre ellas se incluyen programas institucionales, campañas de sensibilización, iniciativas regionales, proyectos europeos y acciones lideradas por el tercer sector. A nivel nacional, Repubblica Digitale constituye un marco estratégico que promueve el desarrollo de competencias digitales y la inclusión a través de acciones coordinadas, como la Red de Facilitación Digital, que apoya a los ciudadanos, especialmente a los adultos, en el uso seguro de los servicios digitales. Del mismo modo, la campaña I Navigati, promovida por instituciones financieras y públicas, se centra específicamente en la sensibilización sobre el fraude en línea y los riesgos de ciberseguridad, en particular en el contexto de los servicios financieros digitales. A nivel regional, el programa Pane e Internet, desarrollado por la Región de Emilia-Romaña, ofrece oportunidades de formación estructuradas para adultos, con un fuerte énfasis en las competencias prácticas, incluida la seguridad en línea y el uso responsable de las herramientas digitales. Desde la perspectiva europea, el proyecto Erasmus+ DIGITOL ofrece un ejemplo relevante de educación no formal dirigida

a personas mayores, con el objetivo de mejorar las competencias digitales y promover un uso seguro de las tecnologías digitales. Por último, la Fondazione Mondo Digitale desempeña un papel clave en el contexto italiano mediante la implementación de programas educativos inclusivos que apoyan a los grupos vulnerables, incluidos los adultos, en el desarrollo de la concienciación digital y las habilidades de ciberseguridad. En conjunto, estas iniciativas demuestran un enfoque multinivel y con múltiples actores para la educación en seguridad digital, que combina políticas, formación, concienciación e innovación.

Estas son las buenas prácticas identificadas:

1. *Repubblica Digitale (República Digital)*

<i>Título de buena práctica</i>	Repubblica Digitale (República Digital)
<i>Tipo de buena práctica</i>	Iniciativa nacional
<i>Organización implementadora</i>	Comité Técnico Directivo, coordinado por el Departamento de Transformación Digital de la Oficina del primer ministro, Italia. https://innovazione.gov.it/
<i>Objetivos principales</i>	● Reducir la brecha digital, combatir todas las formas de analfabetismo digital y promover la educación en tecnologías del futuro, apoyando así el desarrollo del país. ● Garantizar una transición gradual e inclusiva hacia una sociedad plenamente digital.
<i>Grupo(s) destinatario(s)</i>	Principalmente: ● ciudadanos en riesgo de exclusión digital (como las personas mayores o quienes viven en zonas remotas); ● trabajadores que necesitan mejorar sus competencias tecnológicas; ● estudiantes que desean adquirir competencias digitales; ● la administración pública para modernizar los servicios gubernamentales; ● organizaciones del tercer sector para crear una amplia red de facilitadores digitales.
<i>Resultados educativos e impacto</i>	● En 2024, 272 270 empleados públicos se inscribieron en itinerarios de aprendizaje personalizados para mejorar

	sus competencias digitales a través de la plataforma del programa. Además, se introdujo una nueva directiva que, desde 2025, exige al menos 40 horas de formación anual para cada empleado público, con un enfoque específico en la digitalización, lo que supone un cambio significativo de tendencia con respecto al pasado. ● El fondo de Repubblica Digitale ha financiado 73 proyectos que, en 2024, formaron a más de 13 000 personas (incluidos jóvenes inactivos, desempleados y trabajadores en situación de riesgo), contribuyendo a cubrir la brecha de profesionales de las TIC en el mercado laboral italiano. ● Los Centros de Educación Digital se financiaron con 60 millones de euros del PNRR (Plan Nacional de Recuperación y Resiliencia), lo que representa un esfuerzo por fortalecer el sistema universitario en los ámbitos de la transferencia de tecnología y la formación avanzada, apoyando la preparación de especialistas altamente cualificados. ● «Punti Digitale Facile» (Puntos Digitales Fáciles). Estos centros habían involucrado a más de 1,8 millones de ciudadanos en octubre de 2025, contribuyendo a reducir la brecha digital y promoviendo el acceso a los servicios digitales para el público en general. ● Las iniciativas de formación y digitalización involucran activamente a las entidades públicas, las empresas y el tercer sector. Esta estrategia orienta las intervenciones tanto en la esfera pública como en la privada, fomentando la continuidad a largo plazo más allá de las inversiones extraordinarias.
<i>Descripción de la actividad y enfoque metodológico</i>	Un pilar fundamental de esta actividad es el Servizio Civile Digitale (Servicio Civil Digital), un programa en el que jóvenes voluntarios de entre 18 y 28 años trabajan durante 12 meses como mentores, guiando a los ciudadanos a través del proceso de aprender mediante la práctica. Este aprendizaje entre iguales e intergeneracional se sustenta además en los Punti Digitale Facile (Puntos Digitales Fáciles): con más de 4000 centros físicos establecidos en todo el país, estos centros sirven como espacios

	comunitarios accesibles a los que los ciudadanos pueden acudir para activar su identidad digital, como el SPID o la CIE (Tarjeta de Identidad Electrónica). Más allá de la simple activación, los facilitadores imparten la formación necesaria para manejar estas herramientas, enseñando a los usuarios a acceder a historiales sanitarios, pagar impuestos en línea o firmar documentos digitales. Además, Repubblica Digitale puso en marcha la «Coalición Italiana para las Competencias Digitales y el Empleo», una alianza abierta que tiene como objetivo identificar e involucrar al mayor número posible de partes interesadas (por ejemplo, empresas, organismos públicos, ONG, etc.) para crear una red digital y humana de personas dispuestas a cooperar y desarrollar una cultura científico-tecnológica nacional. Hasta la fecha, más de 180 organizaciones se han sumado a la Coalición Italiana y han puesto en marcha más de 220 proyectos. Para adherirse a la coalición, una organización debe suscribir formalmente el «Manifiesto de Repubblica Digitale», garantizando que todos los miembros se comprometen con los mismos valores de inclusión, ética y soberanía digital.
<i>Características innovadoras</i>	La iniciativa utiliza tanto la educación formal como la no formal, integradas en sus diversas actividades y proyectos, y valora enormemente la cooperación multisectorial, tanto del sector público como del privado, así como de la sociedad civil. Una característica distintiva de su modelo de enfoque es el uso de un enfoque entre iguales y el aprendizaje intergeneracional. Estos elementos, combinados con un compromiso con la inclusión amplia y un enfoque en los grupos vulnerables, la consolidan como una base estratégica e integrada para la alfabetización digital y la formación a nivel nacional.
<i>Enlace / Referencia</i>	https://repubblicadigitale.gov.it/portale/

Material es visuales



[https://](https://repubblicadigitale.gov.it/portale/-/l-italia-delle-competenze-digitali-si-fa-rete-i-risultati-raggiunti-e-le-sfide-del-futuro-martedì%3AC-31-marzo-a-roma)

repubblicadigitale.gov.it/portale/-/l-italia-delle-competenze-digitali-si-fa-rete-i-risultati-raggiunti-e-le-sfide-del-futuro-martedì%3AC-31-marzo-a-roma



Evaluación de adaptabilidad de Repubblica Digitale (República Digital)

Criterios	Totalmente	En cierta medida	En absoluto	Comentarios (opcional)
a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)	☒	☐	☐	
b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)	☒	☐	☐	
c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)	☐	☒	☐	

2. I Navigati

Título de buena práctica	I Navigati
--------------------------	------------

<i>Tipo de buena práctica</i>	Campaña, herramienta en línea
<i>Organización implementadora</i>	CERTFin (Equipo de Respuesta a Emergencias Informáticas del sector financiero italiano) https://www.certfin.it/en/
<i>Objetivos principales</i>	Promover la alfabetización digital, sensibilizar y educar a la población sobre el uso informado y seguro de las herramientas y plataformas digitales, con el fin de evitar caer en las trampas tendidas por los ciberdelincuentes.
<i>Grupo(s) destinatario(s)</i>	El público destinatario es amplio: desde jóvenes hasta adultos, el público principal está formado por personas que utilizan habitualmente canales digitales (banca electrónica, aplicaciones de pago, comercio en línea) para gestionar sus finanzas y personas con competencias digitales limitadas que tienen dificultades para distinguir una estafa de un proceso legítimo.
<i>Resultados educativos e impacto</i>	● Los usuarios aprenden a detenerse y verificar las solicitudes a través de los canales oficiales antes de actuar. ● Los participantes adquieren las habilidades necesarias para identificar estafas sofisticadas que eluden los filtros tradicionales. ● Al centrarse en el «factor humano», la campaña reduce significativamente la vulnerabilidad de los participantes. Los usuarios aprenden a identificar deepfakes sofisticados de voz o vídeo generados por IA, lo que evita que caigan víctimas de estafas emocionales que suplantán la identidad de familiares.
<i>Descripción de la actividad y enfoque metodológico</i>	● La campaña suele desarrollarse en «oleadas» anuales, que a menudo alcanzan su punto álgido en octubre, coincidiendo con el <i>Mes Europeo de la Ciberseguridad</i>. La campaña se promociona a través de los principales canales de televisión, la radio, el sitio web oficial y las

	redes sociales. La campaña utiliza la narración de historias para facilitar la comprensión de temas complejos: ● Una serie web de vídeos cortos en los que los miembros de la familia de Navigati abordan diferentes riesgos inherentes al mundo digital; ● El podcast «Al Sicuro», presentado por la experta en tecnología Fjona Cakalli, que habla sobre diferentes fraudes en línea, convirtiendo estas lecciones en audio en una forma de ofrecer consejos prácticos sobre cómo detectar los trucos psicológicos de los estafadores.
<i>Características innovadoras</i>	Lo que realmente distingue a I Navigati es su uso innovador de la narración y una estrategia multimedia multicanal diseñada para convertir temas complejos de ciberseguridad en situaciones cotidianas con las que el público pueda identificarse. La campaña se centra en la «familia Navigati», experta en seguridad digital, cuyas aventuras domésticas sirven de modelos educativos para el público. A través de una serie de episodios de vídeo cortos (de unos 3 minutos cada uno), la familia muestra cómo defenderse y reconocer las primeras señales de alerta de una estafa. Este tono familiar y desenfadado hace que los consejos técnicos sean accesibles y menos intimidantes para los no expertos. Para garantizar que el mensaje llegue a los ciudadanos que están en movimiento, la campaña también incluye una breve serie de podcasts, que ofrece lecciones de audio flexibles sobre seguridad digital.
<i>Enlace / Referencia</i>	https://inavigati.certfin.it/index.html
<i>Materiales visuales</i>	Cobertura mediática: https://www.bancaditalia.it/media/notizia/i-navigati-al-via-la-nuova-campagna-sulla-sicurezza-informatica/?dotcache=refresh

Evaluación de adaptabilidad de I Navigati

Criterios	Totalmente	En cierta medida	En absoluto	Comentarios (opcional)
a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)	☒	☐	☐	
b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)	☒	☐	☐	
c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)	☒	☐	☐	

3. Pane e Internet

Título de buena práctica	Pane e Internet
Tipo de buena práctica	Proyecto/Formación
Organización implementadora	Región de Emilia-Romaña, Italia, pei@paneeinternet.it
Objetivos principales	Promover el desarrollo de las competencias digitales y reforzar la red regional tanto a nivel local como regional, así como mejorar la concienciación digital de los ciudadanos sobre cuestiones globales.
Grupo(s) destinatario(s)	Ciudadanos de cualquier edad que utilicen la tecnología para acceder a la información, utilizar servicios en línea y aprovechar las oportunidades digitales disponibles en su comunidad.
Resultados educativos e impacto	Los programas de formación de Pane e Internet se han diseñado y puesto en práctica de acuerdo con el modelo europeo DigComp, el marco de referencia para las competencias digitales de los ciudadanos, y sus cursos han sido reconocidos por la Comisión Europea como una de las mejores prácticas europeas en el ámbito de la alfabetización digital.

	Los participantes pueden introducirse gradualmente en el mundo digital mediante seminarios web y cursos adaptados a sus necesidades y conocimientos. Los participantes no solo mejoran su propia conciencia digital, sino que se convierten en contribuyentes activos a la transformación de Emilia-Romaña en una región más avanzada y tecnológicamente inclusiva, impulsando un cambio colectivo hacia una comunidad más conectada y preparada para el futuro.
<i>Descripción de la actividad y enfoque metodológico</i>	La iniciativa funciona ofreciendo numerosos talleres y cursos en línea. A lo largo del año, ofrece docenas de cursos y seminarios web gratuitos que tienen una duración variable en función del tema. Una acción permanente es el mantenimiento de más de 100 Puntos Pel (Punti Pane e Internet) en toda la región, gracias a la colaboración con los ayuntamientos y los municipios, lo que garantiza que el apoyo digital sea siempre físicamente accesible dentro de la comunidad. Pane e Internet ofrece cursos de alfabetización digital a medida, que van desde conocimientos informáticos básicos y el uso del hardware hasta la sensibilización avanzada en materia de ciberseguridad. Este enfoque por niveles garantiza que los usuarios puedan pasar de operaciones técnicas básicas a identificar y defenderse de riesgos online complejos. A la hora de crear los cursos, se presta especial atención también a los grupos vulnerables, garantizando el máximo alcance y accesibilidad.
<i>Características innovadoras</i>	La Comisión Europea ha reconocido el programa educativo de Pane e Internet como una de las mejores prácticas de Europa en el ámbito de la alfabetización digital. Las sesiones de formación y los seminarios web se celebran en línea para garantizar la máxima accesibilidad, llegando también a zonas remotas de la región. Al mismo tiempo, el proyecto mantiene una fuerte presencia territorial a través de centros físicos estratégicamente ubicados en toda la región. Estos centros locales son esenciales para fomentar la cooperación comunitaria y garantizar la amplia difusión

	de las herramientas digitales.
<i>Enlace / Referencia</i>	https://www.paneeinternet.it/
<i>Materiales visuales</i>	https://www.paneeinternet.it/public/elenco-news

Evaluación de la adaptabilidad de Pane e Internet

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☒	☐	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

4. Proyecto Erasmus+ DIGITOL

<i>Título de buena práctica</i>	Proyecto Erasmus+ <i>DIGITOL</i>
<i>Tipo de buena práctica</i>	Proyecto
<i>Organización implementadora</i>	Asociación compuesta por seis organizaciones de seis países europeos diferentes: Consorzio Comunità Brianza (Italia), Pro Arbeit (Alemania), 50PLUS Hellas (Grecia), Znanie (Bulgaria), Tree Agency (Estonia) y AGE Platform Europe (Bélgica).
<i>Objetivos principales</i>	DIGITOL promueve valores de la UE como la solidaridad y la diversidad a través de programas innovadores de alfabetización digital. El proyecto tiene como objetivo crear un Internet más respetuoso, al tiempo que combate la discriminación y la xenofobia uniendo a las generaciones para identificar y contener las noticias falsas y el discurso de odio en línea.
<i>Grupo(s) destinatario(s)</i>	Adultos mayores europeos (mayores de 55 años)

<i>Resultados educativos e impacto</i>	● Se formó a 10 jóvenes (de entre 18 y 30 años) que participaron en un curso para educadores de 30 horas centrado en la lucha contra las noticias falsas y la polarización. ● 25 personas mayores (mayores de 55 años) participaron en el programa de desarrollo de capacidades DIGITOL, de 60 horas de duración, dirigido por jóvenes y expertos externos, cuyo objetivo era dotar a los participantes de herramientas teóricas y prácticas para comprender mejor la evolución de la sociedad contemporánea en consonancia con nuestros valores europeos.
<i>Descripción de la actividad y enfoque metodológico</i>	● Formación de educadores (ToT): Los «Jóvenes Embajadores» (de entre 18 y 30 años) aprendieron a ser mentores intergeneracionales. Adquirieron no solo competencias digitales, sino también técnicas pedagógicas para enseñar a las personas mayores. ● Programa de desarrollo de capacidades (CBP): La fase educativa principal, en la que los Jóvenes Embajadores dirigen talleres para personas mayores (de 55 años o más) sobre alfabetización mediática, identificación de noticias falsas y lucha contra el discurso de odio en línea. ● Acciones piloto y actividades de seguimiento: Los participantes pasan del aula al mundo real organizando «Bibliotecas Humanas» y «Festivales Digitol» para promover la cohesión social y los valores europeos en sus comunidades locales.
<i>Características innovadoras</i>	https://digitol.eu/it/
<i>Enlace / Referencia</i>	https://digitol.eu/wp-content/uploads/2020/07/DIGITOL-Project-Brochure-English.pdf Kit de herramientas: https://digitol.eu/wp-

	content/uploads/2022/01/toolkit-ITA-DEF.pdf
--	---

Evaluación de la adaptabilidad del proyecto Erasmus+ DIGITOL

Criterios	Totalmente	En cierta medida	En absoluto	Comentarios (opcional)
a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)	☒	☐	☐	
b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)	☒	☐	☐	
c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)	☒	☐	☐	

5. Fondazione Mondo Digitale

Título de buena práctica	Fondazione Mondo Digitale
Tipo de buena práctica	Formación
Organización implementadora	Fondazione Mondo Digitale ETS, Italia, info@mondodigitale.org https://www.mondodigitale.org/
Objetivos principales	● Promover una cultura de innovación y fomentar una nueva economía basada en el conocimiento como motor del desarrollo del país. ● El uso de las tecnologías digitales para el progreso social, con el fin de impulsar el crecimiento, el bienestar, la productividad y la competitividad.
Grupo(s) destinatario(s)	Personas de todas las edades y procedencias profesionales: el sitio web permite a los usuarios seleccionar el término que mejor les represente (por ejemplo: <i>mujeres, desempleados, ejecutivos, artistas...</i>)
Resultados educativos e impacto	Las personas que participan en los proyectos y eventos de la Fondazione Mondo Digitale adquieren

	conocimientos especializados en el ámbito STEAM, al tiempo que crean una red de contactos en su entorno. Gracias a la forma en que están estructurados los proyectos, las competencias digitales se complementan con habilidades sociales y ciudadanía activa. Esto se consigue fomentando la participación en eventos, concursos locales y seminarios web.
<i>Descripción de la actividad y enfoque metodológico</i>	La Fondazione Mondo Digitale se centra en ofrecer a los participantes laboratorios STEAM en diferentes áreas. Además, los talleres y seminarios se integran directamente con concursos locales y nacionales, lo que brinda a los participantes oportunidades inmediatas para aplicar conceptos teóricos a través de competiciones prácticas (por ejemplo: RomeCup, Digital Made). Los proyectos pueden abarcar desde talleres cortos e intensivos de 3 horas hasta itinerarios curriculares de un año de duración integrados en el calendario escolar. En todos los proyectos se aplica el aprendizaje mediante la práctica, cuya principal manifestación son los «Gimnasios de Innovación», espacios híbridos físicos y virtuales repartidos por toda Italia donde personas de todas las edades pueden acudir y aprender tanto el dominio técnico como habilidades sociales.
<i>Características innovadoras</i>	Lo que realmente distingue a este proyecto es su página web personalizada, que clasifica las oportunidades en grupos destinatarios específicos (desde mujeres y jóvenes hasta personas mayores, migrantes, artistas...) permitiendo a los usuarios identificar al instante los cursos e iniciativas más adecuados para su crecimiento personal o profesional. Esta accesibilidad se combina con una filosofía de aprendizaje mediante la práctica, en la que las actividades educativas prácticas se entrelazan directamente con concursos nacionales y locales. Al participar en estos concursos, los alumnos pueden aplicar de inmediato sus conocimientos teóricos a retos del mundo real.
<i>Enlace / Referencia</i>	https://www.mondodigitale.org/

<i>Materiales visuales</i>	https://youtu.be/m-si=DBQRTWNVSPVP4Ycx https://www.repubblica.it/tecnologia/sicurezza/2020/02/04/news/google_premia_4_progetti_italiani_su_sicurezza_online-247591358/
----------------------------	--

Evaluación de la adaptabilidad de la *Fondazione Mondo Digitale*

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☒	☐	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

4.2 España

Como parte de la fase de investigación de digiSAFE, se llevó a cabo un mapeo de las mejores prácticas nacionales para identificar iniciativas eficaces en España que promuevan la seguridad digital, la prevención del fraude y la alfabetización digital entre los adultos, con especial relevancia para las personas de más de 45 años. El objetivo de este análisis era destacar los enfoques existentes que puedan servir de base para el desarrollo del Currículo de Educación No Formal de digiSAFE y el Kit de Herramientas para la Prevención del Fraude Digital. Las buenas prácticas seleccionadas representan una amplia gama de actores y metodologías, entre los que se incluyen instituciones públicas, organismos encargados de hacer cumplir la ley, organizaciones no gubernamentales, campañas nacionales de sensibilización e iniciativas de formación comunitarias. En conjunto, demuestran cómo se abordan los retos de la seguridad digital en España a través de la prevención, la educación y el empoderamiento, en lugar de recurrir exclusivamente a medidas técnicas o normativas.

Se prestó especial atención a las iniciativas que adoptan enfoques de aprendizaje no formal y accesible, reconociendo que los adultos mayores de 45 años suelen beneficiarse más de métodos educativos prácticos, basados en la experiencia y fáciles

de usar. Las prácticas identificadas se centran en reforzar la confianza digital, sensibilizar sobre los riesgos en línea, mejorar la capacidad de reconocer el fraude y las estafas, y fomentar el uso responsable de las tecnologías digitales en la vida cotidiana.

Además, las buenas prácticas seleccionadas muestran un alto grado de adaptabilidad y transferibilidad a otros contextos nacionales y europeos. Muchas de ellas son escalables, inclusivas y están diseñadas para ser aplicadas por diferentes tipos de organizaciones, lo que las hace especialmente adecuadas para su reproducción en el marco del proyecto digiSAFE. A continuación se presentan las cinco buenas prácticas identificadas en España:

1. **Fundación Cibervoluntarios – Digital Inclusion and Digital Skills for Adults**

<i>Título de buena práctica</i>	Fundación Cibervoluntarios – Inclusión y competencias digitales para adultos
<i>Tipo de buena práctica</i>	Proyecto / Formación / Talleres
<i>Organización implementadora</i>	Fundación Cibervoluntarios, España https://www.cibervoluntarios.org
<i>Objetivos principales</i>	Reducir la brecha digital dotando a adultos y personas mayores de competencias digitales, confianza y concienciación para participar de forma segura en la sociedad digital.
<i>Grupo(s) destinatario(s)</i>	Adultos, personas mayores, grupos vulnerables, adultos mayores de 45 años.
<i>Resultados educativos e impacto</i>	Los participantes mejoran sus competencias digitales básicas e intermedias, aumentan su confianza en el uso de herramientas digitales y desarrollan una mayor conciencia sobre los riesgos en línea, el fraude y la desinformación.
<i>Descripción de la actividad y enfoque metodológico</i>	Actividades de formación digital gratuitas impartidas en línea y de forma presencial a través de centros comunitarios, asociaciones e instituciones públicas. La metodología se basa en la educación no formal, ejercicios prácticos, el aprendizaje entre iguales y situaciones digitales de la vida real.
<i>Características innovadoras</i>	Tutoría digital dirigida por voluntarios, enfoque comunitario e itinerarios de aprendizaje personalizados para adultos y personas mayores.
<i>Enlace / Referencia</i>	https://www.cibervoluntarios.org
<i>Materiales visuales</i>	Materiales de formación, vídeos, infografías,

	informes de proyectos y recursos en línea disponibles en el sitio web de la organización.
--	---

Evaluación de la adaptabilidad de la Fundación Cibervoluntarios – inclusión y competencias digitales para adultos

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☒	☐	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

2. Aula Mentor – Programa de Educación para Adultos y Competencias Digitales

<i>Título de buena práctica</i>	Aula Mentor – Programa de Educación para Adultos y Competencias Digitales
<i>Tipo de buena práctica</i>	Formación / Aprendizaje en línea Programa
<i>Organización implementadora</i>	Ministerio de Educación y Formación Profesional, España https://www.aulamentor.es
<i>Objetivos principales</i>	Promover el aprendizaje permanente proporcionando a los adultos un acceso flexible a las competencias digitales y a la formación en TIC.
<i>Grupo(s) destinatario(s)</i>	Adultos (mayores de 18 años), incluidos los mayores de 45 años.

<i>Resultados educativos e impacto</i>	Los alumnos adquieren competencias digitales básicas, mejoran su autonomía en el uso de herramientas en línea y aumentan su confianza en los entornos digitales.
<i>Descripción de la actividad y enfoque metodológico</i>	Cursos en línea con el apoyo de mentores formados que permiten a los adultos aprender a su propio ritmo a través de un modelo de aprendizaje no formal flexible y adaptado a las necesidades de los alumnos adultos.
<i>Características innovadoras</i>	Cobertura a nivel nacional, aprendizaje con el apoyo de mentores y acceso flexible para los estudiantes adultos.
<i>Enlace / Referencia</i>	https://www.aulamentor.es
<i>Materiales visuales</i>	Catálogos de cursos en línea, capturas de pantalla de la plataforma y materiales informativos disponibles en el sitio web oficial.

Evaluación de la adaptabilidad de Aula Mentor – Programa de educación para adultos y competencias digitales

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☐	☒	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

3. Policía Nacional – Plan Mayor Seguridad

<i>Título de buena práctica</i>	Policía Nacional – Plan Mayor Seguridad
<i>Tipo de buena práctica</i>	Campaña / Iniciativa de sensibilización
<i>Organización implementadora</i>	Policía Nacional, España https://www.policia.es
<i>Objetivos principales</i>	Prevenir los delitos y fraudes que afectan a las personas mayores mediante la sensibilización sobre los riesgos digitales y fuera de línea y la promoción de comportamientos seguros.
<i>Grupo(s) destinatario(s)</i>	Adultos mayores, personas de la tercera edad, asociaciones de personas mayores.
<i>Resultados educativos e impacto</i>	Mayor concienciación sobre las estafas, mejora de la capacidad para reconocer las estafas y mayor confianza entre los ciudadanos de edad avanzada y las instituciones públicas.
<i>Descripción de la actividad y enfoque metodológico</i>	Charlas informativas y talleres impartidos por agentes de policía en centros comunitarios y asociaciones, utilizando ejemplos prácticos y orientación enfocada en la prevención.
<i>Características innovadoras</i>	Participación directa de profesionales de las fuerzas del orden y una fuerte implicación de la comunidad.
<i>Enlace / Referencia</i>	https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
<i>Materiales visuales</i>	Carteles, folletos, materiales de presentación e imágenes de la campaña disponibles a través de los canales de la Policía Nacional.

Evaluación de la adaptabilidad de la Policía Nacional – Plan Mayor Seguridad

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores,</i>	☐	☒	☐	

<i>profesionales)</i>				
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☐	☒	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

4. **INCIBE – Línea de asistencia y programa de concienciación sobre ciberseguridad 017**

<i>Título de buena práctica</i>	INCIBE – Línea de asistencia y programa de concienciación sobre ciberseguridad 017
<i>Tipo de buena práctica</i>	Servicio público / Sensibilización Campaña / Herramienta en línea
<i>Organización implementadora</i>	Instituto Nacional de Ciberseguridad (INCIBE), España https://www.incibe.es
<i>Objetivos principales</i>	Mejorar la concienciación de los ciudadanos sobre los riesgos de ciberseguridad y ofrecer orientación sobre la prevención del fraude y el comportamiento digital seguro.
<i>Grupo(s) destinatario(s)</i>	Población general, adultos, personas mayores, usuarios vulnerables.
<i>Resultados educativos e impacto</i>	Los usuarios mejoran su concienciación sobre las amenazas digitales, aumentan su capacidad para reconocer el fraude y las estafas, y adoptan prácticas más seguras en Internet.
<i>Descripción de la actividad y enfoque metodológico</i>	Línea de ayuda pública gratuita que ofrece apoyo personalizado por teléfono, chat y aplicaciones de mensajería, combinada con campañas de sensibilización y recursos educativos en línea.
<i>Características innovadoras</i>	Acceso multicanal, asistencia personalizada en tiempo

	real e integración de la formación con la respuesta ante incidentes.
<i>Enlace / Referencia</i>	https://www.incibe.es/linea-017

Evaluación de la adaptabilidad de INCIBE – Línea de asistencia y programa de concienciación sobre ciberseguridad 017

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☐	☒	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

5. Programas regionales de competencias digitales para personas mayores (España)

<i>Título de buena práctica</i>	Programas regionales de competencias digitales para personas mayores (España)
<i>Tipo de buena práctica</i>	Formación / Talleres / Iniciativa pública
<i>Organización implementadora</i>	Administraciones públicas regionales y locales, España
<i>Objetivos principales</i>	Promover la inclusión digital y el uso seguro de las tecnologías digitales entre las personas mayores a nivel local.
<i>Grupo(s) destinatario(s)</i>	Personas mayores, adultos mayores, adultos con escasas competencias digitales.
<i>Resultados educativos</i>	Los participantes mejoran sus competencias digitales

<i>impacto</i>	básicas, aumentan su confianza en el uso de los servicios en línea y adquieren conciencia de los riesgos en línea y las estrategias de prevención del fraude.
<i>Descripción de la actividad y enfoque metodológico</i>	Actividades de formación práctica impartidas en centros comunitarios, bibliotecas o centros de educación de adultos a través de sesiones en grupos reducidos orientadas a la práctica.
<i>Características innovadoras</i>	Enfoque localizado, participación directa de la comunidad y adaptación a las necesidades específicas de los alumnos.

Evaluación de la adaptabilidad de los programas regionales de competencias digitales para personas mayores (España)

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, autoridades)</i>	☒	☐	☐	
<i>c) Diferentes temas o retos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	

4.3 Slovakia

La fase de investigación documental identificó cinco buenas prácticas nacionales diferenciadas en Eslovaquia, lideradas por el sector privado, organizaciones sin ánimo de lucro y redes comunitarias. Estas iniciativas ofrecen enfoques altamente adaptables para combatir la exclusión digital y prevenir el fraude en línea entre las personas mayores. Bezpečne na nete (Seguros en la Red). Creado por la empresa eslovaca de ciberseguridad ESET, este portal educativo integral ofrece recursos gratuitos y accesibles sobre

seguridad digital. Aunque está disponible para el público en general, sus artículos, podcasts y vídeos explicativos resultan especialmente eficaces para adultos y personas mayores. La plataforma traduce amenazas complejas de ciberseguridad —como el malware, el phishing y la privacidad de los datos— a un lenguaje sencillo y cotidiano. Su principal innovación consiste en aprovechar la experiencia en ciberseguridad del sector privado para ofrecer al público contenido educativo de alta calidad, constantemente actualizado, que los usuarios pueden consultar a su propio ritmo.

Zrelí na dobu digitálnu (Maduros para la Era Digital). Gestionado por el Fondo de Dotación de Slovak Telekom, este programa de subvenciones y formación tiene como objetivo específico la inclusión digital de las personas mayores. La iniciativa financia y apoya a organizaciones locales, residencias de mayores y centros comunitarios para que impartan cursos de alfabetización digital adaptados a sus necesidades. La metodología se centra en entornos de aprendizaje práctico en grupos pequeños, donde las personas mayores pueden practicar de forma segura el uso de smartphones, la gestión de cuentas en línea y la identificación de estafas habituales. Este enfoque descentralizado garantiza que la formación llegue a las personas mayores en sus comunidades locales, haciendo que el aprendizaje sea altamente accesible y socialmente enriquecedor.

Zodpovedne.sk (Responsablemente.sk). Gestionado por la asociación cívica eSlovensko, este centro nacional de concienciación se enfoca en el uso seguro de internet en todas las generaciones. Para el grupo demográfico de mayores de 45 años, ofrece manuales impresos específicos, vídeos instructivos y servicios de asesoramiento sobre amenazas cibernéticas. La iniciativa actúa como herramienta educativa preventiva, enseñando a los adultos a proteger sus dispositivos, salvaguardar sus datos personales y reconocer la manipulación psicológica en línea. Su principal fortaleza radica en su larga trayectoria y en su extenso archivo de materiales localizados y fáciles de comprender, que pueden ser ampliamente distribuidos por educadores y ONG.

Senior bezpečne online (Mayores seguros en línea) – Seminarios. Organizados a través de las sedes locales de la Unión de Pensionistas de Eslovaquia (JDS) en colaboración con expertos regionales en TI, estos seminarios de base comunitaria ofrecen formación directa con apoyo entre iguales. Los talleres se celebran en espacios comunitarios conocidos y se centran principalmente en amenazas inmediatas, como las estafas financieras locales, las tiendas en línea fraudulentas y la comunicación segura con familiares. La fortaleza metodológica radica en el modelo de confianza entre pares: aprender dentro de una red de personas con experiencias similares reduce significativamente la ansiedad que suelen sentir las personas mayores al adoptar nuevos hábitos digitales.

Academias Smart Senior en Bibliotecas Regionales. Las bibliotecas públicas de toda Eslovaquia, como las bibliotecas regionales de Žilina y Bratislava, se han convertido en centros vitales para la formación digital de adultos. Estas instituciones organizan

regularmente cursos estructurados de «Smart Senior». Bibliotecarios y formadores voluntarios de TI guían a los participantes en la navegación digital básica, la evaluación de la información en línea y el reconocimiento de correos electrónicos fraudulentos. Esta práctica utiliza la infraestructura comunitaria de confianza ya existente para ofrecer formación continua, gratuita y altamente accesible, convirtiéndola en un modelo fácilmente adaptable para cualquier municipio. A continuación se presentan las 5 buenas prácticas identificadas:

1. *Bezpečne na nete (Safely on the Net)*

<i>Título de buena práctica</i>	Bezpečne na nete (Safely on the Net)
<i>Tipo de buena práctica</i>	Herramienta en línea / Campaña
<i>Organización implementadora</i>	ESET, Slovakia. https://bezpecnenanete.eset.com/sk/
<i>Objetivos principales</i>	Incrementar la concienciación sobre las amenazas de ciberseguridad y ofrecer formación práctica y gratuita sobre cómo navegar por internet de forma segura, adaptada a todos los grupos de usuarios, incluidas las personas mayores.
<i>Grupo(s) destinatario(s)</i>	Público en general, adultos, personas mayores, educadores y familias.
<i>Resultados educativos e impacto</i>	El portal funciona como un centro educativo centralizado que ofrece materiales de aprendizaje paso a paso. La metodología se basa en traducir conceptos complejos de seguridad informática (como el malware, el phishing o las filtraciones de datos) a un lenguaje sencillo y cotidiano. Los contenidos están categorizados según el nivel de habilidad y las situaciones vitales de los usuarios, lo que facilita su consulta por parte de las personas mayores a su propio ritmo.
<i>Descripción de la actividad y enfoque metodológico</i>	Aprovecha la profunda experiencia en ciberseguridad de una empresa tecnológica líder del sector privado (ESET) para ofrecer contenido educativo completamente gratuito, de alta calidad y sin carácter comercial para el bien público.

<i>Características innovadoras</i>	It leverages the profound, global cybersecurity expertise of a leading private-sector tech company (ESET) to provide completely free, high-quality, and non-commercial educational content for the public good.
<i>Enlace / Referencia</i>	https://bezpecnenanete.eset.com/sk/
<i>Materiales visuales</i>	Capturas de pantalla del portal y de la biblioteca de podcasts disponibles en: https://bezpecnenanete.eset.com/sk/

Adaptability Assessment of Bezpečne na nete (Safely on the Net):

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	Los contenidos ya están segmentados por grupos de edad y nivel de competencia técnica.
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, administraciones públicas)</i>	☒	☐	☐	Las empresas del sector privado en toda Europa podrían replicar este modelo de RSC.
<i>c) Diferentes temáticas o desafíos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	El formato de la plataforma permite incorporar fácilmente nuevas temáticas, como las amenazas de la IA.

2. Zrelí na dobu digitálnu (Mature for the Digital Age)

<i>Título de buena práctica</i>	Proyecto / Financiación / Formación
---------------------------------	-------------------------------------

<i>Tipo de buena práctica</i>	Fondo de Dotación de Slovak Telekom (Nadačný fond Telekom pri Nadácii Pontis), Eslovaquia. https://nadacnyfondtelekom.sk/
<i>Organización implementadora</i>	Promover la alfabetización digital y sensibilizar a la ciudadanía sobre el uso informado y seguro de las herramientas y plataformas digitales, con el fin de evitar caer en las trampas tendidas por los ciberdelincuentes.
<i>Objetivos principales</i>	Personas mayores de 65 años, ONG locales, residencias de mayores y centros comunitarios.
<i>Grupo(s) destinatario(s)</i>	El programa de subvenciones ha financiado a decenas de organizaciones locales con más de 200.000 €, formando a miles de personas mayores. Los participantes mejoran su pensamiento crítico, aprenden a verificar fuentes de información y desarrollan resiliencia frente a la manipulación emocional utilizada por los defraudadores.
<i>Resultados educativos e impacto</i>	En lugar de un curso centralizado único, se trata de un mecanismo de subvenciones que capacita a entidades locales para impartir formación. Los proyectos apoyados utilizan metodologías de aprendizaje práctico en grupos pequeños. Las personas mayores reciben formación en entornos familiares para practicar de forma segura el uso de smartphones, identificar estafas y comunicarse con sus familiares, garantizando una instrucción personalizada y adaptada. Asimismo, se les ofrece orientación práctica para detectar las tácticas psicológicas empleadas por los estafadores.
<i>Descripción de la actividad y enfoque metodológico</i>	El modelo de financiación descentralizado se apoya en gran medida en las redes comunitarias de base, garantizando que la formación digital llegue a las personas mayores aisladas en zonas rurales, que no asistirían a cursos masivos organizados por el Estado.
<i>Características innovadoras</i>	https://nadacnyfondtelekom.sk/

<i>Enlace / Referencia</i>	Proyecto / Financiación / Formación
<i>Materiales visuales</i>	Detalles de la campaña disponibles en: https://nadacnyfondtelekom.sk/aktual-ne-vyzvy/

Adaptability Assessment of Zrelí na dobu digitálnu (Mature for the Digital Age)

<i>Crterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☐	☒	☐	El modelo de subvenciones está diseñado específicamente para las necesidades y el ritmo de las personas mayores.
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, administraciones públicas)</i>	☒	☐	☐	Cualquier fundación empresarial o entidad pública puede adoptar esta metodología de subvención descentralizada.
<i>c) Diferentes temáticas o desafíos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	Las subvenciones pueden orientarse anualmente hacia temáticas específicas, como el phishing o la IA.

3. **Zodpovedne.sk (Responsibly.sk)**

<i>Título de buena práctica</i>	Campaña / Herramienta en línea
<i>Tipo de buena práctica</i>	Asociación Cívica eSlovensko, Eslovaquia. https://www.zodpovedne.sk/
<i>Organización implementadora</i>	Sensibilizar a la ciudadanía a escala nacional sobre la seguridad en internet, prevenir la ciberdelincuencia y proporcionar recursos educativos y servicios de asesoramiento sobre amenazas cibernéticas para todas las generaciones.
<i>Objetivos principales</i>	Público en general, adultos, personas mayores, familias y educadores.
<i>Grupo(s) destinatario(s)</i>	Las personas mayores aprenden a buscar información de forma autónoma, gestionar cuentas de correo electrónico y reconocer comunicaciones fraudulentas. La iniciativa favorece un sentimiento de independencia e integración en la sociedad digital moderna.
<i>Resultados educativos e impacto</i>	Las bibliotecas organizan cursos estructurados de varias semanas de «Smart Senior» o sesiones abiertas de atención informática. Bibliotecarios y formadores voluntarios de TI guían a pequeños grupos a través de ejercicios prácticos. La metodología es altamente paciente, permitiendo a las personas mayores practicar en los ordenadores de la biblioteca o en sus propios dispositivos, abarcando desde el encendido del dispositivo hasta la seguridad avanzada en internet.

<i>Descripción de la actividad y enfoque metodológico</i>	Utiliza de forma ingeniosa la infraestructura existente, ampliamente confiable y accesible, de las bibliotecas públicas para ofrecer formación continua, gratuita y no intimidante para adultos.
<i>Características innovadoras</i>	https://www.krajskakniznicazilina.sk/
<i>Enlace / Referencia</i>	Descripciones de los cursos en: https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/
<i>Materiales visuales</i>	Campaña / Herramienta en línea

Adaptability Assessment of Zdpovedne.sk (Responsibly.sk)

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☒	☐	☐	Las bibliotecas atienden a toda la comunidad y pueden adaptar las clases a cualquier grupo demográfico.
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, administraciones públicas)</i>	☒	☐	☐	Puede ser aprovechado por centros escolares, centros de educación de adultos y administracion

				es públicas.
c) <i>Diferentes temáticas o desafíos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	Se actualiza continuamente para abordar nuevos fenómenos como el juego en línea, la IA y el uso indebido de datos.

4. **Erasmus+ project DIGITOL**

<i>Título de buena práctica</i>	Erasmus+ project DIGITOL
<i>Tipo de buena práctica</i>	Proyecto
<i>Organización implementadora</i>	Unión de Pensionistas de Eslovaquia (JDS) en colaboración con expertos regionales en TI y universidades. https://www.jednotadochodcov.sk
<i>Objetivos principales</i>	Ofrecer formación localizada con apoyo entre iguales que ayude a las personas mayores a navegar de forma segura por internet, reconocer las estafas financieras locales y reducir la ansiedad en torno a las herramientas digitales.
<i>Grupo(s) destinatario(s)</i>	Personas mayores y adultos jubilados.
<i>Resultados educativos e impacto</i>	Los participantes logran pasar de evitar las herramientas digitales a utilizarlas de forma activa y segura: smartphones, aplicaciones de mensajería y banca en línea, reduciendo significativamente su aislamiento y vulnerabilidad ante el fraude básico.

<i>Descripción de la actividad y enfoque metodológico</i>	Se trata de seminarios de base comunitaria organizados directamente por la unión de pensionistas en espacios comunitarios locales. La metodología hace hincapié en el aprendizaje entre iguales y en la aplicación práctica e inmediata. Los temas son altamente relevantes para la vida cotidiana: identificar tiendas en línea fraudulentas, reconocer noticias falsas y aprender a ignorar o bloquear comunicaciones no solicitadas.
<i>Características innovadoras</i>	El modelo de confianza entre iguales es altamente eficaz. Aprender dentro de una red de personas con experiencias similares (otros jubilados) reduce drásticamente la barrera psicológica y la ansiedad que las personas mayores experimentan frecuentemente en las clases de informática formales y de ritmo rápido.
<i>Enlace / Referencia</i>	https://www.jednotadochodcov.sk/
<i>Materiales visuales</i>	N/D

Adaptability Assessment of Erasmus+ project DIGITOL

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas mayores, profesionales)</i>	☐	☒	☐	El modelo de apoyo entre iguales funciona mejor cuando los participantes comparten una edad o experiencias vitales similares.

b) <i>Diferentes organizaciones (p. ej., ONG, centros educativos, administraciones públicas)</i>	☒	☐	☐	Altamente adaptable para centros comunitarios , ONG locales y clubes de personas mayores.
c) <i>Diferentes temáticas o desafíos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	Los seminarios pueden incorporar fácilmente nuevos panoramas de amenazas en el debate.

5. *Smart Senior Academies at Regional Libraries*

<i>Título de buena práctica</i>	<i>Smart Senior Academies at Regional Libraries</i>
<i>Tipo de buena práctica</i>	Formación / Proyecto
<i>Organización implementadora</i>	Bibliotecas públicas regionales (p. ej., Krajská knižnica Žilina), Eslovaquia. https://www.krajskakniznicazilina.sk/
<i>Objetivos principales</i>	Transformar las bibliotecas públicas en centros vitales de formación digital para adultos, enseñando a las personas mayores la navegación básica en dispositivos y cómo evaluar de forma segura la información en línea.
<i>Grupo(s) destinatario(s)</i>	Personas mayores, adultos en situación de desventaja y miembros de la comunidad local.

<i>Resultados educativos e impacto</i>	Las personas mayores aprenden a buscar información de forma autónoma, gestionar cuentas de correo electrónico y reconocer comunicaciones fraudulentas. La iniciativa fomenta un sentimiento de independencia e integración en la sociedad digital moderna.
<i>Descripción de la actividad y enfoque metodológico</i>	Las bibliotecas organizan cursos estructurados de varias semanas de «Smart Senior» o sesiones abiertas de atención informática. Bibliotecarios y formadores voluntarios de TI guían a pequeños grupos a través de ejercicios prácticos. La metodología es altamente paciente, permitiendo a las personas mayores practicar en los ordenadores de la biblioteca o en sus propios dispositivos, abarcando desde el encendido del dispositivo hasta la seguridad avanzada en internet.
<i>Características innovadoras</i>	Utiliza de forma ingeniosa la infraestructura existente, ampliamente confiable y accesible, de las bibliotecas públicas para ofrecer formación continua, gratuita y no intimidante para adultos.
<i>Enlace / Referencia</i>	https://www.krajskakniznicazilina.sk/
<i>Materiales visuales</i>	Descripciones de los cursos en: https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/

Adaptability Assessment Smart Senior Academies at Regional Libraries

<i>Criterios</i>	<i>Totalmente</i>	<i>En cierta medida</i>	<i>En absoluto</i>	<i>Comentarios (opcional)</i>
<i>a) Diferentes grupos destinatarios (p. ej., jóvenes, personas</i>	☒	☐	☐	Las bibliotecas atienden a toda la

<i>mayores, profesionales)</i>				comunidad y pueden adaptar las clases a cualquier grupo demográfico.
<i>b) Diferentes organizaciones (p. ej., ONG, centros educativos, administraciones públicas)</i>	☒	☐	☐	Este modelo puede ser replicado por cualquier institución pública que disponga de espacio y ordenadores.
<i>c) Diferentes temáticas o desafíos (p. ej., privacidad, desinformación, ciberseguridad)</i>	☒	☐	☐	El plan de estudios puede orientarse desde el uso básico del hardware hasta la formación avanzada contra el phishing.

5. Análisis de los Resultados de la Encuesta

5.1 Italia

Propósito y Metodología

La encuesta italiana se realizó en el marco de la evaluación de necesidades nacional con el objetivo de recopilar datos cuantitativos sobre la alfabetización digital, la concienciación sobre la seguridad en línea y la exposición al fraude digital entre los adultos mayores de 45 años en Italia. El cuestionario se administró en línea a través de Google Forms y se difundió por múltiples canales para garantizar una amplia cobertura.

Inicialmente, se distribuyó dentro de la red de la Associazione Italiana Socio-Educatori per la Cooperazione (AISEC APS) a través de herramientas de comunicación interna, incluidos intercambios de correo electrónico y presentaciones durante las asambleas anuales de la asociación. Asimismo, la encuesta se difundió a través de los canales de comunicación oficiales de Confcooperative Lazio Nord, con la que AISEC está afiliada, mediante boletines informativos, circulares y correos electrónicos dirigidos a su red en las provincias de Rieti, Viterbo y Roma.

A efectos del análisis nacional, únicamente se consideraron las respuestas de los participantes residentes en Italia. La muestra final estuvo compuesta por 63 encuestados mayores de 45 años, entre los que se encontraban 39 mujeres y 24 hombres. El grupo de edad más numeroso fue el de 45 a 54 años (28 encuestados), seguido del de 65 a 74 (19), el de 55 a 64 (14) y el de 75 o más (2).

Desde una perspectiva territorial, los encuestados procedían de una amplia área de la región del Lacio, incluyendo tanto el norte de Lacio como el área metropolitana de Roma. La muestra fue heterogénea en términos de contexto de residencia, abarcando áreas urbanas, rurales y semiurbanas, así como distintas situaciones laborales y niveles educativos. Esta diversidad ofrece una visión integral de las experiencias, prácticas y necesidades percibidas de los adultos mayores de 45 años en el contexto italiano.

Resultados principales

El conjunto de datos italiano indica que los adultos mayores de 45 años son, en general, usuarios activos de las tecnologías digitales, aunque su nivel de confianza varía según el tipo de competencia.

El uso diario de dispositivos digitales está ampliamente extendido: el 77,8% de los encuestados valoró su uso de smartphones u ordenadores en los niveles más altos (4 o 5), con una puntuación media de 4,19/5. La confianza general en el uso de internet también es relativamente alta (media de 3,79/5), lo que sugiere que la mayoría de los participantes se sienten cómodos realizando actividades habituales en línea.

Esta confianza se vuelve menos consistente cuando se evalúan competencias específicas de seguridad digital. Los comportamientos más sólidos reportados guardan relación con prácticas preventivas básicas en la navegación cotidiana. Una gran mayoría de encuestados afirmó evitar hacer clic en enlaces desconocidos o sospechosos (73,0%) y verificar la información antes de compartirla en línea (71,4%), mientras que el 60,3% declaró bloquear o denunciar mensajes, perfiles o sitios web sospechosos. Estos hallazgos evidencian la existencia de hábitos defensivos básicos desarrollados a través de la experiencia.

Al mismo tiempo, las competencias más técnicas o especializadas revelan carencias significativas. Menos de la mitad de los encuestados (47,6%) declaró ser capaz de identificar si un sitio web es seguro, por ejemplo, verificando el protocolo HTTPS o los indicadores de seguridad. De igual modo, solo el 50,8% se mostró seguro a la hora de ajustar la configuración de privacidad o seguridad en sus dispositivos, y la misma proporción indicó utilizar contraseñas seguras y únicas. Los resultados son aún más débiles en lo relativo al mantenimiento de dispositivos y software: únicamente el 36,5%

afirmó actualizar regularmente sus dispositivos, aplicaciones y software antivirus, mientras que una parte significativa expresó incertidumbre en este ámbito.

La debilidad más crítica concierne al reconocimiento de contenidos generados o manipulados por inteligencia artificial. Solo el 38,1% de los encuestados se valoró positivamente en su capacidad para identificar imágenes, vídeos o mensajes alterados, y menos de la mitad declaró verificar regularmente si el contenido digital podría haber sido manipulado. Esto confirma una brecha competencial significativa en relación con los riesgos digitales emergentes.

La concienciación sobre el fraude en línea existe, pero es desigual según el tipo de amenaza. Los riesgos tradicionales, como el phishing y la desinformación en redes sociales, son relativamente conocidos, con aproximadamente dos tercios de los encuestados reportando una concienciación moderada o alta. La concienciación es algo menor para las estafas relacionadas con tiendas en línea falsas, el fraude en pagos o el robo de identidad, y disminuye aún más ante las amenazas basadas en IA. Solo el 54,0% de los encuestados declaró tener una concienciación moderada o alta sobre las estafas generadas por IA, mientras que una proporción considerable indicó tener escasa o ninguna concienciación.

La experiencia directa con el fraude también es significativa. Más de un tercio de los encuestados (38,1%) declaró haber sido víctima de algún tipo de fraude digital, principalmente fraude bancario o financiero y estafas de compras falsas, seguidas de phishing y robo de identidad. Esto indica que la exposición a los riesgos digitales no solo se percibe, sino que también se experimenta de forma concreta.

La preocupación por ser víctima de fraude en el futuro es especialmente elevada: el 84,1% de los encuestados expresó niveles claros de preocupación al respecto. En conjunto, los resultados ponen de manifiesto una discrepancia entre el uso digital habitual y las competencias más avanzadas en materia de seguridad.

Interpretación

Los resultados italianos confirman que la interacción digital frecuente no se traduce necesariamente en competencias efectivas de seguridad digital entre los adultos mayores de 45 años.

Una primera cuestión clave puede describirse como una «ilusión de competencia». Muchos participantes se apoyan en el uso rutinario y en el aprendizaje experiencial, desarrollando hábitos preventivos básicos como evitar enlaces sospechosos o verificar información de manera informal. Sin embargo, esta familiaridad no está respaldada por un conocimiento estructurado, lo que se traduce en debilidades en áreas como el reconocimiento de sitios web seguros, la gestión de la configuración de privacidad, el mantenimiento de las actualizaciones de software y la identificación de contenidos manipulados o generados por IA. Como resultado, los usuarios pueden sobreestimar su capacidad para navegar de forma segura en entornos digitales.

Una segunda vulnerabilidad crítica está relacionada con la naturaleza cambiante de las amenazas en línea. La dificultad para reconocer contenidos generados por IA señala un cambio en el riesgo digital, donde las estrategias tradicionales de detección resultan cada vez más insuficientes. Esto evidencia una brecha generacional, ya que las nuevas formas de fraude requieren nuevas formas de conciencia crítica y técnica.

Los datos apuntan también a una tendencia hacia estrategias informales y reactivas de afrontamiento. Muchos encuestados recurren a la intuición, a comportamientos de evitación o al apoyo externo —como pedir ayuda a familiares— en lugar de estrategias estructuradas de prevención. Si bien estos enfoques pueden ofrecer cierta protección parcial, resultan insuficientes en escenarios más complejos y pueden contribuir a la inseguridad o a una participación limitada en los servicios digitales.

Al mismo tiempo, el elevado nivel de preocupación por la posible victimización, combinado con la importante proporción de encuestados que ya ha experimentado fraudes, indica una fuerte necesidad percibida de apoyo. Los participantes son conscientes de los riesgos, pero carecen de las herramientas necesarias para gestionarlos eficazmente.

Desde una perspectiva formativa, estos hallazgos subrayan la necesidad de intervenciones educativas específicas, prácticas y accesibles. La formación debe ir más allá de la concienciación general y centrarse en el desarrollo de competencias concretas, como el reconocimiento de patrones fraudulentos, la verificación de la información digital, la gestión segura de los datos personales y la respuesta adecuada ante situaciones sospechosas. Se debe prestar especial atención a los riesgos emergentes, especialmente los vinculados a la inteligencia artificial y a los contenidos manipulados.

Los enfoques educativos deben ser accesibles y estar fundamentados en situaciones de la vida real, con el fin de reducir la brecha entre las prácticas digitales cotidianas y las competencias de seguridad más avanzadas. Fortalecer la confianza digital de manera estructurada e informada será esencial para apoyar a los adultos mayores de 45 años en su transición hacia un uso seguro, autónomo y resiliente de las tecnologías digitales.

5.2 España

Propósito y Metodología

La encuesta española se realizó en el marco de la evaluación de necesidades de digiSAFE con el objetivo de recopilar datos cuantitativos sobre los hábitos digitales, la concienciación ante los riesgos en línea, las experiencias con el fraude digital y las necesidades formativas de los adultos mayores de 45 años. El objetivo era obtener evidencias comparables entre los países socios.

El cuestionario se administró en línea y se distribuyó a través de las redes de la Asociación UNO, incluidas asociaciones locales y canales informales de aprendizaje para adultos. La participación fue voluntaria y anónima, en pleno cumplimiento del Reglamento General de Protección de Datos (RGPD).

Se recogió un mínimo de 50 respuestas válidas de participantes españoles mayores de 45 años, cumpliendo los requisitos de comparabilidad del proyecto y garantizando la fiabilidad del conjunto de datos. La muestra incluyó una ligera mayoría de mujeres (58,8%). Los encuestados se concentraron en los grupos de edad de 45 a 54 años y de 65 a 74, siendo todos los participantes mayores de 45 años.

La muestra contaba con un nivel educativo relativamente alto, con la mayoría de los participantes en posesión de estudios secundarios o superiores. Una proporción significativa estaba jubilada (47,1%), mientras que el resto estaba empleada o ejercía como autónoma. Desde una perspectiva territorial, la mayoría de los participantes residía en zonas urbanas, con una menor proporción en contextos rurales o semiurbanos. En su conjunto, la muestra ofrece una visión representativa de los adultos mayores de 45 años con presencia digital activa en España, al tiempo que refleja diferencias en las situaciones vitales y en los niveles de autonomía digital.

Resultados principales

El conjunto de datos español muestra que los adultos mayores de 45 años participan activamente en el entorno digital, especialmente en actividades cotidianas. La mayoría de los encuestados declaró utilizar herramientas digitales a diario, principalmente para la comunicación (aplicaciones de mensajería y correo electrónico), la banca en línea, las redes sociales y el acceso a servicios públicos.

Al mismo tiempo, los resultados revelan vulnerabilidades importantes. El uso diario general de dispositivos alcanza un nivel moderado (media de 3,29/5), mientras que la confianza general en el uso de internet es ligeramente inferior (media de 3,00/5), con una proporción considerable de encuestados que reportan confianza limitada. Las respuestas cualitativas sugieren que muchas personas recurren a apoyos externos —en

particular de familiares más jóvenes— cuando se encuentran con dificultades en línea, lo que indica cierto grado de dependencia digital en lugar de una plena autonomía.

Las competencias digitales autoevaluadas son, en general, limitadas en varios ámbitos clave. Las competencias básicas, como el reconocimiento de sitios web seguros, muestran niveles de confianza relativamente bajos (media de 2,76/5), mientras que las habilidades más técnicas —como ajustar la configuración de privacidad, gestionar contraseñas seguras o identificar contenidos generados por IA— representan los ámbitos más débiles. Además, muchos encuestados declararon incertidumbre a la hora de distinguir mensajes legítimos de intentos de phishing y de saber cómo actuar adecuadamente en caso de sospecha de fraude.

La concienciación sobre los riesgos en línea varía según el tipo de amenaza. Las formas tradicionales de fraude, como el phishing y las ofertas de inversión falsas, son relativamente bien reconocidas, y varios encuestados declararon haber tenido experiencia directa con estos riesgos. Por el contrario, la concienciación sobre amenazas más recientes —especialmente las relacionadas con la inteligencia artificial, como los deepfakes o la desinformación generada por IA— es significativamente menor, con una proporción notable de participantes que desconocen estas formas de engaño.

Los comportamientos de seguridad autoevaluados revelan un patrón mixto. Las prácticas más intuitivas, como evitar enlaces sospechosos o verificar la información antes de compartirla, son relativamente habituales. Sin embargo, los comportamientos más técnicos y preventivos, como actualizar el software regularmente, gestionar la configuración de privacidad o verificar contenidos manipulados, se adoptan de manera menos sistemática. Esto sugiere que la concienciación básica no siempre se traduce en prácticas de protección efectivas.

Las experiencias con el fraude digital son relativamente frecuentes. Más de un tercio de los encuestados (35,3%) declaró haber sido víctima de estafas en línea, principalmente phishing, compras fraudulentas y fraude financiero. Incluso en los casos en que no se produjo pérdida económica, estas experiencias contribuyeron a una reducción de la confianza en los entornos digitales y a un incremento de la incertidumbre en las interacciones en línea.

La preocupación por ser víctima de fraude en el futuro es notablemente elevada, con más del 80% de los encuestados expresando niveles de preocupación moderados o altos. Al mismo tiempo, los participantes mostraron un fuerte interés en recibir más formación, especialmente en áreas como el reconocimiento y la prevención del fraude en línea, la protección de datos personales, la seguridad en la banca digital, la identificación de desinformación y el desarrollo de estrategias prácticas para mejorar la seguridad digital en la vida cotidiana.

En conjunto, los resultados ponen de manifiesto una brecha entre la participación digital generalizada y las competencias más avanzadas en materia de seguridad digital.

Interpretación

Los resultados españoles apuntan a una brecha estructural entre la participación digital y la capacidad de gestionar los riesgos en línea de forma autónoma entre los adultos mayores de 45 años.

Si bien el uso digital básico está ampliamente extendido, el conocimiento específico relacionado con la prevención del fraude, las prácticas de ciberseguridad y el reconocimiento de riesgos sigue siendo limitado. Esto crea una situación en la que los individuos participan activamente en entornos digitales sin estar plenamente equipados para navegar por ellos de forma segura, lo que incrementa su exposición tanto a amenazas tradicionales como emergentes.

Es importante destacar que esta vulnerabilidad no se debe a una falta de motivación ni a una resistencia a la tecnología. Al contrario, los encuestados expresaron una clara disposición a aprender y mejorar sus competencias. El problema principal radica en la escasa disponibilidad de formación accesible, específica y orientada a la práctica, centrada en la seguridad digital.

Los datos también revelan una dependencia de estrategias de aprendizaje informales y reactivas. Muchos participantes recurren a familiares, al método de ensayo y error o a búsquedas en línea para resolver problemas, en lugar de basarse en conocimientos estructurados o en formación formal. Si bien estas estrategias pueden proporcionar soluciones temporales, no garantizan una protección consistente o eficaz, especialmente en escenarios de riesgo más complejos o en constante evolución.

Además, la escasa concienciación sobre las amenazas relacionadas con la IA pone de relieve un desafío creciente. A medida que los riesgos digitales se vuelven más sofisticados, las formas tradicionales de detección basadas en la intuición o en la experiencia previa resultan cada vez más insuficientes. Esto refuerza la necesidad de actualizar las competencias de seguridad digital en consonancia con los avances tecnológicos.

El elevado nivel de preocupación por la victimización futura, combinado con la frecuencia de las experiencias pasadas de fraude, indica una fuerte necesidad percibida de apoyo. Los encuestados son conscientes de los riesgos, pero carecen de la confianza y las herramientas necesarias para abordarlos con eficacia.

Desde una perspectiva formativa, estos resultados subrayan la importancia de desarrollar intervenciones educativas específicas, accesibles y adaptadas a los adultos en

formación. La formación debe centrarse en el fortalecimiento de competencias concretas, como el reconocimiento de patrones fraudulentos, la gestión segura de datos personales, la verificación de contenidos digitales y la respuesta adecuada ante situaciones sospechosas.

Los enfoques educativos no formales son especialmente pertinentes en este contexto. Los programas deben utilizar un lenguaje claro, situaciones de la vida real y ejercicios prácticos para reducir la brecha entre las prácticas digitales cotidianas y las competencias de seguridad más avanzadas. Fortalecer la autonomía y la resiliencia digital será esencial para apoyar a los adultos mayores de 45 años en su participación segura y confiada en la sociedad digital.

5.3 Eslovaquia

Propósito y Metodología

La encuesta eslovaca se realizó en el marco de la evaluación de necesidades de digiSAFE con el objetivo de evaluar los hábitos digitales, la confianza técnica, la concienciación ante los riesgos en línea y las experiencias con el fraude digital entre los adultos mayores de 45 años. Los datos recabados están destinados a informar directamente el desarrollo del currículo educativo y el kit de herramientas de seguridad digital del proyecto.

La investigación adoptó un enfoque cuantitativo, utilizando un cuestionario en línea estandarizado diseñado para garantizar la accesibilidad y la comparabilidad entre los países socios. La encuesta incluyó una combinación de preguntas de escala Likert y de opción múltiple, orientadas a evaluar áreas clave como el uso diario de internet, las competencias digitales autopercibidas, la concienciación sobre amenazas cibernéticas tanto tradicionales como emergentes, y las experiencias directas con el fraude en línea.

A nivel transnacional, se recogió un total de 131 respuestas. A efectos del análisis nacional, el conjunto de datos se filtró cuidadosamente para incluir únicamente a los encuestados residentes en Eslovaquia o en otro país europeo, de acuerdo con los criterios del proyecto. Este proceso dio como resultado una muestra final de 51 respuestas válidas, cumpliendo el umbral mínimo requerido para la comparabilidad.

La muestra está compuesta principalmente por personas en fase de actividad profesional y jubilación temprana: el 43% de los encuestados tiene entre 45 y 54 años, el 35% entre 55 y 64, y el 22% tiene 65 o más. Las mujeres representan el 65% de la muestra. Los participantes tienen un nivel educativo relativamente elevado, con la mayoría en posesión de cualificaciones de educación secundaria superior o postsecundaria, y están distribuidos de forma bastante equitativa entre zonas urbanas (55%) y rurales (45%). En su conjunto, la muestra refleja una población con participación digital activa y características sociodemográficas diversas.

Resultados principales

El conjunto de datos eslovaco revela un alto nivel de participación digital entre los adultos mayores de 45 años, acompañado de importantes brechas en materia de competencia en ciberseguridad.

La conectividad es especialmente elevada: el 92% de los encuestados declara usar a diario un smartphone u ordenador. La confianza general para realizar actividades básicas en línea, como el correo electrónico o las compras en internet, también es relativamente alta (68%). Sin embargo, este uso frecuente no se traduce en seguridad técnica efectiva.

Se identifican carencias importantes en las competencias básicas de seguridad digital. Solo el 35% de los encuestados se siente plenamente seguro para reconocer si un sitio web es seguro, por ejemplo, identificando protocolos HTTPS o indicadores de seguridad. De igual modo, menos de la mitad (41%) declara ser capaz de ajustar la configuración de privacidad y seguridad en sus dispositivos. Estos resultados sugieren que, aunque los usuarios están operativamente activos en línea, carecen de las competencias técnicas necesarias para gestionar los riesgos de forma independiente.

Se observa una clara divisoria en la concienciación sobre los diferentes tipos de amenazas cibernéticas. Los riesgos tradicionales son ampliamente reconocidos: el 85% de los encuestados declara tener una concienciación moderada o alta sobre correos electrónicos de phishing, mensajes SMS fraudulentos y tiendas en línea falsas. Por el contrario, la concienciación sobre las amenazas emergentes es significativamente menor. Un dato llamativo es que el 78% de los participantes declara tener escasa o ninguna concienciación sobre las estafas generadas por IA, como los deepfakes o la clonación de voz. Del mismo modo, el 72% indica poca confianza en su capacidad para identificar contenidos o noticias manipulados por IA.

La experiencia directa con el fraude digital también es notable. Un cuarto de los encuestados (25%) declara haber sido víctima de estafas en línea. Los patrones de respuesta entre las víctimas revelan un problema crítico: la mayoría recurre a reacciones informales, con el 62% declarando que eliminó el mensaje malicioso o buscó ayuda entre familiares y amigos. Solo una pequeña minoría (15%) comunicó el incidente formalmente a bancos, plataformas en línea o las autoridades.

En conjunto, los resultados apuntan a un fuerte desequilibrio entre los altos niveles de actividad digital y la capacidad limitada para gestionar tanto los riesgos en línea tradicionales como los emergentes.

Interpretación

Los resultados eslovacos ponen de manifiesto una marcada brecha entre la participación digital y la competencia efectiva en ciberseguridad entre los adultos mayores de 45 años.

Si bien los encuestados son usuarios frecuentes y confiados de las tecnologías digitales para fines cotidianos, su capacidad para gestionar riesgos sigue siendo limitada. Esto crea una «brecha de confianza», en la que los individuos poseen las competencias operativas necesarias para navegar por los entornos digitales, pero carecen de los conocimientos técnicos requeridos para garantizar su propia seguridad. La adopción digital parece estar impulsada principalmente por la comodidad y la necesidad, más que por una comprensión integral del ecosistema digital.

Una vulnerabilidad clave concierne a la rápida evolución de las amenazas digitales. Si bien los encuestados demuestran un sólido conocimiento de las formas tradicionales de ciberdelincuencia, como el phishing o las tiendas en línea falsas, están significativamente menos preparados para hacer frente a formas de fraude más avanzadas. La escasa concienciación sobre las estafas generadas por IA y la limitada capacidad para identificar contenidos manipulados indican una brecha generacional crítica. Estas amenazas emergentes se apoyan a menudo en la manipulación psicológica y en estímulos emocionales, lo que las hace más difíciles de detectar mediante estrategias convencionales.

Otro aspecto importante se refiere a las respuestas conductuales ante los incidentes cibernéticos. Los datos revelan una fuerte dependencia de mecanismos informales de afrontamiento, como ignorar mensajes sospechosos o buscar ayuda en redes personales. La tasa extremadamente baja de denuncias formales sugiere tanto una falta de conocimiento sobre los procedimientos oficiales como la presencia de barreras psicológicas, incluida la vergüenza, el miedo o la sensación de inevitabilidad. Esto limita la eficacia de los mecanismos institucionales de protección y aumenta el impacto a largo plazo del fraude.

Desde una perspectiva formativa, estos resultados apuntan a la necesidad de un cambio desde la participación digital básica hacia competencias de seguridad digital más estructuradas y proactivas. Las intervenciones educativas deben priorizar enfoques prácticos y basados en escenarios, que permitan a los participantes reconocer y responder a situaciones de la vida real, especialmente las que implican estafas sofisticadas o impulsadas por IA.

Además, la formación debe incluir orientaciones claras y accesibles sobre la configuración de la privacidad y la seguridad, así como instrucciones paso a paso sobre cómo denunciar incidentes y buscar apoyo institucional. Abordar la dimensión

psicológica de la ciberdelincuencia —normalizando la victimización y reduciendo el estigma— también será esencial para fomentar comportamientos más proactivos y seguros.

Fortalecer tanto la competencia técnica como la confianza del usuario será fundamental para apoyar a los adultos mayores de 45 años en Eslovaquia en su transición desde estrategias pasivas o reactivas hacia una participación más autónoma, informada y resiliente en el entorno digital.

6. Análisis Transnacional

La comparación de los resultados nacionales de Italia, España y Eslovaquia revela un conjunto de convergencias notables que apuntan a un desafío europeo común, junto con algunas diferencias nacionales significativas que tienen implicaciones para el diseño de intervenciones educativas adaptadas.

6.1 Desafíos comunes entre países

Los tres países presentan una brecha consistente y estructuralmente significativa entre la participación digital y la competencia en seguridad digital. Los adultos mayores de 45 años en Italia, España y Eslovaquia son, en mayor o menor medida, usuarios habituales y activos de internet, que utilizan los servicios digitales para comunicarse, realizar operaciones bancarias, buscar información y hacer comercio electrónico. Sin embargo, en los tres contextos, la confianza autoevaluada y la competencia real descienden marcadamente cuando se evalúan competencias de seguridad digital más específicas: reconocimiento de sitios web seguros, gestión de la configuración de privacidad, mantenimiento de actualizaciones de software y gestión segura de datos.

Un segundo patrón convergente es la debilidad casi universal para reconocer contenidos generados o manipulados por IA. En los tres países, este es consistentemente el ámbito más vulnerable entre los encuestados, muy por debajo de la concienciación sobre amenazas tradicionales como el phishing o las tiendas en línea falsas. Este hallazgo es especialmente urgente: el fraude basado en IA —deepfakes, clonación de voz, mensajes de estafa generados por IA— es la categoría de amenaza digital de más rápido crecimiento, y es precisamente aquella para la que la población mayor de 45 años en Europa está menos preparada.

Un tercer desafío compartido es la dependencia de estrategias informales y reactivas de afrontamiento. En Italia, España y Eslovaquia por igual, muchos encuestados recurren a la intuición, la precaución o el apoyo externo de familiares, en lugar de contar con conocimientos y competencias estructuradas. Este enfoque de «defensa informal» puede reducir algunos riesgos, pero resulta totalmente inadecuado ante el engaño sofisticado

asistido por IA. Además, tiende a reforzar los comportamientos de evitación digital en lugar de construir una resiliencia genuina.

Por último, los tres países registran niveles significativos de preocupación por la victimización futura (84,1% en Italia, más del 80% en España, elevado también en Eslovaquia) y tasas notables de victimización pasada: 38,1% en Italia, 35,3% en España y 25% en Eslovaquia. La brecha entre preocupación y competencia es una característica constante en el conjunto de datos transnacional.

6.2 Principales diferencias

A pesar de estas convergencias, existen diferencias significativas entre los tres contextos nacionales. Italia y Eslovaquia presentan niveles muy altos de participación digital diaria (77,8% y 92% respectivamente, valorando el uso diario de dispositivos en los niveles más altos), mientras que los encuestados españoles muestran patrones de participación algo más moderados (media de uso diario de dispositivos de 3,29/5). Esto sugiere que los encuestados españoles, aunque digitalmente activos, pueden estar algo menos inmersos en rutinas digitales intensivas que sus homólogos italianos y eslovacos.

La naturaleza de las amenazas de fraude predominantes varía según el contexto. En Eslovaquia se ha documentado un patrón de amenaza especialmente grave y específico: sofisticados ataques de vishing en los que los defraudadores suplantan la identidad de agentes de policía o funcionarios bancarios para manipular a las víctimas y conseguir que transfieran fondos. Esta forma de ingeniería social explota la confianza institucional de maneras que están menos documentadas en los contextos italiano y español. Eslovaquia también se enfrenta a un desafío particular relacionado con el volumen e impacto de las campañas de desinformación, amplificadas por la situación geopolítica del país.

Las tasas de denuncia formal de incidentes difieren notablemente. Los encuestados eslovacos mostraron una tasa de denuncia formal alarmantemente baja (solo el 15% de las víctimas comunicó el incidente formalmente), significativamente inferior a la registrada en los contextos italiano y español. Esto apunta a una cultura del estigma en torno a la victimización más arraigada en Eslovaquia y/o a un menor conocimiento de los canales institucionales de denuncia, lo que constituye un ámbito específico que requiere intervención específica.

Italia presenta una infraestructura institucional y programática más sólida para la inclusión digital (Repubblica Digitale, CPIA, Programa GOL) en comparación con Eslovaquia, donde los programas de ámbito nacional son más recientes y han llegado a menos personas. España ocupa una posición intermedia, con marcos nacionales sólidos (INCIBE, España Digital 2026), pero con una implementación desigual según las regiones.

6.3 Patrones de comportamiento

En los tres países, los encuestados exhiben un patrón de comportamiento consistente: la confianza en las tareas rutinarias de alta frecuencia (consultar el correo electrónico, realizar operaciones bancarias en línea, usar aplicaciones de mensajería) coexiste con la inseguridad y la escasa competencia en las tareas de baja frecuencia pero de alto riesgo (verificar la seguridad de los sitios web, configurar la privacidad, identificar contenidos manipulados). Este patrón sugiere que la habitualidad digital genera una falsa sensación de competencia global que no se extiende a los comportamientos críticos en materia de seguridad.

La confianza en las herramientas digitales es, en general, moderada o alta para las plataformas y servicios conocidos y de uso habitual, pero disminuye significativamente cuando se enfrenta a fuentes desconocidas, solicitudes no familiares o situaciones ambiguas. Los encuestados de los tres países tienden a gestionar esta ambigüedad mediante la evitación (no hacer clic, no participar) en lugar de la verificación activa: un enfoque que reduce el riesgo, pero no lo gestiona.

La exposición al riesgo es mayor en Italia (tasa de victimización del 38,1%), seguida de España (35,3%) y, a continuación, de Eslovaquia (25%). Sin embargo, estas diferencias pueden reflejar en parte diferencias en la composición de la muestra y en los canales de difusión de la encuesta. En los tres países, las formas más habituales de fraude experimentado son de naturaleza financiera (fraude bancario, compras falsas, phishing), lo que confirma que el ámbito financiero es el principal escenario de perjuicio.

6.4 Perspectivas transnacionales de las buenas prácticas

En Italia, España y Eslovaquia, el análisis de las buenas prácticas revela una serie de patrones comunes que trascienden los contextos nacionales específicos y ponen de relieve enfoques compartidos en materia de educación sobre seguridad digital para adultos mayores de 45 años.

Un fuerte énfasis en el aprendizaje no formal y orientado a la práctica emerge de manera consistente en los tres países. Las iniciativas raramente se basan únicamente en la instrucción teórica; priorizan las actividades prácticas, los escenarios de la vida real y las orientaciones paso a paso. Esto refleja la necesidad de traducir los riesgos digitales abstractos en situaciones concretas y comprensibles para los adultos en formación. En Eslovaquia, esta orientación es especialmente visible en las Academias Smart Senior organizadas en las bibliotecas públicas regionales, donde bibliotecarios y formadores voluntarios guían a pequeños grupos a través de ejercicios prácticos a su propio ritmo, y en los seminarios de base comunitaria organizados por la Unión de Pensionistas (JDS), centrados en amenazas inmediatas y localmente relevantes, como las tiendas en línea fraudulentas y las llamadas telefónicas falsas.

Muchas buenas prácticas adoptan también un enfoque comunitario e inclusivo, implementado a través de centros locales, asociaciones o instituciones públicas que ya son familiares y de confianza para el grupo destinatario. En los tres países, los entornos de aprendizaje están diseñados para ser accesibles y de bajo umbral de entrada, reduciendo las barreras a la participación y fomentando la confianza entre los participantes. El modelo descentralizado de Eslovaquia —especialmente a través del programa Zrelí na dobu digitálnu del Fondo de Dotación de Slovak Telekom, que canaliza la financiación directamente hacia residencias de mayores y centros comunitarios— ofrece un ejemplo particularmente replicable de cómo la prestación comunitaria puede llegar a las personas mayores aisladas en zonas rurales que no asistirían a cursos de gran escala organizados de forma centralizada.

El uso del aprendizaje entre iguales y de modelos intergeneracionales o de apoyo entre pares representa otra característica compartida. En Italia, esto es más visible en iniciativas como el Servicio Civil Digital, mientras que en España el mentoring voluntario y la participación comunitaria desempeñan un papel similar. En Eslovaquia, el modelo de confianza entre iguales adoptado en los seminarios de la JDS, donde el aprendizaje tiene lugar dentro de redes de jubilados con experiencias similares, demuestra que reducir la ansiedad psicológica en torno a las herramientas digitales es tan importante como transmitir contenidos. Los adultos mayores de 45 años se benefician consistentemente de procesos de aprendizaje colaborativos y socialmente integrados, más que de modelos individuales y autodirigidos.

Un patrón más visible en Eslovaquia que en los otros dos países es la participación activa del sector privado en la educación digital pública. El portal Bezpečne na nete, creado por la empresa de ciberseguridad ESET, ejemplifica cómo la experiencia del sector privado puede canalizarse hacia contenidos educativos gratuitos, continuamente actualizados y accesibles al público: un modelo que otros contextos europeos podrían replicar a través de marcos de responsabilidad social corporativa.

Junto a estas convergencias, se pueden observar diferencias significativas. Italia muestra una mayor integración entre las estrategias nacionales y las iniciativas de múltiples niveles, con acciones coordinadas que vinculan marcos de política, programas de formación y campañas de concienciación. España presenta un panorama más descentralizado y variado, con una amplia gama de actores que operan a nivel nacional, regional y local, a veces sin una fuerte coordinación entre ellos. Eslovaquia ocupa una posición intermedia: aunque su marco institucional es sólido (coordinado por entidades como el NBÚ y MIRRI), el alcance de los programas formales entre el grupo de 45 a 64 años sigue siendo limitado, y las iniciativas más eficaces tienden a ser no formales y de base comunitaria.

La evidencia global de los tres países socios apunta a la misma conclusión: una educación eficaz en seguridad digital para los adultos mayores de 45 años se basa en una combinación de accesibilidad, relevancia práctica, aprendizaje social y confianza. Estos elementos representan componentes transferibles clave que deberían informar directamente el desarrollo del currículo y el kit de herramientas de digiSAFE.

7. Conclusiones principales

Las siguientes conclusiones principales emergen del análisis transnacional de los resultados de la investigación nacional:

1. La participación digital no equivale a seguridad digital. En Italia, España y Eslovaquia, los adultos mayores de 45 años son usuarios activos y frecuentes de internet, aunque demuestran consistentemente una competencia reducida en competencias específicas de seguridad digital, como el reconocimiento de sitios web seguros, la configuración de la privacidad y la gestión de la seguridad de las cuentas.
2. Las amenazas basadas en IA representan la brecha más crítica y universal. La concienciación y el reconocimiento de las estafas generadas por IA, los deepfakes y los contenidos manipulados son los ámbitos de competencia más débiles en los tres países. Al mismo tiempo, constituye la categoría de amenaza en línea de más rápido crecimiento, lo que la convierte en la prioridad más urgente de intervención educativa.
3. Las estrategias informales de afrontamiento predominan y resultan insuficientes. La respuesta conductual primaria ante el riesgo percibido en los tres países es informal, intuitiva y reactiva (evitación, apoyo familiar, precaución general) en lugar de estructurada y proactiva. Este enfoque ofrece una protección inadecuada frente a la ingeniería social sofisticada y al fraude asistido por IA.
4. Las tasas de victimización pasada son elevadas e infraestimadas. Entre una cuarta parte y casi dos quintos de los encuestados en los tres países declararon haber tenido una experiencia directa con el fraude digital, confirmando que estos riesgos no son teóricos, sino reales e inmediatos para el grupo destinatario.
5. La preocupación es elevada, pero no está respaldada por las competencias necesarias. En los tres países, la gran mayoría de los encuestados (más del 80%) expresa una clara preocupación por la victimización futura. Este alto nivel de preocupación, combinado con los déficits de competencia reconocidos, indica una demanda fuerte e insatisfecha de formación específica.
6. La denuncia formal de incidentes está críticamente infrautilizada. Un patrón consistente en los tres países —más pronunciado en Eslovaquia— es la tendencia a gestionar los incidentes de fraude de forma informal, sin notificarlo a los bancos,

las plataformas o las fuerzas del orden. Esta subnotificación limita las respuestas sistémicas y deja a las víctimas sin apoyo institucional.

7. La «brecha de confianza» es una vulnerabilidad sistémica. En los tres países, los encuestados tienden a sobreestimar su seguridad digital global basándose en su alta competencia en tareas rutinarias, mientras subestiman su vulnerabilidad específica en situaciones de alto riesgo y menor familiaridad. Esta ilusión de competencia requiere enfoques educativos que cuestionen las suposiciones previas y construyan una conciencia digital genuinamente crítica.
8. Los marcos de política nacional existen, pero su implementación es desigual. Los tres países han desarrollado marcos regulatorios y programas de competencias digitales pertinentes, pero su alcance entre el grupo demográfico de mayores de 45 años sigue siendo limitado, especialmente en Eslovaquia y en las zonas rurales de los tres países.

8. Deficiencias detectadas y necesidades de formación

Sobre la base de la investigación documental, el análisis de la encuesta y la comparación transnacional, se han identificado las siguientes brechas específicas y necesidades formativas para los adultos mayores de 45 años en Italia, España y Eslovaquia. Si bien varias de estas brechas son comunes a los tres contextos, su intensidad y manifestación difieren de maneras directamente relevantes para el diseño del currículo.

8.1 Brechas de competencias

En los tres países, se evidencia una brecha significativa entre la frecuencia con la que los adultos mayores de 45 años utilizan las tecnologías digitales y su capacidad real para gestionar los riesgos en línea. En Eslovaquia, el 92% de los encuestados declaró usar a diario un smartphone u ordenador —una cifra coherente con las altas tasas de conectividad observadas en Italia y España— y, sin embargo, esta frecuencia no se traduce en un conocimiento estructurado de las prácticas de seguridad digital. En Eslovaquia, solo el 35% de los encuestados se sentía seguro para reconocer un sitio web seguro, y menos de la mitad (41%) declaró saber cómo ajustar la configuración de privacidad y seguridad en sus propios dispositivos. Este patrón, que el informe eslovaco describe acertadamente como una «brecha de confianza», está estructuralmente presente en los tres países, aunque parece más agudo en España, donde la fuerte dependencia de los familiares como fuente principal de apoyo digital sugiere una forma de dependencia más que una autonomía digital genuina.

Más concretamente, la capacidad de verificar técnicamente la seguridad y autenticidad de los entornos digitales sigue siendo débil en los tres países: identificar sitios web seguros (indicadores HTTPS, iconos de candado), reconocer marcadores de correos

electrónicos de phishing o distinguir mensajes SMS legítimos de fraudulentos son competencias que una parte significativa de los encuestados no ha desarrollado. La gestión de la seguridad de dispositivos y cuentas —incluida la configuración de la privacidad, el uso de contraseñas seguras y únicas, la activación de la autenticación en dos pasos y la realización de actualizaciones regulares de software y antivirus— es practicada por una minoría y comprendida por aún menos personas. Los encuestados italianos parecen algo más seguros en algunos comportamientos de protección rutinarios, mientras que los participantes españoles y eslovacos muestran mayor incertidumbre a la hora de aplicar estas prácticas de forma consistente.

8.2 Brechas de conocimiento

La brecha de conocimiento más crítica y universal en los tres países concierne al reconocimiento de contenidos generados o manipulados por IA. En Italia, este es ya uno de los ámbitos de competencia más débiles, con puntuaciones de autoevaluación consistentemente bajas en la identificación de riesgos basados en IA. Los datos eslovacos refuerzan este hallazgo con especial claridad: el 78% de los encuestados indicó tener escasa o ninguna concienciación sobre las estafas generadas por IA, como los deepfakes y la clonación de voz, y el 72% admitió poca o ninguna confianza para identificar contenidos o noticias manipulados por IA. En España, la concienciación sobre dichas amenazas es aún menos desarrollada, con una proporción significativa de encuestados que declaró tener escaso o ningún conocimiento de las estafas relacionadas con la IA. En los tres contextos, esta es la brecha educativa más urgente: requiere una formación específica basada en escenarios, más que una concienciación genérica.

Más allá de las amenazas relacionadas con la IA, persisten importantes déficits de conocimiento sobre los mecanismos de la ingeniería social y las tácticas de manipulación psicológica utilizadas por los ciberdelincuentes. En Eslovaquia, esto se ve agravado por un panorama de amenazas específico y especialmente dañino: los defraudadores suplantan frecuentemente la identidad de agentes de policía o empleados bancarios mediante tecnología de suplantación de números, explotando precisamente el tipo de confianza institucional que las personas mayores son más propensas a otorgar —un patrón que la formación formal aún no ha abordado de manera adecuada. El conocimiento de los derechos de protección de datos y de los procedimientos formales a seguir tras un incidente de fraude (a quién denunciarlo, qué opciones de recuperación existen) es también críticamente insuficiente en los tres países.

8.3 Brechas de concienciación y respuesta ante incidentes

Otra brecha, consistentemente presente pero de distinta intensidad en los tres países, concierne al comportamiento ante incidentes y a las conductas de denuncia. Entre el 25%

de encuestados eslovacos que habían experimentado fraude digital, solo el 15% optó por denunciar formalmente el incidente a un banco, una plataforma o las fuerzas del orden. La mayoría (62%) simplemente eliminó el mensaje malicioso o buscó ayuda informal entre familiares o amigos. Este patrón se reproduce en los resultados italianos y españoles, y refleja un conjunto compartido de barreras psicológicas: la vergüenza, el estigma y un sentimiento de fatalismo ante la ciberdelincuencia desincentivan activamente a las víctimas de recurrir a los sistemas de apoyo institucional. Para abordar esta barrera es necesario no solo proporcionar orientación procedimental sobre los canales de denuncia, sino también un esfuerzo deliberado para destigmatizar la victimización dentro de los programas educativos.

En el plano de la concienciación general, la brecha más significativa concierne a las amenazas emergentes. Las estafas basadas en IA, los deepfakes, la clonación de voz y la desinformación generada por IA son categorías de riesgo con las que la mayoría de los encuestados en los tres países tienen un conocimiento limitado o nulo. Existe también una falta más amplia de concienciación sobre las consecuencias concretas de la victimización (financieras, sociales y psicológicas), lo que puede contribuir a infravalorar el riesgo entre quienes aún no han sido directamente afectados.

En su conjunto, el panorama comparativo entre Italia, España y Eslovaquia subraya la importancia de diseñar enfoques formativos que sean a la vez transversalmente coherentes y adaptables a las necesidades nacionales específicas. Eslovaquia presenta una vulnerabilidad especialmente pronunciada en relación con las amenazas impulsadas por IA y la explotación de la confianza institucional, mientras que España muestra una mayor dependencia de redes de apoyo informales, e Italia refleja una línea de base de confianza técnica ligeramente superior, aunque aún frágil. Estas diferencias apuntan al valor de un marco curricular modular que pueda abordar las brechas de competencias compartidas, al tiempo que permite la contextualización a nivel nacional.

9. Recomendaciones para el desarrollo curricular

La evidencia recopilada en las tres fases nacionales de investigación proporciona una base clara y fundamentada en la evidencia para el Currículo de Educación No Formal (ENF) de digiSAFE. Las siguientes recomendaciones recogen las brechas y necesidades formativas identificadas en la Sección 8 y se estructuran en torno a los ámbitos temáticos que el currículo debe abordar.

9.1 Módulos temáticos

El currículo está organizado en una secuencia estructurada de componentes de aprendizaje, compuesta por seis módulos principales, apoyados por una fase inicial de orientación y un paso final de cierre y planificación de la acción.

El diseño general permite una flexibilidad en la impartición. El currículo completo puede implementarse como un taller intensivo de 2 días, como una serie de sesiones más cortas, o en un formato mixto que combine elementos presenciales y en línea. Al mismo tiempo, cada módulo está diseñado para funcionar como una sesión independiente de aproximadamente 90 minutos, lo que hace que el currículo sea adaptable a diferentes entornos de aprendizaje y limitaciones de tiempo.

Esta estructura modular garantiza que el currículo pueda ser a la vez completo y flexible, permitiendo tanto la entrega del programa completo como intervenciones específicas basadas en las necesidades locales concretas.

1. Módulo 0: Orientación y evaluación previa. Este módulo introductorio responde a los diversos niveles de confianza digital de partida identificados en todos los países socios. La investigación muestra que, si bien muchos adultos mayores de 45 años son usuarios digitales activos, su concienciación sobre los riesgos y sus competencias autopercebidas varían significativamente. Este módulo es esencial para generar confianza, reducir la ansiedad inicial y ayudar a los participantes a reflexionar sobre sus propios hábitos digitales, su exposición al riesgo y sus necesidades de aprendizaje antes de abordar contenidos más técnicos.
2. Módulo 1: Uso digital seguro en el día a día. Este módulo aborda directamente la brecha identificada entre el uso digital frecuente y la comprensión limitada de los principios básicos de seguridad. En todos los países, los encuestados reportaron altos niveles de participación digital diaria, pero mostraron inconsistencias a la hora de reconocer entornos seguros y aplicar comportamientos de protección rutinarios. El módulo ayuda a los participantes a identificar prácticas de uso seguro, reconocer señales de confianza y desarrollar hábitos digitales cotidianos más conscientes y seguros.
3. Módulo 2: Phishing, smishing y patrones de estafa. Este módulo responde a los altos niveles de exposición al fraude en línea identificados en la investigación. En los tres países, el phishing, los mensajes fraudulentos y las estafas financieras fueron las amenazas más comúnmente experimentadas por los encuestados. Los resultados destacan la necesidad de que los participantes reconozcan los patrones de estafa, identifiquen las señales de advertencia y desarrollen la capacidad de hacer una pausa y evaluar críticamente las comunicaciones sospechosas antes de actuar.
4. Módulo 3: Pagos seguros, compras en línea y protección financiera. Este módulo se justifica por la amplia experiencia de fraude financiero y ofertas falsas en línea reportada en los conjuntos de datos. Muchos encuestados indicaron dificultades para distinguir transacciones legítimas de fraudulentas, especialmente en las compras en línea y los pagos digitales. El módulo se centra en el fortalecimiento de

comportamientos financieros más seguros, ayudando a los participantes a reconocer plataformas poco fiables y a aplicar estrategias de toma de decisiones más seguras.

5. Módulo 4: Privacidad, contraseñas y protección del dispositivo. Este módulo aborda las debilidades consistentes en las prácticas técnicas de seguridad identificadas en todos los países. La investigación evidencia un conocimiento limitado y un uso inconsistente de la configuración de privacidad, las contraseñas seguras y las actualizaciones de software. Estas carencias aumentan significativamente la vulnerabilidad ante las amenazas cibernéticas. El módulo se centra, por tanto, en reforzar la protección de las cuentas y en promover rutinas de seguridad prácticas y cotidianas.
6. Módulo 5: IA, desinformación y contenidos manipulados. Este módulo responde a una de las brechas más críticas y transversales identificadas en la investigación: la limitada capacidad para reconocer contenidos generados por IA y las formas emergentes de manipulación digital. En todos los países socios, la concienciación sobre las amenazas basadas en IA —como los deepfakes, la clonación de voz y los medios sintéticos— era significativamente menor que la concienciación sobre los riesgos tradicionales. Este módulo tiene como objetivo desarrollar el pensamiento crítico y las competencias de verificación necesarias para navegar por entornos de información digital cada vez más complejos.
7. Módulo 6: Qué hacer cuando algo va mal. Este módulo aborda una brecha importante en el conocimiento y el comportamiento de respuesta identificada en los conjuntos de datos. Muchos encuestados declararon incertidumbre sobre cómo actuar en caso de fraude y recurrieron principalmente a estrategias informales, como ignorar los incidentes o pedir ayuda a familiares. Las tasas de denuncia formal fueron bajas. El módulo se centra, por tanto, en proporcionar rutas de respuesta claras, mejorar la confianza en la gestión de incidentes y aumentar la concienciación sobre los mecanismos de apoyo disponibles.
8. Cierre: Plan personal de seguridad digital. El componente de cierre responde a la necesidad de traducir el aprendizaje en un cambio conductual concreto. Los resultados de la investigación muestran altos niveles de preocupación por los riesgos digitales, pero estrategias limitadas y estructuradas para abordarlos. Este paso final ayuda a los participantes a consolidar sus conocimientos, definir acciones personales de seguridad y aumentar su confianza en su capacidad para navegar de forma segura y autónoma por los entornos digitales.

9.2 Principios metodológicos

Los resultados de la investigación apuntan claramente a un conjunto de principios metodológicos que deben guiar el diseño del currículo:

1. Aprendizaje no formal y experiencial: el currículo debe fundamentarse en situaciones de la vida real, estudios de caso y ejercicios prácticos, más que en la instrucción teórica. Los adultos mayores de 45 años responden mejor al aprendizaje que es inmediatamente aplicable a su experiencia digital cotidiana.
2. Práctica basada en escenarios: se debe prestar especial atención a los escenarios simulados en los que los participantes puedan practicar de forma segura el reconocimiento y la respuesta ante intentos de fraude (correos electrónicos de phishing, llamadas sospechosas, mensajes generados por IA), sin riesgo real.
3. Lenguaje y formato accesibles: los conceptos técnicos de ciberseguridad deben traducirse a un lenguaje claro y sin jerga. Se deben utilizar materiales visuales, guías paso a paso y contenidos multimedia para apoyar a los participantes con diferentes niveles de alfabetización.
4. Complejidad gradual: el currículo debe estar estructurado para construir la confianza de manera progresiva, comenzando por los riesgos más fácilmente reconocibles y avanzando hacia amenazas más complejas y emergentes. Este enfoque gradual evita abrumar a los participantes y reduce los comportamientos de evitación digital.
5. Destigmatización de la victimización: dada la documentada reticencia a denunciar formalmente los incidentes de fraude, el currículo debe abordar explícitamente los aspectos psicológicos de la victimización por ciberdelincuencia, normalizando la experiencia y empoderando a los participantes para buscar apoyo institucional sin vergüenza.
6. Adaptabilidad a los contextos nacionales y locales: aunque el marco curricular debe ser transnacional, los módulos deben permitir su adaptación para reflejar las tipologías de fraude específicas, los marcos jurídicos y los canales de denuncia relevantes en cada país socio.

10. Conclusión

El Informe Transnacional del proyecto digiSAFE sintetiza los hallazgos de la investigación nacional realizada en Italia, España y Eslovaquia, ofreciendo un panorama completo y fundamentado en la evidencia de los desafíos en materia de seguridad digital y las necesidades formativas de los adultos mayores de 45 años en tres países europeos.

La evidencia es clara y consistente: aunque los adultos del grupo destinatario son cada vez más activos en los entornos digitales —utilizando internet para operaciones

bancarias, comunicación, servicios públicos e información—, no están suficientemente equipados para navegar por los riesgos en línea que conllevan estas actividades. La brecha entre la participación digital y la competencia en seguridad digital es una característica estructural de los tres contextos nacionales, no un fallo individual. Refleja el ritmo de la transformación digital, la insuficiencia de la oferta educativa existente dirigida a este grupo de edad, y la naturaleza en rápida evolución de las amenazas — especialmente la emergencia del fraude impulsado por IA, que supera las estrategias actuales de concienciación y defensa.

La investigación ha identificado brechas concretas y susceptibles de intervención: en competencias (verificación técnica, seguridad del dispositivo, reconocimiento de contenidos IA), en conocimientos (mecanismos del fraude, derechos de protección de datos, procedimientos de denuncia) y en concienciación (amenazas emergentes de IA, canales de apoyo institucional). Estas brechas constituyen el insumo directo para el Currículo de Educación No Formal de digiSAFE y el Kit de Herramientas de Prevención del Fraude Digital, que se desarrollarán en la siguiente fase del proyecto.

Las buenas prácticas identificadas en los tres países demuestran que las intervenciones educativas eficaces, accesibles y de base comunitaria para el grupo demográfico de mayores de 45 años son perfectamente viables. Iniciativas que van desde la red italiana de facilitación digital hasta los seminarios de aprendizaje entre iguales eslovacos y los programas de mentoring digital voluntario españoles muestran qué funciona y ofrecen modelos replicables para las producciones educativas de digiSAFE.

Al construir directamente sobre los hallazgos de la investigación nacional presentada en este informe, el proyecto digiSAFE establece un vínculo claro entre la evidencia y la acción. Las brechas, necesidades y patrones conductuales identificados informarán directamente el diseño y la estructura del Currículo de Educación No Formal y del Kit de Herramientas de Prevención del Fraude Digital, garantizando que ambos resultados estén fundamentados en las necesidades reales de los usuarios. De este modo, el proyecto está en posición de realizar una contribución significativa y mensurable a la resiliencia digital de los adultos mayores en Italia, España, Eslovaquia y más allá, apoyando una participación más segura, informada y autónoma en la sociedad digital europea.

Bibliografía / Referencias

1. Agency for Digital Italy (AgID) (n.d.). Digital Skills Initiatives. <https://www.agid.gov.it/it/agenzia/competenze-digitali>
2. Bank of Italy (n.d.). Financial Education and Cybersecurity Awareness. <https://economiepertutti.bancaditalia.it>
3. CERTFin (n.d.). I Navigati Campaign. <https://inavigati.certfin.it/index.html>
4. Civic Association eSlovensko (n.d.). Zodpovedne.sk. <https://www.zodpovedne.sk/>

5. Department for Digital Transformation, Italy (n.d.). Repubblica Digitale Strategy. <https://repubblicadigitale.gov.it/portale/strategia>
6. Digitálna koalícia (n.d.). Improving the Digital Skills of Seniors. <https://digitalnakoalicia.sk>
7. Digital Skills and Jobs Platform – European Commission (2024). Spain: A Snapshot of Digital Skills. <https://digital-skills-jobs.europa.eu/en/latest/briefs/spain-snapshot-digital-skills>
8. Digital Skills and Jobs Platform – European Commission (2024). Slovakia: A Snapshot of Digital Skills. <https://digital-skills-jobs.europa.eu/en/latest/briefs/slovakia-snapshot-digital-skills>
9. ESET (n.d.). Bezpečne na nete. <https://bezpecnenanete.eset.com/sk/>
10. EU DisinfoLab (2023). Disinformation Landscape in Slovakia. <https://www.disinfo.eu>
11. European Commission (2024). Slovakia 2025 Digital Decade Country Report. <https://digital-strategy.ec.europa.eu/en/factpages/slovakia-2025-digital-decade-country-report>
12. European Commission (2025). Italy Digital Decade Country Report 2025. <https://digital-strategy.ec.europa.eu/en/factpages/italy-2025-digital-decade-country-report>
13. European Commission – Joint Research Centre (2025). How to Reach the EU Target of 80% of Adults with Basic Digital Skills by 2030. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/how-reach-eu-target-80-adults-basic-digital-skills-2030-2025-03-05_en
14. European Parliament and Council of the EU (2016). Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). OJ L 119, 4.5.2016.
15. European Parliament and Council of the EU (2022). Directive (EU) 2022/2555 – NIS2 Directive.
16. Eurostat (2024). Digitalisation in Europe – 2024 Edition. <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024>
17. Fundación Cibervoluntarios (n.d.). Digital Inclusion Programmes. <https://www.cibervoluntarios.org>
18. Gobierno de España (2018). Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDgdd). BOE.
19. Gobierno de España (2021). Plan Nacional de Competencias Digitales. <https://portal.mineco.gob.es>
20. Gobierno de España (2022). España Digital 2026 – Agenda Nacional de Transformación Digital. <https://espanadigital.gob.es/espana-digital>
21. INCIBE (2024). Los incidentes de ciberseguridad de 2023 gestionados por INCIBE. <https://www.incibe.es>

22. INCIBE (n.d.). Línea de Ayuda en Ciberseguridad 017. <https://www.incibe.es/linea-017>
23. ISTAT (2024). Citizens and ICT Report. https://www.istat.it/wp-content/uploads/2025/04/REPORT_CITTADINI-E-ICT_2024.pdf
24. ISTAT (2024). Digital Skills Statistics. <https://www.istat.it/wp-content/uploads/2024/04/2.pdf>
25. ISTAT (2025). Crimes Against Persons and Property Report. Italian National Institute of Statistics.
26. Italian Data Protection Authority – Garante (n.d.). Personal Data Protection Code. <https://www.garanteprivacy.it>
27. Krajská knižnica Žilina (n.d.). Smart Senior Academies. <https://www.krajskakniznicazilina.sk/>
28. Ministerio de Educación y Formación Profesional, Spain (n.d.). Aula Mentor. <https://www.aulamentor.es>
29. Ministry of Investments, Regional Development and Informatization of the Slovak Republic – MIRRI (n.d.). Digitálni seniори Programme. <https://www.digitalniseniori.gov.sk>
30. Ministry of Labour and Social Policies, Italy (n.d.). GOL Programme. <https://www.lavoro.gov.it/temi-e-priorita/occupazione/focus/pagine/programma-gol>
31. National Cybersecurity Agency – ACN, Italy (n.d.). National Cybersecurity Strategy 2022–2026. <https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza>
32. National Security Authority – NBÚ, Slovak Republic (2021). National Cybersecurity Strategy 2021–2025. <https://www.nbu.gov.sk/national-cybersecurity-strategy-of-the-slovak-republic-for-years-2021-2025/>
33. OECD (2024). Enhancing the Digital Skills of Seniors in the Slovak Republic. <https://www.oecd.org/en/about/programmes/dg-reform/enhancing-the-digital-skills-of-seniors-in-the-slovak-republic.html>
34. Policía Nacional, Spain (n.d.). Plan Mayor Seguridad. https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
35. Polizia Postale, Italy (n.d.). Annual Cybersecurity Reports and Data. <https://www.commissariatodips.it>
36. Repubblica Digitale (2025). Quarto rapporto di monitoraggio – Ottobre 2025. Department for Digital Transformation, Italy.
37. SafeHorizon Project (2026). Spain's Situation in the Cyberspace Domain. <https://www.project-safehorizon.eu>
38. Slovak Republic (2018). Act No. 18/2018 Coll. on the Protection of Personal Data. National Council of the Slovak Republic.

39. Slovak Republic (2018). Act No. 69/2018 Coll. on Cybersecurity. <https://www.sk-cert.sk>
40. Slovak Republic (2024). Act No. 366/2024 Coll. – Transposition of the NIS2 Directive. National Council of the Slovak Republic.
41. Slovak Telekom Endowment Fund (n.d.). Zrelí na dobu digitálnu. <https://nadacnyfondtelekom.sk/>
42. Union of Pensioners in Slovakia – JDS (n.d.). <https://www.jednotadochodcov.sk/>