YBER.EU.VET

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

CYBER.EU.VET

KA226 – Partnerships for Digital Education Readiness

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

Informe del Consorcio

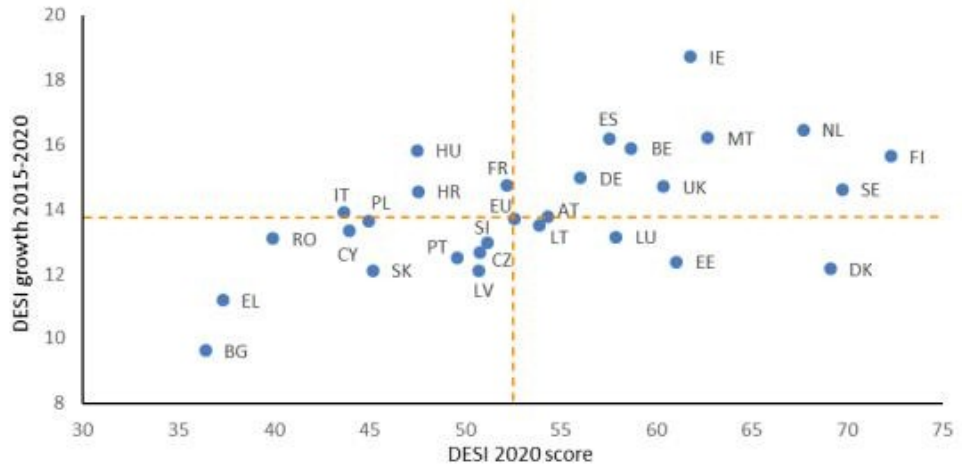
sobre los principales retos de la ciberseguridad y las mejores prácticas

Índice de Contenidos

Introducción

Dado que el mundo está cada vez más digitalizado, se ha hecho más evidente que la práctica debe combinarse con la política actual. En el contexto europeo se presta mucha atención a las políticas de alfabetización digital y de ciberseguridad, pero hay menos ejemplos de iniciativas que se considere que cumplen estos objetivos en consonancia con las políticas desarrolladas. Para observar detenidamente hasta qué punto las competencias digitales y de ciberseguridad son un tema central y divergente, resulta útil considerar el Índice de la Economía y la Sociedad Digitales (DESI) de 2020.

Como parte de su panorama general, el DESI supervisa el rendimiento digital general de Europa y mide el nivel de competitividad digital de los países de la UE. Al proporcionar información sobre la situación de la digitalización en cada Estado miembro, ayuda a determinar los ámbitos en los que hay que invertir y adoptar nuevas medidas. Hacia un futuro digital adaptado a las necesidades de las personas y respetuoso con los valores fundamentales de la UE, la Comisión presentó en febrero de 2020 una visión de la transformación digital "Modelar el futuro digital de Europa". El informe DESI 2020 evalúa la economía y la sociedad digitales al comienzo de la pandemia utilizando datos de 2019.



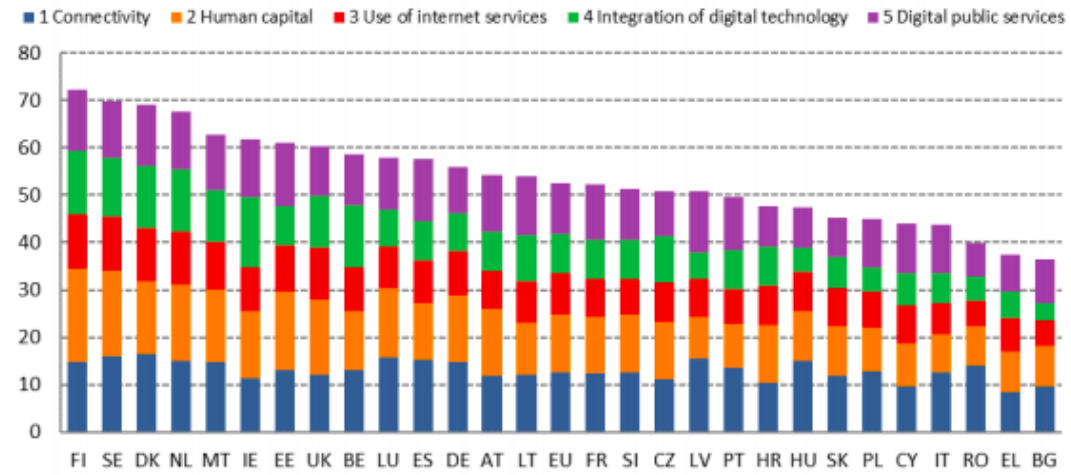
Source: DESI 2020, European Commission.

En concreto, este índice investiga y recopila datos sobre:

- Conectividad: La disponibilidad de un acceso rápido y fiable a Internet (incluidas conexiones fijas y móviles) es vital en la era actual de prestación en línea de servicios sociales y económicos clave;
- Capital humano: La columna vertebral de la sociedad digital son las competencias digitales de sus ciudadanos. Los usuarios de servicios digitales y las personas con movilidad limitada pueden realizar actividades básicas en línea a través de estos dispositivos;
- Uso de Internet: A medida que avanzaba la pandemia, cada vez más personas utilizaban Internet. El confinamiento generalizado dio lugar a un acceso regular a los medios sociales y las plataformas de entretenimiento, así como a los servicios de teletrabajo y comercio electrónico;
- Integración de la tecnología digital: Las empresas adoptaron rápidamente nuevas modalidades de trabajo para adaptarse a las medidas gubernamentales que reducían la interacción social;

- En medio de las medidas de distanciamiento social, es necesario continuar las actividades gubernamentales para garantizar que los servicios públicos digitales aporten beneficios. Harán falta servicios públicos digitales sólidos en todos los Estados miembros para lograr una estrategia de salida exitosa de la pandemia actual.

Este análisis resulta útil al considerar el consorcio de socios cuyos países miembros se diferencian en gran medida en cuanto a resultados en materia de seguridad digital y cibernética. De hecho, tres de ellos (por orden de clasificación, Irlanda, España y Alemania) obtienen una puntuación mejor que la media de la UE, mientras que los otros cuatro (Francia, Letonia, Portugal e Italia) obtienen resultados inferiores.



Source: DESI 2020, European Commission.

Es importante subrayar que los resultados del DESI 2020 no parecen confirmar una correspondencia lineal entre el PIB del país y la difusión de las competencias digitales. De hecho, España, por ejemplo, clasificada como la 5ª economía de la UE sólo ocupa el 10º lugar en el Índice de Economía y Sociedad Digitales. Recientemente se han introducido varias iniciativas en algunos de los países que integran el consorcio para mejorar la digitalización de la economía y la sociedad. Como país líder de la UE en preparación para el 5G, Alemania ha tomado varias

medidas para avanzar en la digitalización, incluidas iniciativas en las áreas de seguridad informática, supercomputación, IA y blockchain. En Francia se han realizado numerosos esfuerzos para facilitar la digitalización de las empresas y los servicios públicos, incluidos esfuerzos para crear un ecosistema de apoyo a las empresas tecnológicas de nueva creación. El Gobierno italiano adoptó "Italia 2025" en diciembre de 2020, un plan quinquenal que sitúa la innovación y la digitalización en el centro de un "proceso de transformación radical y estructural del país". En los próximos años, estas iniciativas -que requieren una aplicación sostenida en el tiempo y también es probable que requieran inversiones- podrían traducirse en el avance de estos Estados miembros en el DESI.

Otro aspecto significativo a la hora de considerar el nivel de competencias digitales y de ciberseguridad se refiere al impacto de la pandemia COVID-19 en relación con estos temas. Aunque tal relación entre la emergencia sanitaria y el número de ciberataques no está inmediatamente clara para la mayoría del público en general, en realidad, la primera ha dado lugar a un aumento de los segundos Los ciberdelincuentes son muy flexibles a la hora de explotar nuevos acontecimientos, como hemos visto con la reciente emergencia sanitaria. Con la adopción de nuevas estrategias digitales en 2020 (por ejemplo, el trabajo a distancia), muchas empresas se han abierto inadvertidamente a una serie de nuevos vectores de ataque que los delincuentes no han tardado en explotar. Entre otros, el imprevisto de COVID-19 se utilizó para propagar intentos de malware: por ejemplo, correos electrónicos en nombre de la Organización Mundial de la Salud, indicando que el archivo adjunto incluye la información más reciente sobre la pandemia; enlaces a gráficos que muestran la propagación del virus, cuya funcionalidad era robar datos de los usuarios; correos electrónicos maliciosos a instituciones sanitarias en relación con la entrega de equipos de protección contra COVID-19 y muchos otros.

Para completar este Informe de Investigación del Consorcio, utilizamos la investigación documental, que consistió en localizar y recopilar datos, publicaciones, informes de la UE,

legislaciones nacionales y europeas siguiendo las referencias proporcionadas a lo largo del informe. En concreto, el estudio exploró la cuestión de la alfabetización digital y la ciberseguridad en los diferentes contextos nacionales, centrándose en la formación del profesorado de EFP. Además, este informe de investigación del consorcio destaca algunos de los actores clave que participan en el sector de la ciberseguridad, incluidos los organismos nacionales y la Agencia de la Unión Europea para la Ciberseguridad (ENISA), que coopera con los Estados miembros y los organismos de la UE, y ayuda a Europa a prepararse para futuros retos cibernéticos.

1. Investigación documental sobre las competencias digitales de los educadores de EFP.

Alemania:

- El Informe de Datos de FP (2019) elaborado por el Instituto Federal Alemán de Formación Profesional (BIBB), incluyó la "digitalización" entre las 3 tendencias clave para las ocupaciones de formación profesional y la FP en general.
- Más concretamente, el informe afirmaba que "la digitalización va a reforzar los cambios estructurales del mercado laboral", lo que conduce a la necesidad de un cambio en las capacidades de formación dentro de los respectivos campos. En consecuencia, en el futuro, el mercado laboral alemán y europeo tendrá una necesidad especial de especialistas profesionales altamente cualificados.
- Como se señala en la Resolución de la Conferencia Permanente de Ministros de Educación y Asuntos Culturales (2016-2017) - "Bildung in der digitalen Welt" (Educación en el mundo digital)- en el ámbito de la formación profesional, el fomento de las

competencias relacionadas con el trabajo en el contexto de los procesos digitales de trabajo y empresariales es una parte esencial de la competencia de los profesores como punto de partida de sus actividades didácticas.

- El Ministerio Federal de Educación e Investigación (BMBF) y el Instituto Federal de Formación Profesional (BIBB) abordan desde 2015 cuestiones de investigación, desarrollo y práctica, relacionadas con la transformación digital del mundo laboral y la formación profesional.

Irlanda:

- Una de las estrategias clave de Irlanda en relación con las competencias digitales de los educadores de EFP es la Estrategia Digital Nacional, que se puso en marcha en julio de 2013.
- La estrategia se centra en el compromiso digital y destaca cómo Irlanda puede beneficiarse de una sociedad digitalmente comprometida.
- La estrategia establece una visión clara para el avance digital de Irlanda a través de la implementación de una serie de acciones prácticas para ayudar a aumentar el número de ciudadanos y empresas que participan en línea a través de la industria y la empresa, la formación ciudadana, las escuelas y la educación.
- En cuanto a las competencias digitales de los educadores de EFP, los datos siguen poniendo de manifiesto que existe una brecha cada vez mayor entre los educadores que utilizan dispositivos digitales en sus clases como herramienta de aprendizaje y los que no.
- Muchos educadores han declarado que creen que los dispositivos digitales pueden "provocar distracciones" entre los alumnos. Sin embargo, por el contrario, muchos educadores creen que los dispositivos digitales y las aplicaciones en las actividades de

aprendizaje pueden capacitar a los alumnos y ayudarles a adquirir habilidades para la vida en el siglo XXI, como pagar facturas en línea o solicitar empleo.

Portugal:

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

Italia:

- En el ámbito de la educación, las acciones se llevaron a cabo principalmente a través de la aplicación del Plan Nacional de Escuela Digital (Piano Nazionale Scuola Digitale- PNSD).
- Se trata del documento guía del Ministerio de Educación, Universidad e Investigación para el lanzamiento de una estrategia global de innovación para la escuela italiana y para un nuevo posicionamiento de su sistema educativo en la era digital.
- La mayoría de las acciones para la formación del personal escolar se han dirigido a las escuelas primarias y secundarias, que representan la mayoría de las escuelas en Italia, mientras que se ha prestado escasa atención al sector de la Educación y Formación Profesional (EFP).

- En este sentido, se han puesto en marcha proyectos para la educación técnica postsecundaria y los institutos de formación profesional (Istituti Tecnici Superiori - ITS) con un enfoque particular en el fortalecimiento de las habilidades de los estudiantes.
- Por ejemplo, en 2019, el proyecto "ITS 4.0" involucró a más de 1.170 estudiantes de ITS y alrededor de 130 empresas asociadas en 106 proyectos de innovación tecnológica centrados en tecnologías como la impresión 3D, la realidad virtual y el big data.

España:

- La Agenda Digital para España (ADpE, Agenda Digital para España) publicada en 2013, es la hoja de ruta para el cumplimiento de los objetivos marcados por la Agenda Digital para Europa en 2015 y 2020, así como la consecución de objetivos específicos para el desarrollo de la economía y la sociedad digital en España. Se estructura en torno a seis grandes objetivos y varios planes específicos. El sexto objetivo trata sobre el fomento de la inclusión y alfabetización digital y la formación de nuevos profesionales TIC. Entre sus medidas específicas cabe destacar, a efectos de este análisis, las siguientes:
    - actualizar el Catálogo Nacional de Cualificaciones Profesionales en materia de competencias y formación en TIC, e incluir esta actualización en las ofertas formativas acreditativas de las cualificaciones profesionales;maximizar la eficiencia en la gestión y asignación de fondos de formación para la formación continua en TIC, tanto para trabajadores del sector privado como del sector público, con especial atención al uso de plataformas de formación virtual online;
    - destinar parte de los recursos disponibles para la formación profesional continua a la adquisición y mejora de las competencias digitales de los profesionales de las TIC;
    - reajustar la formación profesional relacionada con las TIC incluyendo, entre otras acciones, cursos de especialización en el ámbito educativo;

- promover una mejora de la oferta universitaria dirigida a la formación de profesionales de las TIC mediante su adaptación a las necesidades del mercado, contemplando nuevos perfiles profesionales en el ámbito de las TIC y aumentando la eficiencia del sistema.

Francia:

- Si observamos el ritmo de la formación sobre el uso de las TIC en las universidades francesas que la imparten, vemos que no existen políticas claras y sostenidas de formación de formadores en el uso de las TIC/E. Alrededor del 58% señala que sólo se imparte una sesión de formación al año, frente a un 7,4% al mes y un 0,5% a la semana.
- La Agencia Nacional Francesa de Seguridad de los Sistemas de Información (ANSSI) ha constatado un aumento muy rápido del nivel de la ciberamenaza en Francia. Continuando una trayectoria iniciada en 2019, el número de ciberataques se ha disparado: el número de víctimas se ha multiplicado así por 4 en un año.
- Las estadísticas muestran que la densidad de la formación informática varía de una región francófona a otra. Esto se debe a varias razones, las más importantes de las cuales están sin duda relacionadas con las instituciones académicas y sus gobiernos.
- Las oficinas regionales o los CNF podrían realizar más adelante otros estudios para ver las diferencias, en función de sus propias políticas locales o regionales de educación digital.

Letonia:

- Aunque actualmente en Letonia faltan estudios de investigación y datos sobre ciberseguridad y otras competencias digitales de los educadores de EFP y otros centros educativos, es obvio que la transición a la enseñanza a distancia, debido a las crisis covid-19, resultó ser un reto importante para muchos profesores.

- En cuanto a las estrategias nacionales, los documentos de planificación del nuevo periodo presupuestario (2021-2027) destacan los siguientes aspectos:
    - El desarrollo de las competencias digitales en el sector educativo (Directrices de Transformación Digital 2021- 2027) - prevé el desarrollo de las competencias digitales de los educadores y directores de centros educativos, el desarrollo y uso de las competencias digitales en el proceso educativo, así como el apoyo al desarrollo de las competencias digitales de los adultos empleados;
    - El desarrollo de las competencias digitales está incluido en el programa de desarrollo de las competencias profesionales de los educadores (Directrices de Desarrollo de la Educación 2021- 2027). En 2020, el Ministerio de Educación y Ciencia de la República de Letonia ha establecido la mejora de la competencia digital de los educadores como objetivo prioritario de la competencia profesional, asignando para ello financiación adicional (0,5 millones de euros);
    - La necesidad de concienciar a alumnos y educadores sobre la seguridad de la información, la protección de la privacidad y el uso de servicios electrónicos fiables (Estrategia de Ciberseguridad 2019-2022, área de actuación "Concienciación pública, educación e investigación");
    - El desarrollo de las competencias digitales de la sociedad en general (Directrices de Desarrollo de la Educación 2021-2027, Directrices de Transformación Digital 2021-2027), ya que las competencias digitales se equiparan ahora con la alfabetización y la aritmética en términos de su importancia y, al menos en el nivel básico, son necesarias para todos, independientemente del área de actividad (competencias digitales = competencias transversales). Deben tomarse medidas para educar a la población en las competencias digitales básicas, la

alfabetización mediática y la alfabetización informacional, que incluye todo el conjunto de competencias básicas, incluidas las cibercompetencias;

La atención que se ha prestado al mencionado índice DESI en la introducción de este informe de investigación se justifica por la precisión con la que describe el estado de la cuestión y el carácter divergente según los distintos países europeos. Dicha precisión también se ve confirmada por los informes nacionales individuales relativos a las competencias digitales de los educadores de EFP.

Creemos que es especialmente beneficioso comparar los dos extremos del consorcio, con el fin de comprender cómo afectan los diferentes grados en competencias digitales a la población nacional, y a los educadores de EFP en concreto. Consideraremos en primer lugar el caso de Irlanda, que ocupa el 6º lugar en la clasificación DESI.

Según la Oficina Central de Estadística de Irlanda (CSO), en 2018, el 89% de los hogares tienen acceso a Internet en casa. Además, más del 30% de todos los datos de la UE se alojan en Irlanda, ya que muchas de las mayores empresas tecnológicas del mundo tienen su sede en Europa. Cuando se juntan ambas estadísticas, no hace falta decir que garantizar que Irlanda sea un país preparado para la ciberseguridad es de vital importancia. A lo largo de este informe nacional, se hará referencia a la legislación clave que existe en Irlanda en relación tanto con la alfabetización digital como con la

ciberseguridad. A medida que el mundo sigue adaptándose a "vivir con COVID-19", es necesario garantizar que el panorama de la lucha contra la ciberdelincuencia y los modelos de mejores prácticas sigan influyendo en la política y la práctica.

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

comprometida. La estrategia establece una visión clara para el avance digital de Irlanda a través de la aplicación de una serie de acciones prácticas para ayudar a aumentar el número de ciudadanos y empresas que participan en línea a través de la industria y la empresa, la formación de los ciudadanos, las escuelas y la educación. En 2021, la Ministra de Educación, Norma Foley, anunció el desarrollo de una nueva Estrategia Digital para las escuelas de primaria. La estrategia se centrará principalmente en el uso de la tecnología digital en la educación y mejorará el aprendizaje mediante la integración de la tecnología en el futuro. En el ámbito de la educación superior en Irlanda, uno de los avances más notables es la Hoja de ruta para el aprendizaje digital en la educación superior: 2015 - 2017, que se elaboró para apoyar un "enfoque coordinado y multinivel para fomentar la alfabetización digital, las habilidades y la confianza entre los estudiantes de todos los niveles educativos".

En cuanto a la educación y formación continua, se creó un Departamento de Educación Superior y Continua, Investigación, Innovación y Ciencia relativamente nuevo. Dentro de la estrategia trienal del departamento, un área clave de atención es la relativa a las competencias digitales, con la que pretenden aplicar una nueva estrategia a diez años para mejorar la alfabetización, la aritmética y las competencias digitales. Además, se centran en reformar la formación profesional e invertir en la promoción de las competencias digitales. En cuanto a las competencias digitales de los educadores de EFP, los datos siguen poniendo de manifiesto que existe una brecha cada vez mayor entre los educadores que utilizan dispositivos digitales en sus clases como herramienta de aprendizaje y los que no lo hacen.

Muchos educadores han declarado que creen que los dispositivos digitales pueden "provocar distracciones" entre los alumnos. Sin embargo, por el contrario, muchos educadores creen que los dispositivos digitales y las aplicaciones en las actividades de aprendizaje pueden empoderar a los alumnos y ayudarles a adquirir habilidades para la vida del siglo XXI, como pagar facturas en línea o solicitar empleo. Una última estrategia intergubernamental que merece la pena

destacar desde una perspectiva irlandesa es la Iniciativa Future Jobs Ireland de 2018, que hace hincapié en una filosofía de aprendizaje permanente. Dentro de sus cinco temas clave, el segundo se centra en "la innovación y la tecnología, incluida la preparación para la transición a la economía digital". La estrategia es fundamental para los debates sobre la necesidad de más investigación e inversión en el ámbito de la alfabetización digital.

Esta comprensión y apreciación compartidas de los medios digitales confirman a Irlanda como un país líder en términos de integración de la tecnología digital. Entre otros, dicha integración resulta ser uno de los principales problemas para el contexto italiano.
En Italia, menos de la mitad de la población tiene competencias digitales básicas y el porcentaje de especialistas en TIC, que constituye sólo el 1% de los licenciados italianos, sigue estando por debajo de la media de la UE, aunque ha aumentado en los últimos años. Además, los datos de la Encuesta Internacional sobre Enseñanza y Aprendizaje de la OCDE (2013) sitúan a Italia en el primer lugar en cuanto a las necesidades de formación en TIC de sus profesores. Al menos el 36% de los profesores italianos declararon no estar suficientemente preparados para la enseñanza digital, frente a una media de la OCDE del 17%, lo que demuestra que es necesaria una formación específica.

En los últimos años, en términos de respuesta política, Italia ha incorporado medidas sobre competencias digitales en varias estrategias sectoriales. En el ámbito de la educación, las acciones se llevaron a cabo principalmente a través de la aplicación del Plan Nacional de Escuela Digital (Piano Nazionale Scuola Digitale - PNSD), que es el documento directriz del Ministerio de Educación, Universidad e Investigación para la puesta en marcha de una estrategia global de innovación para la escuela italiana y para un nuevo posicionamiento de su sistema educativo en la era digital. Es un pilar fundamental de La Buona Scuola (ley 107/2015), una visión operativa que refleja la posición del Gobierno respecto a los retos de innovación más importantes del sistema público y, en el centro de esta visión, están la innovación del sistema escolar y las

oportunidades de la educación digital. Las áreas de intervención identificadas por el PNSD son: acceso, espacios y entornos de aprendizaje, administración digital, identidad digital, competencias de los estudiantes, emprendimiento y mercado laboral, contenidos digitales, formación del personal. Respecto a este último punto, el PNSD defiende que la formación del profesorado debe centrarse en la innovación educativa, teniendo en cuenta las tecnologías digitales como soporte para la implantación de nuevos paradigmas educativos y la planificación operativa de las actividades. Los objetivos de esta acción son:

- Reforzar la preparación del personal en el ámbito de las competencias digitales, llegando a toda la comunidad escolar;
- Promover el vínculo entre la innovación educativa y las tecnologías digitales;
- Desarrollar estándares eficaces, sostenibles y continuos en el tiempo para la formación en innovación educativa;
- Reforzar la formación en innovación educativa a todos los niveles (inicial, entrante, en servicio).

Con el fin de fomentar la formación del profesorado en temas informáticos, se firmó un Memorando de Entendimiento con organismos de formación y se proporcionaron recursos financieros para facilitar la participación en los cursos, tales como:

- Memorando de Entendimiento no. 785 de 22 de enero de 2021 entre el Ministerio de Educación y Cisco "Innovación y mejora de las competencias digitales en la escuela" y programa de formación "Profesores conectados y seguros".
- Memorando de Entendimiento no. 4 de 28 de octubre de 2020 entre el Ministerio de Educación y S.O.S. El Telefono Azzurro Onlus para la realización de actividades conjuntas de educación y formación para promover la educación para la ciudadanía digital y el uso consciente de las tecnologías digitales, medios de comunicación social y cursos de formación para profesores..

Hasta ahora, la mayoría de las acciones para la formación del personal escolar se han dirigido a las escuelas primarias y secundarias, que representan la mayoría de las escuelas en Italia, mientras que se ha prestado poca atención al sector de la Educación y Formación Profesional (EFP). En este sentido, se han puesto en marcha proyectos para la educación técnica postsecundaria y los institutos de formación profesional (Istituti Tecnici Superiori - ITS) con un enfoque particular en el fortalecimiento de las habilidades de los estudiantes. Por ejemplo, en 2019, el proyecto "ITS 4.0" contó con la participación de más de 1.170 estudiantes de ITS y unas 130 empresas asociadas en 106 proyectos de innovación tecnológica centrados en tecnologías como la impresión 3D, la realidad virtual y el big data.

Otra herramienta que contribuirá a la adquisición de competencias digitales está incluida en el Plan Nacional de Recuperación y Resiliencia (Piano Nazionale di Ripresa e Resilienza - PNRR), que forma parte del programa de la UE Next Generation, un paquete de 750.000 millones de euros, de los que casi la mitad están constituidos por subvenciones, acordado por la Unión Europea en respuesta a la crisis pandémica. El PNRR promoverá el desarrollo de las competencias digitales del personal escolar para fomentar un enfoque accesible, inclusivo e inteligente de la educación digital. El objetivo principal es la creación de un ecosistema de competencias digitales, capaz de acelerar la transformación digital de la organización escolar y de los procesos de aprendizaje y enseñanza, en línea con el marco de referencia europeo de competencias digitales DigComp 2.1 (para alumnos) y DigCompEdu (para profesores). La aplicación de esta línea de actuación corre a cargo del Ministerio de Educación e implicará a unas 650.000 personas, incluidos profesores y personal escolar, y a más de 8.000 centros educativos. El Gobierno tiene la intención de reforzar la formación profesional, en particular el sistema de formación profesional terciaria (ITS) y la educación STEM, dando una gran prioridad a la igualdad de género.

Los contextos mencionados representan dos contextos nacionales diferentes. Para tener una indicación más cercana al marco general europeo, puede ser útil analizar el panorama de las competencias digitales en Francia, un país que en la escala DESI está muy cerca e inmediatamente después de la media europea.

La Agencia Nacional de Seguridad de los Sistemas de Información (ANSSI) ha constatado un aumento muy rápido del nivel de la ciberamenaza en Francia. Continuando una trayectoria iniciada en 2019, el número de ciberataques se ha disparado: el número de víctimas se ha multiplicado así por 4 en un año. Esto es particularmente preocupante, especialmente en un contexto en el que cualquier ciberataque es probable que tenga un impacto exacerbado debido a la crisis sanitaria. La falta de concienciación sobre los riesgos cibernéticos, la falta de control sobre los sistemas de información, el incumplimiento de las medidas de higiene informática, la escasez de expertos en ciberseguridad y, en cierta medida, el aumento de la superficie de ataque debido al uso generalizado del teletrabajo, son debilidades explotadas por los ciberdelincuentes. Las campañas de ataques que afectaron a Francia en 2020 lograron perturbar a muchas empresas y causaron importantes pérdidas financieras. El uso masivo de servicios digitales externalizados, a menudo menos seguros, es una práctica generalizada que los atacantes no dejan de explotar. Las estadísticas muestran que la densidad de la formación informática varía de una región francófona a otra. Esto se debe a varias razones. Entre ellas, la más significativa está sin duda relacionada con las instituciones académicas y sus gobiernos. Las oficinas regionales o los CNF podrían realizar más adelante otros estudios para ver las diferencias, en función de sus propias políticas locales o regionales de educación digital. Las estadísticas de formación muestran que las necesidades temáticas que han sido objeto de talleres de formación también varían de una región a otra. La frecuencia temática en este sentido también depende de factores endógenos relacionados con la demanda y la oferta en función de las necesidades y los niveles de avance en los ámbitos de las TIC/E y la EAD de los socios locales.

2. Investigación documental sobre los principales problemas de seguridad digital en los países socios

Alemania:

- Para analizar el contexto específico alemán y extraer un análisis de necesidades, es especialmente significativo el examen del Barómetro Digital 2020, una encuesta en línea representativa de ciudadanos particulares sobre ciberseguridad, realizada conjuntamente por la BSI y la Comisión de Prevención del Delito de la Policía Estatal y Federal alemana.
- En los últimos años, en el panorama alemán y europeo, la ciberdelincuencia ha sido la principal causa de los recientes ciberataques. El informe de la BSI de 2020 confirmó las filtraciones de datos y las vulnerabilidades críticas detectadas en productos de software y hardware. Esta investigación también ha observado un aumento de los ciberdelitos masivos dirigidos a ciudadanos particulares, empresas comerciales y otras instituciones que utilizan programas maliciosos.
- La vulnerabilidad más común explotada por el malware es una vulnerabilidad en el sistema anfitrión. En el caso de los productos de software o hardware, las vulnerabilidades pueden encontrarse en las pasarelas, como las que operan entre oficinas o redes de producción, o pueden deberse a errores humanos de ingeniería social.
- Este grado de digitalización no está exento de riesgos y peligros. Uno de cada cuatro encuestados declaró haber sido víctima de ciberdelincuencia en el último año. La tasa global de ciberdelincuencia en 2020 se mantiene constante. Las compras en línea y el acceso de terceros a cuentas en línea son los tipos de fraude más comunes que afectan a las víctimas (44%) y (30%), respectivamente.

A pesar de los resultados, dos tercios de los encuestados expresaron su deseo de recibir más información sobre la prevención del robo de datos (66%). El asesoramiento más solicitado consiste en consejos prácticos, como la forma de garantizar contraseñas seguras para varias cuentas en línea (59 %), seguido de consejos sobre el software más adecuado para proteger las cuentas en línea (52 %) y consejos sobre los pros y los contras de los gestores de contraseñas (49 %).

Irlanda:

- Las amenazas a la ciberseguridad en Irlanda siguen aumentando, y el ataque más reciente tuvo lugar en 2021 contra el Health Service Executive (HSE) de Irlanda, que ha tenido y sigue teniendo efectos devastadores en el sistema sanitario irlandés.
- Irlanda alberga más del 30% de los datos de la UE debido al número de centros de ciberseguridad con sede en el país. Aunque esto ofrece muchas oportunidades, también se traduce en un mayor nivel de amenaza de ciberdelincuencia. Como Irlanda es una democracia liberal abierta, se considera especialmente vulnerable a los llamados ataques del tipo "hackear y filtrar".
- La segunda Estrategia Nacional de Ciberseguridad 2019 - 2024 de Irlanda se puso en marcha en un intento de aumentar la preparación del país en materia de ciberseguridad. Los objetivos clave de la estrategia son:
    - Garantizar la preparación de Irlanda en materia de ciberseguridad y responder y gestionar los incidentes de ciberseguridad, incluidos los relativos a la seguridad nacional,
    - Proteger y gestionar cualquier interrupción de los servicios relacionados con infraestructuras nacionales críticas derivada de ciberataques,
    - Seguir creciendo y desarrollando el sector de la ciberseguridad en Irlanda y estar preparados para la ciberseguridad,

- Implantar en las empresas irlandesas las mejores tecnologías y medidas disponibles a nivel internacional,
- Aumentar la concienciación y desarrollar las capacidades de las organizaciones y los particulares en materia de ciberseguridad.

- En 2018 se puso en marcha un Plan de Acción para la Seguridad en Línea que contiene veinticinco acciones bajo cinco objetivos principales centrados en legislar las infracciones penales relativas a la ciberdelincuencia, eliminar el material ilegal y dañino e impulsar la seguridad en línea.

Portugal:

- Los principales temas de seguridad digital que hay que garantizar son:
  - Nivel básico
    - Identificar la exposición de su infraestructura y aplicaciones escolares en el entorno en línea y adoptar medidas de mitigación de riesgos (tanto estructurales como de comportamiento);
    - Identificar y mitigar las vulnerabilidades;
    - Identificar información personal en internet que pueda ser utilizada en un ataque;
    - Adquirir un conjunto de comportamientos adecuados en el uso del ciberespacio;
  - Niveles intermedio y avanzado:
    - Entornos técnicos de programación de seguridad
    - Ingeniería social
    - Exploración de fuentes de datos abiertas
    - Redes inalámbricas
    - Cifrado y contraseñas

Italia:

- El problema de seguridad más extendido en los últimos tres años en Italia es el phishing de contraseñas, señalado por el 48% de los directivos italianos, frente al 36% de los europeos. Además, el 28% de los directivos italianos tiene problemas relacionados con el acceso y la identidad (en línea con el porcentaje europeo), seguido del problema del malware basado en ingeniería social (24%).
- Además, sólo el 42% de las personas de entre 16 y 74 años tiene competencias digitales básicas y el porcentaje de licenciados en informática y TIC es muy bajo en comparación con los datos europeos.
- El Gobierno aborda las competencias digitales en "Italia 2025", una estrategia quinquenal de innovación y digitalización lanzada en 2019. En particular, la estrategia incluye "República Digital", una iniciativa promovida y coordinada por el Ministerio de Innovación Tecnológica y Digitalización.
- La iniciativa pretende crear una alianza entre las organizaciones públicas y privadas y los ciudadanos, e invitarles a emprender acciones concretas para promover las competencias digitales. Se centra en tres líneas de actuación:
    - impulsar las competencias digitales básicas
    - Promover la mejora y el reciclaje de la mano de obra;
    - desarrollar las competencias en TIC y tecnologías emergentes.
- Se dará un paso más con "Italia digitale 2026", que establece cinco ambiciosos objetivos que deberán alcanzarse en los próximos años:
    - Difundir la identidad digital, garantizando que sea utilizada por el 70% de la población;
    - Superar la brecha de competencias digitales, con al menos un 70% de la población digitalmente

- Lograr que cerca del 75% de las AP italianas utilicen servicios en la nube;
- Alcanzar al menos el 80% de los servicios públicos esenciales prestados en línea;
- Alcanzar, en colaboración con el Mise, el 100% de las familias y empresas italianas con redes de ultra banda ancha.

España:

- La Estrategia Española de Activación para el Empleo 2017-20 tiene como objetivo consolidar la recuperación económica mediante el impulso de Programas y Recursos de Ciberseguridad para que los Centros de FP puedan hacer frente a los retos del mercado laboral presente y futuro derivados de la globalización y la digitalización. Establece las medidas a llevar a cabo, tanto a nivel estatal como autonómico, por los Servicios Públicos de Empleo (SPE);
- En términos cuantitativos, uno de los objetivos es la formación en competencias digitales de al menos 225.000 jóvenes: el 75% en competencias básicas y el 25% en competencias digitales avanzadas, lo que representa el 40% y el 38% respectivamente de la población joven menor de 30 años.
    - apoyo a la puesta en marcha de proyectos de base tecnológica para mujeres jóvenes, facilitando un consultor que asesore a estas emprendedoras sobre su plan de negocio y ofreciendo servicios de seguimiento;
    - acciones formativas específicas para mujeres jóvenes de zonas rurales en tecnologías TIC y nuevos sectores de futuro, aprovechando las posibilidades de las nuevas tecnologías y con formadores y tutores, incluyendo la enseñanza online;

- promoción del emprendimiento, el autoempleo y las nuevas oportunidades laborales que ofrece la economía digital y las diferentes fórmulas de economía social y economía de plataformas digitales, dentro de las políticas de activación del empleo;
- mejora de la visibilidad de las mejores prácticas desarrolladas para comprender cuáles son los principales temas de seguridad digital.

- Programa Operativo Nacional de Empleo Juvenil (presupuesto 39 millones de euros). Como ejemplo, el Programa incluye un itinerario de Formación en Transformación Digital para el empleo.
- El proyecto, ejecutado por la EOI con la colaboración de Google, tiene como objetivo mejorar la empleabilidad de los jóvenes que han abandonado los estudios a una edad temprana, han perdido su empleo o tienen dificultades para encontrar su primer trabajo.

Francia:

- Los ministros de Educación Superior del espacio francófono se reunieron el 5 de junio de 2015 en París por iniciativa conjunta de Francia, la OIF (Organisation internationale de la francophonie) y la AUF (Agence universitaire de la francophonie) para examinar el estado y las perspectivas de desarrollo digital del espacio francófono universitario y de FP.
- El principal objetivo de este trabajo era contribuir a la elaboración de una estrategia francófona de formación de formadores en el ámbito de la educación digital y evaluar las necesidades y expectativas de formación de los grupos destinatarios afectados, para después determinar qué se necesita para satisfacer dichas necesidades y expectativas, sobre todo en términos de servicios, contenidos y competencias.
- Según el estudio "Étude sur l'identification des besoins en formation tic/e dans les pays francophones du sud, 2016", Las necesidades de los docentes-investigadores están

fuertemente marcadas por una tendencia unánime hacia la formación en TIC/E y el desarrollo de capacidades relacionadas con la educación digital (80,4%).

- Los riesgos digitales están muy presentes en las representaciones de los jóvenes profesores, que retransmiten fácilmente el discurso mediático. Los tres riesgos que los profesores consideran que afrontan más personalmente son técnicos (66,20%), éticos y jurídicos (55,80%) e informativos (54,70%).

Letonia:

- Según la Estrategia nacional de ciberseguridad 2019-202215, el ciberespacio de Letonia sigue enfrentándose a amenazas a gran escala: phishing, extorsión y malware, intentos de piratear los sistemas, redes y sitios web, ataques de denegación de servicio (DoS) en sistemas de información críticos, así como correo electrónico fraudulento y campañas de ingeniería social para recuperar datos personales o de autenticación para desacreditar a una persona, empresa o institución específica o para cometer delitos.
- - Tanto en Europa como en Letonia, cobraron actualidad los siguientes incidentes: intentos de extorsión monetaria dirigidos principalmente a instituciones financieras o empresas del sector privado (los atacantes realizaron una serie de ataques de prueba, amenazando con suspender el funcionamiento de los sitios web de las empresas u otros recursos mediante ataques de hasta 2 Tb/s).
- En el año 2021, el fraude, el malware y las vulnerabilidades siguen activos - cuentas de WhatsApp robadas a través de códigos de activación que solicitan las cuentas hackeadas de la lista de contactos de la persona; una nueva ola de correos electrónicos de chantaje (sextorsión) - amenazan con distribuir material comprometedor, si el usuario del correo electrónico no hará un rescate.

- El año 2020, con sus cambios globales, ha demostrado que para los educadores de EFP y otras instituciones educativas es importante tener más conocimientos y habilidades sobre el trabajo a distancia seguro cuando se organizan clases en línea y se utilizan herramientas digitales (correos electrónicos, WhatsApp, plataformas de aprendizaje, etc.), así como ser conscientes de las estafas y fraudes de actualidad, especialmente en las redes sociales, para concienciar a sus alumnos y estudiantes.

Aunque la relación entre la pandemia de COVID-19 y el número de ciberataques no está inmediatamente clara para el público más general, en realidad, la primera ha provocado un aumento de los segundos. Los ciberdelincuentes son muy flexibles a la hora de explotar nuevos acontecimientos, como hemos visto con la reciente emergencia sanitaria. Con tantas empresas que este año han adoptado nuevas estrategias digitales (por ejemplo, el trabajo a distancia), se han abierto inadvertidamente a una serie de nuevos vectores de ataque que los delincuentes no han tardado en explotar.

Las oficinas nacionales ofrecen una perspectiva polifacética de los principales problemas digitales y de ciberseguridad. A medida que el aprendizaje a distancia se convierte en la nueva normalidad, los ciberdelincuentes están encontrando nuevas formas de aprovechar técnicas como el phishing, el ransomware, la ingeniería social y otras para lanzar sus ataques. He aquí algunos de los riesgos más críticos encontrados.

1. Acceso remoto seguro

A medida que la enseñanza a distancia va sustituyendo a la presencial, los alumnos y profesores necesitan acceder a herramientas de aprendizaje en línea ubicadas principalmente en la nube,

es decir, aplicaciones para compartir archivos, correos electrónicos, aplicaciones, y a veces necesitan acceder a recursos de la red escolar de forma remota. Si el acceso remoto no está protegido, los hackers pueden penetrar en el sistema y hacerse con el control de toda la red.

2. Acceso a datos sensibles

Las instituciones educativas contienen un tesoro de datos sensibles que pueden venderse en la dark web. Los datos personales de estudiantes, profesores, antiguos alumnos y personal administrativo, así como los datos sensibles relacionados con la investigación y la propiedad intelectual de un centro educativo, pueden ser un auténtico tesoro que un hacker podría vender o por el que podría pedir un rescate. Por ello, es esencial implantar un acceso basado en la identidad, que permita a los usuarios autorizados acceder únicamente a los recursos que necesitan para realizar su trabajo.

3. Malware

El paso a la educación a distancia significa que muchos dispositivos conectados a la red escolar son BYOD (Bring Your Own Device). Es difícil saber si los dispositivos y aplicaciones utilizados están debidamente actualizados con parches y si el propio antivirus está al día. A menos que estos dispositivos remotos se conecten a través de una VPN, es necesario asegurarse de que son seguros antes de que puedan acceder a los recursos de la red de formación. Es importante desplegar capacidades avanzadas de protección web que puedan identificar y bloquear las amenazas web más recientes.

4. Phishing

La ingeniería social y los ataques de phishing son importantes riesgos de ciberseguridad para los centros de formación franceses. Los formadores y los profesores o miembros del personal que son engañados para que hagan clic en enlaces maliciosos pueden dar a los ciberdelincuentes acceso a la red del centro y a recursos valiosos. La mejor manera de contrarrestar los ataques de

ingeniería social y phishing es mediante la concienciación y la formación de los usuarios. Formar y poner a prueba a tus usuarios con ataques simulados ayudará a crear una cultura positiva de concienciación sobre la seguridad y les hará menos vulnerables a las distintas estafas online.

5. Fraude

En lo que respecta al fraude, el año 2020 fue muy intenso, incluidos los ataques de ingeniería social. Entre los intentos de fraude más activos se encontraban las campañas de extorsión, en las que los hackers afirmaban haber pirateado el dispositivo de un usuario y obtenido material comprometedor por el que se fijaba un rescate; los sorteos fraudulentos en nombre de las marcas conocidas, ofreciendo ganar los smartphones más nuevos u otros precios valiosos.

Se observó una nueva tendencia: correos electrónicos de extorsión con la amenaza de filtrar datos. En muchas ocasiones, el objetivo eran las empresas. Anuncios engañosos en las redes sociales, en los que se utilizaban nombres de personajes famosos sin su conocimiento, invitaban a los internautas a invertir en criptomoneda. Los estafadores también realizaron llamadas telefónicas e intentaron persuadir a la gente para que invirtiera. En algunos casos, se observaron repetidos intentos fraudulentos en los que se ofrecía a las víctimas del fraude financiero ayuda para recuperar los recursos perdidos.

Estafas telefónicas: falsificando los números de teléfono de diferentes entidades de crédito y haciéndose pasar por representantes bancarios, los estafadores, aprovechando el escaso conocimiento del público sobre métodos adicionales de autenticación, defraudaron recursos financieros de varios miles de usuarios, causando pérdidas totales por valor de cientos de miles a las entidades de crédito letonas. Adaptación de los piratas informáticos a la necesidad de empezar a trabajar a distancia - teniendo en cuenta las necesidades de las empresas de cambiar rápidamente a una condición de trabajo a distancia y la implementación de la circulación de documentos electrónicos, los piratas informáticos aprovecharon la situación para, por ejemplo, aducir que varios contables de empresas recibieron correos electrónicos en nombre del director o de otro empleado para realizar un pago urgente o cambiar la cuenta de nómina.

Interferencia en la correspondencia comercial de las empresas: al comprometer los correos electrónicos de las empresas o de sus socios colaboradores, permitía a los atacantes elegir un momento adecuado para enviar a una de las partes una factura con una cuenta modificada.
Muchos internautas fueron blanco de mensajes estafadores con enlaces de acceso directo (ej.uz), utilizados para enmascarar el destino real del enlace, en nombre de las instituciones estatales en relación con el estado de emergencia y la situación epidemiológica en el país.
Tiendas en línea falsas - se ha observado una actividad especialmente elevada durante la temporada de vacaciones por medio de anuncios en las redes sociales y debido a las restricciones covid-19 que obligaron a las empresas a vender sus productos en línea.

Puede ser útil emplear algunos datos aportados por los informes nacionales. Por ejemplo, en Francia los riesgos digitales están muy presentes en las representaciones de los jóvenes profesores, que retransmiten fácilmente el discurso de los medios de comunicación. Los tres riesgos que los profesores consideran que afrontan más personalmente son técnicos (66,20%), éticos y jurídicos (55,80%) e informativos (54,70%). Los riesgos psicosociales, cognitivos y socioeconómicos parecen preocuparles menos. Existe una discrepancia sistemática entre las representaciones de los riesgos para ellos mismos y para los alumnos. En efecto, los tres riesgos a los que los profesores consideran que se enfrentan más sus alumnos son los riesgos psicosociales (69,95%), informativos (70,75%) y técnicos (62,80%). Por tanto, los profesores sienten la misma vulnerabilidad que sus alumnos en lo que respecta a los riesgos técnicos, pero consideran que sus alumnos están más expuestos a los problemas relacionados con el acoso o la información falsa en particular. La amplificación de los riesgos para los alumnos puede explicarse por el hecho de que los profesores los perciben como muy vulnerables. Una profesora en prácticas describió a sus alumnos de cuarto curso como muy vulnerables, bastante ingenuos, no necesariamente conscientes del peligro potencial de las redes.

El informe de la Oficina Federal de Seguridad de la Información (BSI) de Alemania señaló que varias campañas se aprovecharon de la confusión y el miedo creados por el COVID-19, entre ellas campañas de malware y phishing, fraudes a directores ejecutivos y estafas. Además, la BSI señaló que estos sucesos podrían haber aumentado las posibilidades de éxito de tales ataques debido a los temores, preocupaciones e inseguridades asociados a tales acontecimientos. En los últimos años, dentro del panorama alemán y europeo, la ciberdelincuencia ha sido la principal causa de los recientes ciberataques. Para analizar el contexto alemán específico y extraer un análisis de necesidades, es especialmente significativo el examen del Barómetro Digital 2020, una encuesta en línea representativa de ciudadanos particulares sobre ciberseguridad, realizada conjuntamente por la BSI y la Comisión de Prevención del Delito de la Policía Estatal y Federal alemana. La transición digital está moldeando activamente nuestra vida cotidiana, desde las compras en línea hasta los wearables (como los brazaletes de seguimiento de la forma física, los smartwatches o las gafas inteligentes), pasando por los nuevos sistemas de pago y de identificación.

Sin embargo, este grado de digitalización no está exento de riesgos y peligros. Uno de cada cuatro encuestados declaró haber sido víctima de la ciberdelincuencia en el último año. La tasa global de ciberdelincuencia en 2020 se mantiene constante. Las compras en línea y el acceso de terceros a cuentas en línea son los tipos de fraude más comunes que afectan a las víctimas (44%) y (30%), respectivamente. La mayoría de los encuestados conocían las recientes recomendaciones de ciberseguridad para prevenir la ciberdelincuencia. Por lo general, estas recomendaciones sólo se siguen cuando tiene sentido que la persona lo haga (41%) o acaba de enterarse de un consejo concreto (39%). La investigación muestra que las personas que ya han sido víctimas varias veces son más propensas a seguir los consejos sólo cuando surge un problema (33%), incluso si ya eran conscientes de ello. Finalmente, a pesar de los resultados, dos tercios de los encuestados expresaron su deseo de recibir más información sobre la prevención del robo de datos (66%). Los consejos más solicitados consisten en sugerencias

prácticas, como formas de garantizar contraseñas seguras para varias cuentas en línea (59%), seguidas de consejos sobre qué software es el más adecuado para proteger las cuentas en línea (52%) y consejos sobre los pros y los contras de los gestores de contraseñas (49%).

Finalmente, otra perspectiva significativa la ofrece Irlanda y las amenazas a la ciberseguridad ocurridas en 2021. Un ataque masivo y coordinado iniciado en mayo de 2021 perturbó el servicio sanitario y los sistemas informáticos de todo el país, robó datos personales de un alto porcentaje de pacientes y sigue exigiendo un rescate por la devolución de los datos. En respuesta, el Health Service Executive (HSE) ha tenido que cerrar los sistemas informáticos de hospitales y servicios sanitarios para protegerse de nuevos robos de datos. Muchos servicios se han visto interrumpidos y se ha filtrado información personal y médica. Sin embargo, hay que señalar que no hay pruebas que apoyen la adquisición de que se hayan producido nuevas estafas con información de los ciudadanos. Irlanda alberga más del 30% de los datos de la UE debido al número de centros de ciberseguridad con sede en el país. Aunque esto ofrece muchas oportunidades, también se traduce en un mayor nivel de amenaza de ciberdelincuencia. Como Irlanda es una democracia liberal abierta, se considera especialmente vulnerable a los llamados ataques del tipo "hackear y filtrar". Por lo general, se considera que estos ataques tienen una motivación política y se centran en la desinformación y las "fake news" (noticias falsas) utilizadas como un intento de desestabilizar al Estado.

Muchos implicados en el sector de la ciberseguridad reclaman una mayor inversión en organismos gubernamentales como el Centro Nacional de Ciberseguridad (NCSC) de Irlanda. Otras amenazas/riesgos que siguen prevaleciendo son los que se ciernen sobre las Infraestructuras Nacionales Críticas (CNI), los sistemas del sector público y los datos que se han esbozado brevemente en párrafos anteriores. Los nuevos problemas que empiezan a surgir son los relacionados con el despliegue de las tecnologías 5G. Aunque esto dará lugar a nuevas

tecnologías y servicios, la ciberseguridad debe estar en el primer plano de la reflexión a medida que muchos países comienzan a adaptarse.

Fuera de una perspectiva nacional y empresarial, los delitos de ciberseguridad continúan ocurriendo prolíficamente a diario entre la persona promedio. A menudo no se denuncian a las fuerzas de seguridad, con solo el cinco por ciento de los ciberdelitos supuestamente denunciados a la policía en Irlanda en 2019. Además, un informe de 2019 encargado por Microsoft en Irlanda concluye que los empleados siguen considerándose el "eslabón débil" del sistema de seguridad debido a la falta de formación en seguridad, la mala gestión de contraseñas, el uso de dispositivos personales con datos relacionados con el trabajo y las posibles infracciones del Reglamento General de Protección de Datos de la UE.

3. Buenas prácticas de programas y recursos de ciberseguridad para centros de FP en la Unión Europea y en cada país socio

Como se especifica en la introducción, el proyecto Cyber.EU.VET implica a un consorcio polifacético y diverso. En lo que respecta a las competencias digitales y de ciberseguridad, los países socios del consorcio presentan diferentes grados de eficacia, perfectamente descritos por el índice DESI.

El análisis académico y la evaluación de las buenas prácticas formaron parte integrante del trabajo de investigación realizado a escala nacional por cada socio del consorcio del proyecto. Esta investigación tuvo como pauta común un análisis de las necesidades en materia de EFP a escala local y nacional. Al llevar a cabo este trabajo, los siete socios nacionales compartieron algunas dificultades relacionadas con la búsqueda de iniciativas de formación y ciberseguridad específicamente diseñadas para profesores de EFP. Si bien esto ha dificultado bastante esta tarea, también ha mostrado aún más claramente la importancia y la necesidad de desarrollar proyectos en este ámbito. Además, ha confirmado el espíritu extremadamente innovador del proyecto CYBER.EU.VET. He aquí una recopilación de las buenas prácticas más relevantes encontradas por cada socio.

3.1 Alemania - Iniciativa EFP 4.0

EFP 4.0 es una iniciativa paraguas, desarrollada en colaboración por el Ministerio Federal de Educación e Investigación (BMBF) y el Instituto Federal de Educación y Formación Profesional (BIBB) desde 2016, que reunió una amplia gama de proyectos dentro de tres pilares principales. El pilar 2 de esta amplia iniciativa (que aún está en curso) está completamente dedicado a la "alfabetización digital/competencia mediática", y tiene como objetivo definir las competencias

mediáticas, que deberían considerarse como un requisito de entrada y como una competencia clave en todas las ocupaciones de la EFP (para aprendices, profesores y formadores). Los programas de financiación para equipar mejor los centros de formación y apoyar a las pequeñas y medianas empresas (PYME) con vistas a la digitalización complementan este enfoque de promoción de la competencia mediática en la EFP. A través del programa especial de digitalización ÜBS (71), el BMBF y el BIBB contribuyen a acelerar la digitalización de los procesos en la formación de aprendices en el contexto de la "EFP 4.0". El programa especial consta de dos líneas de financiación:

1) Se financia la adquisición de equipos digitales seleccionados (dispositivos digitales, máquinas, sistemas y software, como tecnologías domésticas inteligentes, 21 robots industriales, impresoras 3D y medios digitales de enseñanza y aprendizaje, como tabletas y pantallas táctiles), con el fin de modernizar la formación de los aprendices, especialmente de los formados por las PYME;
2) El programa también financia 8 proyectos piloto en centros de competencia que identifican las repercusiones de la digitalización en los perfiles de la actividad profesional y determinan los requisitos y las consecuencias que de ello se derivan para la cualificación del personal cualificado y el personal de formación. En un segundo paso, desarrollan conceptos innovadores de enseñanza y aprendizaje para la EFP 4.0 y los difunden como multiplicadores. El objetivo es garantizar que los resultados sean transferibles y que exista una amplia gama de aplicaciones.

A continuación figuran algunos ejemplos de los proyectos piloto mencionados:

- "Medios digitales en la EFP", que finalizará en 2022 y que se compone de varios subprogramas con diferentes prioridades de financiación, está financiando proyectos nacionales de formación digital que desarrollan nuevos escenarios de aprendizaje y

modernos cursos de formación inicial y continua que promueven la adquisición de competencias en medios digitales;

- "Qualification Initiative Digital Change - Q 4.0", que, desde 2018, financia el desarrollo y la puesta a prueba de nuevos conceptos de formación para formadores de EFP en las empresas. El proyecto consta de dos subproyectos: 1) Seminarios MIKA (Competencia en medios de comunicación y TI para el personal de formación) para promover la competencia pedagógica básica en medios de comunicación, el desarrollo y la prueba de módulos de formación continua para fortalecer las habilidades básicas en medios de comunicación y TI del personal de formación; 2) Q 4.0 NETWORK con el objetivo de adaptar el proceso de formación al cambio digital, teniendo en cuenta también las diferencias regionales y sectoriales. En ambos proyectos, el resultado final podría ser un prototipo de oferta de seminarios probada que podría ponerse a disposición del personal de EFP en todo el país;
- "Digitalización II" desde 2018 para identificar estrategias de diseño de procesos de aprendizaje que utilicen el potencial de los medios digitales para apoyar el aprendizaje exitoso, tanto para individuos como para grupos.

3.2 Francia - Internet sin restricciones

(Dado que en este país concreto faltan buenas prácticas en el ámbito de la EFP, se ha seleccionado este estudio de caso como práctica que cumple los requisitos exigidos pero que no se refiere específicamente al sector de la EFP).

En vista de los constantes casos de ciberacoso, adicción a Internet, encuentros peligrosos en la red y sus trágicas consecuencias para estudiantes muy jóvenes, se ha hecho necesario llamar la

atención de todos sobre los derechos y los límites del comportamiento en línea y, sobre todo, presentar Internet como una herramienta de enriquecimiento y entretenimiento libre de peligros. Creada en 2000, pionera en pedagogía digital y experta en comunicación para el público joven, Tralalere es líder en la producción de programas educativos cross-media: dibujos animados para producciones multimedia, juegos serios, aplicaciones móviles, libros electrónicos, etc. En particular, Tralalere concibió y dirigió el programa nacional de concienciación sobre los riesgos en Internet: www.internetsanscrainte.fr.

Gestionado por Tralalere desde 2008, Internet Sans Crainte es el programa nacional para ayudar a los jóvenes a controlar mejor su vida digital. En concreto, Internet Sans Crainte ofrece un centenar de recursos gratuitos llave en mano para ayudar a profesores, educadores y padres a orientar a los jóvenes de 6 a 18 años hacia un uso consciente y responsable de las pantallas y la tecnología digital. Internet Sans Crainte también ofrece asesoramiento y experiencia sobre cómo apoyar a los jóvenes en su educación digital a través de fichas temáticas. Tralalere e Internet Sans Crainte también coordinan Safer Internet France, programa nacional y europeo para la protección de los menores en Internet, junto con la línea Net Ecoute (e15 Enfance) y el Point de contact. En este marco, Internet Sans Crainte organiza en Francia el Día de Internet Segura, una jornada mundial de sensibilización de los jóvenes para un mejor uso de Internet. Este programa cuenta con el apoyo de la Comisión Europea en el marco de la red Inhope/Insafe, que incluye a 38 países.

BENEFICIARIOS

Internet Sans Crainte, ofrece durante todo el año recursos digitales adaptados a diferentes públicos, incluido:

- Mediadores educativos (profesores, animadores, bibliotecarios, etc.);
- Padres y familias;
- Instituciones y asociaciones..

3.3 Irlanda - Niños ciberseguros

(Dado que en este país no existen buenas prácticas en el ámbito de la EFP, se ha seleccionado una práctica que cumple los requisitos pero que no se refiere específicamente al sector de la EFP).

El proyecto Cybersafe Kids comenzó en 2015 y ahora se ha convertido en una organización benéfica reconocida financiada por varios fondos filantrópicos irlandeses, como The Ireland Funds. Cybersafe Kids imparte una serie de programas de formación centrados en la ciberseguridad en las escuelas de todo el país de Irlanda. La visión de Cybersafe Kids es la de un mundo en el que los niños utilicen la tecnología de forma segura, positiva y satisfactoria. Los principales interesados en Cybersafe Kids son las escuelas participantes de toda Irlanda (alumnos, profesores, directores y tutores), las universidades de investigación asociadas, los financiadores de la organización benéfica y el equipo que participa en la ejecución de los programas. El principal objetivo de la organización benéfica es avanzar, promover y proporcionar educación y formación a niños, padres y profesores de la comunidad para garantizar una navegación segura y responsable en el mundo online. En cuanto al impacto, hasta la fecha, Cybersafe Kids ha llegado a 24.000 niños de entre 8 y 13 años a través de sus programas escolares. Solo en 2020, los programas se pusieron en contacto con 5.986 niños y 1.554 padres en 56 colegios de Irlanda. Además, se distribuyó una encuesta anónima en línea que recopiló datos de 3.764 niños de entre 8 y 12 años sobre su uso de Internet. Según el Informe de los Directores (2019), las principales áreas de impacto fueron las siguientes:

- La impartición de un Programa Educativo y la puesta en marcha de un proyecto de medición de cambios de comportamiento en colaboración con la Universidad de Dublín y el Comité de Niños y Jóvenes (CYPSC);

- La organización de una intensa campaña del "Día de Internet Segura";
- Lanzamiento de contenidos y recursos en línea dirigidos a los padres de niños más pequeños (de 2 a 10 años). En años anteriores se publicó material para niños mayores;
- Desarrollo de una serie de "peticiones" políticas que pretenden influir en la política general del país sobre ciberseguridad.

3.4 España – SPACE: Habilidades para profesionales de la enseñanza contra el ciberacoso.

ANTECEDENTES.

La difusión y el uso generalizados de las nuevas tecnologías están relacionados con el fenómeno del ciberacoso. En 2009 en toda Europa aproximadamente el 18% de los jóvenes europeos entre 13 y 19 años habían sido acosados/acosados/acosados a través de internet y teléfonos móviles, las tasas actuales oscilan entre el 10% y el 52%. El Parlamento Europeo destaca que el ciberacoso aumentó entre los niños de 11 a 16 años del 7% en 2010 al 12% en 2014.

NECESIDADES DE LOS GRUPOS DESTINATARIOS.

El proyecto SPACE responde a las necesidades de formación de los profesores escolares, con el fin de que adquieran competencias para prevenir/contrarrestar el ciberacoso. De hecho, a pesar de que los Estados miembros de la UE han puesto en marcha numerosas iniciativas y proyectos para prevenir y combatir el ciberacoso, éste parece ir en aumento: al tratarse de un fenómeno nuevo, carece de un sistema orgánico de conocimientos, habilidades y acciones educativas estructuradas que garanticen que los profesores adquieran el conocimiento de su dinámica, el dominio de las tecnologías digitales para un uso seguro de la Red, y las competencias para planificar acciones de prevención, información y formación.

OBJETIVOS.

Muchos recursos y contenidos sobre ciberbullying han sido desarrollados por escuelas e instituciones; sin embargo, se trataba de iniciativas aisladas, no recogidas en un único espacio web y, por tanto, no valorizadas. SPACE ha asumido este reto y ha desarrollado un MOOC -curso online abierto y gratuito- sobre ciberacoso para profesores de centros escolares, y una Biblioteca Digital Pública de Recursos Educativos Abiertos multilingüe sobre ciberacoso. Principales objetivos del proyecto:

- mapear y describir las competencias necesarias para prevenir y contrastar el ciberacoso;
- desarrollar una biblioteca digital de REA sobre ciberacoso, con funciones de búsqueda avanzada;
- desarrollar un MOOC para profesores de escuela sobre ciberacoso, utilizando los REA previamente recuperados y etiquetados;
- potenciar y mejorar en los profesores implicados la competencia digital, a saber, la ciberseguridad, el riesgo web y la etiqueta en la red;
- apoyar a los profesores en la adquisición de competencias para intervenir en caso de ciberacoso en la escuela y para planificar y realizar actividades de información y formación con sus alumnos.

PARTICIPANTES.

El principal grupo destinatario del proyecto son los profesores (niveles CINE 2 y CINE 3). Los grupos destinatarios indirectos fueron los directores de centros escolares y el personal no docente; los estudiantes; los padres; las autoridades escolares y los responsables de la toma de decisiones. 139 profesores participaron en la prueba del MOOC y 300 en los eventos multiplicadores organizados en los países socios. La Biblioteca Digital Pública recibió más de 8.00 visitas durante el ciclo de vida del proyecto.

ACTIVIDADES.

El proyecto duró 24 meses, durante los cuales se llevaron a cabo las siguientes actividades:

- realización de un mapa de competencias y de un modelo MOOC
- diseño y desarrollo de una biblioteca digital en línea sobre ciberacoso
- recuperación, catalogación e identificación de REA sobre ciberacoso, e implementación de estos recursos en la biblioteca digital
- creación y personalización de una plataforma CMS para alojar el MOOC;
- diseño, desarrollo y prueba de un MOOC multilingüe sobre ciberacoso;
- creación de un conjunto de herramientas con indicaciones, directrices y recomendaciones sobre el sistema y las herramientas SPACE
- realización de 10 Eventos Multiplicadores en los países socios y una conferencia final;
- realización de 4 reuniones del consorcio
- difusión mediante la creación de un sitio web, folletos, presentaciones, participación como reportero invitado a la Feria DIDACTA en Florencia, artículos en revistas y periódicos.

IMPACTO.

El proyecto ha producido un impacto positivo, promoviendo la concienciación sobre el ciberacoso, un mayor conocimiento de sus dinámicas y métodos de prevención y contraste, y desarrollando un conjunto multidimensional de conocimientos y habilidades en el grupo de profesores europeos implicados. Los profesores y organizaciones implicados en las pruebas han adquirido competencias para prevenir y contrastar el ciberacoso, competencias digitales especializadas sobre ciberseguridad, riesgos en la red y etiqueta en la red, han desarrollado habilidades estratégicas y competencias metodológico-didácticas mejorando su profesionalidad docente, disponen de instrumentos más eficaces para realizar actividades de información y formación a sus alumnos para prevenir el ciberacoso.

3.5 Letonia - Programa "Mejora de la competencia digital del profesorado en forma de entorno electrónico para el uso de tecnologías educativas"

OBJETIVO.

El objetivo del Programa es mejorar la competencia digital de los educadores: enseñarles tecnologías y herramientas que les ayuden a organizar su proceso de trabajo de forma más eficiente. El Programa es implementado desde 2014 por el Ministerio de Educación y Ciencia de la República de Letonia.

BENEFICIARIOS.

El contenido de los cursos en 2020 está diseñado para:

- equipos directivos de centros educativos;
- educadores de centros de formación profesional (EFP) y de enseñanza general;
- profesores de enseñanza primaria;
- profesores de preescolar;
- profesores de varias asignaturas (matemáticas, lengua letona, informática, ingeniería, diseño y tecnología, física, química y biología).

DESCRIPCIÓN.

En 2020, el Ministerio de Educación y Ciencia ha establecido la mejora de la competencia digital de los educadores como un objetivo prioritario de la competencia profesional, asignando financiación adicional. El programa ofrece cursos gratuitos para educadores con diferentes niveles de conocimientos que representan a diversas materias (su campo de especialización, véase la sección Beneficiarios). Los ejecutores de los cursos han desarrollado tareas de aprendizaje detalladas, han atraído a líderes de grupo - consultores para garantizar un régimen

de aprendizaje favorable para los educadores. El contenido de los cursos está diseñado de acuerdo con los requisitos del entorno de aprendizaje moderno.

RESULTADOS OBTENIDOS.

4339 educadores han asistido a cursos largos (con el derecho concedido a trabajar como profesor de informática)

y cortos de desarrollo de competencias profesionales (2014-2020).

INNOVACIÓN.

Enfoque innovador obstaculiza en la organización del proceso - cada participante del curso puede aprender el

contenido a un ritmo y en un momento que les resulten convenientes. Durante el curso, se analizan las tecnologías y herramientas que se pueden utilizar en el proceso de estudio con el fin de promover la colaboración y simplificar la organización del proceso de estudio / proceso de trabajo de los educadores.

3.6 Portugal

A pesar de algunas iniciativas ad-hoc, no se identificaron acciones formativas en materia de ciberseguridad para la FP. Sólo se identificaron en el mercado algunos cursos de educación superior, postgrados o de carácter empresarial, por lo que la formación en ciberseguridad para la FP debería ser una prioridad fundamental para apuntalar el futuro más ciberseguro de nuestro país, es decir, capaz de garantizar la seguridad personal y empresarial.

El Centro Nacional de Ciberseguridad, con la misión de promover el intercambio de conocimientos y una cultura nacional de Ciberseguridad, desarrolló el Programa de Sensibilización y Formación en Ciberseguridad, a través del cual se pretende masificar la

formación y concienciación de los ciudadanos y empleados de las organizaciones por los peligros del uso desinformado del ciberespacio, mediante la realización de acciones de sensibilización y formación en Ciberseguridad en diferentes puntos del territorio nacional, de norte a sur, pasando por las islas, con el apoyo de colaboradores, pero nada dirigido a los centros de FP..

3.7 Italia - Profesores conectados y seguros

ANTECEDENTES.

El programa tiene como objetivo general llevar a cabo acciones dirigidas a innovar y fortalecer las competencias digitales en los centros educativos. En concreto, el programa pretende mejorar las habilidades y conocimientos de los docentes en relación con las nuevas experiencias de enseñanza digital integrada, el funcionamiento y los beneficios del Internet de las Cosas y la importancia de la ciberseguridad. El programa se promueve en el marco del nuevo memorando de entendimiento entre el Ministerio de Educación (Italia) y Cisco.

GRUPOS DESTINATARIOS.

Los beneficiarios del programa son profesores de escuelas italianas de cualquier orden y grado.

ACTIVIDADES.

El programa de formación ofrecido por Cisco a los profesores consta de 3 seminarios web a los que están vinculados 3 cursos de profundización. La participación en todo el programa es totalmente gratuita.

1. Un mundo digital conectado Webinar "DAD y nuevas experiencias de enseñanza digital integrada" impartido por personal de Cisco o socios de Cisco y curso en línea vinculado "Conéctate". Tiempo estimado de realización: 30 horas Descripción general del curso: El

curso enseña a desarrollar conocimientos digitales básicos. La estructura del curso, especialmente interactiva, crea un entorno de fácil acceso para un público que se acerca por primera vez al mundo de las TI.

2. Ciudadanos digitales conscientes: Webinar "Smart City e Internet de las Cosas: nuevos servicios digitales para los ciudadanos" impartido por personal de Cisco o Partners de Cisco y curso online vinculado "Introducción al Internet de las Cosas (IoT)". Tiempo estimado de realización: 20 horas Descripción general del curso: El curso Introducción al IoT (Internet de las Cosas) introduce a los profesores en las tecnologías que soportan el IoT y las oportunidades generadas por el creciente número de conexiones de red entre personas, procesos, datos y cosas.
3. Seguridad informática: Webinar "Cómo protegerse de las amenazas de red" impartido por personal de Cisco o Partners de Cisco y curso online vinculado "Introducción a la Ciberseguridad". Tiempo estimado de realización: 20 horas. Resumen del curso: El curso Introducción a la Ciberseguridad analiza las tendencias en el mundo de las TI, las amenazas y el hecho de estar en total seguridad en el ciberespacio, protegiendo los datos personales.

IMPACTO.

Dado que el proyecto finalizó el 3 de junio, aún se están elaborando las cifras relativas a los profesores formados. Sin embargo, el proyecto es innovador porque combina la formación relacionada con la tecnología con el emprendimiento digital, pero también con la programación.

Conclusión

La investigación realizada para el proyecto CYBER.EU.VET reveló que hay una falta de datos e información sobre las competencias en ciberseguridad y los retos de los educadores de los centros de enseñanza a nivel europeo, así como que hay un número limitado de iniciativas centradas en las cuestiones de ciberseguridad dentro de la EFP, lo que indica que el proyecto CYBER.EU.VET ha abordado el tema emergente en todos los Estados miembros.

No obstante, las iniciativas existentes son exhaustivas y han demostrado su eficacia (véase la sección Buenas prácticas). En la actualidad, la mayoría de las actividades y proyectos se centran en la concienciación sobre la ciberseguridad de la población en general y en la mejora de las competencias digitales generales de los educadores, en lo que ha influido la rápida adaptación al proceso de trabajo/aprendizaje a distancia.

El consorcio asociado es polifacético y una clara expresión de un alcance diferente de las competencias digitales en toda Europa. Sin embargo, independientemente de la clasificación DESI de cada uno de los países, este Informe de Investigación del Consorcio puede utilizarse para extraer indicaciones significativas y válidas para todo el contexto europeo.

El sentimiento de necesidad de formación es claro, incluso entre los profesores de FP que ya han recibido formación en TIC. No se rechaza la necesidad de formación ni se cuestiona su utilidad. También se observa que cuanto más expuestos se sienten los profesores a los riesgos psicosociales, éticos, jurídicos, técnicos o sanitarios, más dicen sentir la necesidad de formación.

Según una encuesta nacional, más de la mitad de los profesores que se sienten vulnerables al ciberacoso consideran que la formación es necesaria. Para ellos, la formación inicial y continua

es una oportunidad para compartir experiencias y analizar métodos de práctica profesional en este campo. Se sigue creyendo que el uso de herramientas digitales en la educación es una forma de enseñar o un objeto que hay que enseñar a los alumnos, y no una parte integrante de su cultura general.

Debe desarrollarse una cultura de las fuentes de información y de las prácticas sobre los riesgos digitales (investigación y vigilancia). También debe reforzarse la formación sobre los retos de la tecnología digital y, en particular, sobre los problemas psicosociales, éticos, jurídicos y técnicos que pueden surgir en el uso de las herramientas digitales y que preocupan a los profesores hasta el punto de llevarles a renunciar a todo uso.

Así pues, el conocimiento de los riesgos digitales puede influir positivamente en las prácticas pedagógicas para educar a los alumnos en la alfabetización digital. Un profesor con una sólida cultura digital será más proclive a utilizar la tecnología digital en el aula con sus alumnos y a hacer de la tecnología digital un objeto de enseñanza-aprendizaje.

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

Referencias

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

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

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

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

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

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

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

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

Buisán García,M.; Valdés, F. (2017), La industria Conectada 4.0., Revista de economía, No 898.

Bihouix P, Mauvilly, K (2016), Le Désastre de l'école numérique, Le Seuil.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Escuela de organizacion industrial, Activa industria 4.0.

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

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

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

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

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

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

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

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

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

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

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

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

Huismann, A. (2020), Vocational education and training for the future of work: Germany, Cedefop ReferNet thematic perspectives series.

Information Technology Security Incident Response Institution, (2021), CERT.LV Annual Report 2020.

Izglītības un zinātnes ministrija (2017), Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā.

Izglītības un zinātnes ministrija (2020), Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OECD (2021), Going Digital in Latvia

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

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

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

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

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

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

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

DISCLAIMER

Es posible rastrear el documento a través del siguiente código qr: