Universidad de Oviedo

RIAICES

Volumen 7, número 2, julio-diciembre, 2025/págs. 31-40

Diseño de un Módulo de Metodologías Aplicadas de Ciberseguridad en la Formación Profesional: Innovación Curricular y Vinculación con el Sector Productivo

Lucía Menéndez Menéndez
Universidad de Oviedo
E-mail: menendezmlucia@uniovi.es
ORCID: https://orcid.org/0000-0001-5042-570X

Carolina González Melgar
Universidad de Oviedo
E-mail: gonzalezmcarolina@uniovi.es
ORCID: https://orcid.org/0000-0001-8426-2152

Covadonga Rodríguez Fernández
Universidad de Oviedo
E-mail: rodriguezcovadonga@uniovi.es
ORCID: https://orcid.org/0000-0002-1082-528X

Adriana Genoveva Samaniego-Benavides
Profesora e investigadora del Ministerio de Educación de Ecuador
E-mail: uo296265@uniovi.es
ORCID: https://orcid.org/0009-0007-0656-0665

Emilio Álvarez Arregui
Universidad de Oviedo
E-mail: alvarezemilio@uniovi.es
ORCID: https://orcid.org/0000-0002-4657-753X

RESUMEN
El presente trabajo analiza el proceso de diseño de un módulo formativo optativo titulado "*Metodologías Aplicadas de Ciberseguridad*, dirigido al Ciclo Formativo de Grado Superior en Desarrollo de Aplicaciones Web. La propuesta surge en el marco de la cooperación entre centros de excelencia de Formación Profesional y el sector empresarial TIC, con el propósito de fortalecer las competencias digitales avanzadas vinculadas a la ciberseguridad. Se expone una justificación contextualizada en las tendencias europeas sobre cualificación digital —particularmente el proyecto *European Software Skills Alliance (ESSA)*—, y se describe un proceso metodológico basado en trabajo colaborativo, grupos focales y validación experta. Los resultados evidencian la necesidad de integrar la ciberseguridad de forma transversal en la formación técnica, la relevancia de los enfoques *DevSecOps* y la importancia de desarrollar competencias para el desarrollo seguro de software. El estudio concluye destacando la pertinencia del modelo de cooperación educación–empresa como vía efectiva de innovación curricular y desarrollo profesional docente.

Palabras clave: ciberseguridad; innovación educativa; formación profesional; competencias digitales; currículo.

ISSN: 2340-6194
DOI: https://doi.org/10.17811/ria.7.2.2025.31-40

Desenho de um Módulo de Metodologias Aplicadas de Cibersegurança no Ensino Profissional: Inovação Curricular e Vinculação com o Setor Produtivo

RESUMO

Este estudo analisa o processo de concepção de um módulo formativo optativo denominado *Metodologias Aplicadas de Cibersegurança*, destinado ao Curso Técnico Superior em Desenvolvimento de Aplicações Web. A proposta surge no contexto da cooperação entre centros de excelência de Formação Profissional e o setor empresarial de TIC, com o objetivo de fortalecer as competências digitais avançadas relacionadas à cibersegurança. Apresenta-se uma justificativa baseada nas tendências europeias de qualificação digital — especialmente o projeto *European Software Skills Alliance (ESSA)* — e descreve-se uma metodologia colaborativa que inclui grupos focais e validação por especialistas. Os resultados demonstram a necessidade de integrar a cibersegurança de forma transversal na formação técnica, ressaltando a relevância das abordagens *DevSecOps* e do desenvolvimento seguro de software. Conclui-se que a cooperação entre educação e setor produtivo constitui uma estratégia eficaz de inovação curricular e de desenvolvimento profissional docente.

Palavras-chave: cibersegurança; inovação educacional; formação profissional; competências digitais; currículo.

Design of a Module on Applied Cybersecurity Methodologies in Vocational Education: Curricular Innovation and Linkage with the Productive Sector

ABSTRACT

This paper analyzes the design a process of an elective training module entitled *Applied Cybersecurity Methodologies*, aimed at the Higher Vocational Education cycle in Web Application Development. The proposal emerges within a collaborative framework between Vocational Education Excellence Centers and the ICT business sector, seeking to strengthen advanced digital skills related to cybersecurity. The study presents a contextually grounded justification based on European digital, particularmente trends — particularly the *European Software Skills Alliance (ESSA), y* — and describes a methodological approach involving collaborative work, focus groups, and expert validation. Results highlight the need to integrate cybersecurity transversally into technical education, emphasizing the relevance of *DevSecOps* approaches and secure software seguro. The study concludes by underlining the effectiveness of education–industry cooperation as a means of curricular innovation and professional development.

Keywords: cybersecurity; educational innovation; vocational education; digital skills; curriculum.

1. Justificación y objetivos

La aceleración tecnológica y la creciente digitalización de los procesos productivos han situado la ciberseguridad como una competencia clave en todos los niveles educativos y profesionales. En el contexto de la Formación Profesional de Grado Superior (FP), particularmente en el perfil de *Desarrollo de Aplicaciones Web*, se observa una brecha significativa entre los conocimientos técnicos del alumnado y las demandas de seguridad que requiere el sector empresarial. Esta brecha no responde únicamente a la rápida evolución tecnológica, sino también a la insuficiente integración curricular de la ciberseguridad como competencia transversal dentro de los programas formativos.

La presente investigación se enmarca en un proceso de innovación curricular y vinculación con el sector productivo, cuyo propósito ha sido diseñar un módulo optativo titulado "Metodologías Aplicadas de Ciberseguridad". Este módulo busca responder a los retos actuales del desarrollo web seguro y promover la formación de técnicos con competencias que trasciendan la mera programación, incorporando la dimensión ética, legal y de gestión de riesgos que caracteriza a la ciberseguridad contemporánea.

El trabajo se justifica por tres razones fundamentales: Primero, la creciente vulnerabilidad de las infraestructuras digitales, agravada por el incremento del volumen y la sensibilidad de los datos procesados en entornos web. Segundo, el alineamiento con las políticas europeas de cualificación digital y empleabilidad, especialmente las impulsadas por el programa *Erasmus+ Sector Skills Alliances* y el proyecto *European Software Skills Alliance (ESSA, 2023–2027)*, que promueven el desarrollo de competencias específicas en ciberseguridad, inteligencia artificial y desarrollo de software seguro. Tercero, la necesidad de fortalecer la cooperación entre el ámbito educativo y el empresarial, de modo que los programas formativos respondan con pertinencia a los requisitos reales del mercado laboral.

Desde una perspectiva pedagógica, la propuesta parte del reconocimiento de la FP como espacio estratégico de innovación educativa, donde convergen la formación técnica, la práctica profesional y la investigación aplicada. Diseñar un módulo de ciberseguridad supone, por tanto, avanzar hacia un modelo de formación basado en competencias profesionales integradas, en el que el alumnado no solo adquiera conocimientos instrumentales, sino también capacidades para analizar, prevenir y mitigar riesgos tecnológicos.

En términos de impacto social y educativo, la justificación del módulo se sostiene además en la necesidad de formar profesionales digitalmente competentes, críticos y éticamente responsables, capaces de garantizar la seguridad de los sistemas, la protección de datos y el cumplimiento normativo (GDPR, LOPDGDD, ENS), la ciberseguridad, entendida como componente de la ciudadanía digital, se convierte así en un eje vertebrador del aprendizaje para la vida y el trabajo en la sociedad del conocimiento.

Objetivos del estudio

El objetivo general de esta comunicación es presentar el proceso de diseño del módulo formativo "Metodologías Aplicadas de Ciberseguridad", desarrollado en colaboración entre instituciones educativas y agentes empresariales del ámbito TIC, como una experiencia de innovación curricular orientada a la mejora de la calidad de la Formación Profesional.

De este propósito general se derivan los siguientes objetivos específicos:

1. Diagnosticar las necesidades formativas en materia de ciberseguridad identificadas por el sector empresarial vinculado al desarrollo web.
2. Analizar los referentes normativos, curriculares y de cualificación profesional para fundamentar el diseño del módulo.
3. Diseñar la estructura pedagógica y los resultados de aprendizaje del módulo, integrando marcos de referencia internacionales en seguridad y desarrollo seguro (*OWASP*, *DevSecOps*, *Secure SDLC*).
4. Validar el diseño curricular mediante la consulta y participación de expertos procedentes de centros de excelencia en ciberseguridad y empresas del *Cluster TIC de Asturias*.
5. Contribuir al debate académico sobre la incorporación de la ciberseguridad como competencia transversal en la educación técnica superior.

El artículo que se presenta, por lo tanto, no aborda la implementación ni la evaluación de resultados de aprendizaje, sino que se centra en la fase de diseño curricular y su fundamentación teórica, metodológica e institucional como punto de partida para futuras experiencias de innovación educativa.

2. Revisión de fuentes documentales

2.1. Marco teórico: la ciberseguridad como competencia transversal en la educación técnica

En las dos últimas décadas, la ciberseguridad ha pasado de ser un campo especializado de la ingeniería informática a convertirse en una competencia transversal de carácter estratégico en todos los ámbitos del conocimiento. Diversos organismos internacionales, como la Unión Europea, la UNESCO y la OCDE, han subrayado la necesidad de integrar la ciberseguridad en los sistemas educativos, no solo como una competencia técnica, sino también ética, social y ciudadana, vinculada a la alfabetización digital avanzada (Comisión Europea, 2023; UNESCO, 2022).

En el contexto europeo, documentos como el European Digital Competence Framework (DigComp 2.2) (Vuorikari et al., 2022) definen la ciberseguridad como una de las dimensiones esenciales de la competencia digital, articulada en torno a la protección de datos personales, la gestión de riesgos, la identidad digital y la seguridad en línea. Este marco promueve una visión integral de la seguridad que trasciende el conocimiento instrumental y fomenta una cultura de prevención y responsabilidad compartida.

Asimismo, la Agenda Europea de Capacidades 2020 y el programa Erasmus+ Sector Skills Alliances reconocen que la seguridad digital es una prioridad en el desarrollo de las competencias profesionales del futuro (Comisión Europea, 2020). En este marco, el proyecto European Software Skills Alliance (ESSA, 2023–2027) constituye un referente central, al establecer un modelo colaborativo entre instituciones educativas, organismos públicos y empresas para la formación, mejora y recapacitación (reskilling) en competencias de software y ciberseguridad. España participa en esta alianza a través de la representación del *Cluster TIC Asturias*, lo que sitúa esta experiencia en sintonía con las políticas europeas de innovación educativa y desarrollo profesional.

Desde una perspectiva pedagógica, la inclusión de la ciberseguridad en los programas de Formación Profesional se alinea con las teorías contemporáneas de la formación basada en competencias (Tobón, 2013; Zabalza, 2021). Este enfoque considera que el aprendizaje técnico debe integrarse con competencias cognitivas, socioemocionales y éticas, permitiendo al alumnado actuar de manera reflexiva en entornos laborales complejos. De este modo, el diseño curricular de un módulo de ciberseguridad no se limita a la transmisión de conocimientos tecnológicos, sino que promueve la capacidad de pensar y actuar con criterio de seguridad en contextos reales de desarrollo web.

Por otro lado, el concepto de seguridad desde el diseño (*security by design*) constituye un eje epistemológico central en la formación moderna de desarrolladores. Según el *Open Web Application Security Project (OWASP, 2021)*, la incorporación de la seguridad en todas las fases del ciclo de vida del software es una práctica esencial para garantizar la integridad, disponibilidad y confidencialidad de la información. Modelos como DevSecOps o Secure SDLC se han convertido en estándares de referencia para integrar la ciberseguridad en los procesos ágiles de desarrollo, y su comprensión resulta indispensable en la formación técnica avanzada (Goues et al., 2022).

Finalmente, la relación entre ciberseguridad y ética profesional ha adquirido un papel creciente en el debate educativo. Autores como Floridi (2016) o Bynum (2019) sostienen que la seguridad no puede entenderse solo como protección técnica, sino también como garantía de derechos digitales y expresión de una ciudadanía responsable. Por ello, la educación en ciberseguridad debe incluir la reflexión crítica sobre la privacidad, la transparencia algorítmica y los impactos sociales de la inteligencia artificial.

2.2. Revisión empírica: innovación curricular y colaboración entre educación–empresa

En el ámbito empírico, la literatura reciente evidencia la importancia de los modelos de colaboración entre instituciones educativas y el sector empresarial para el diseño de programas formativos adaptados a las necesidades del mercado digital (Álvarez-Arregui & Rodríguez, 2020; OCDE, 2021). Estos modelos de *triple hélice* —educación, empresa y Administración Pública— favorecen la transferencia de conocimiento y la actualización continua de las competencias profesionales (Etzkowitz & Leydesdorff, 2000).

Diversos estudios han mostrado que la participación de empresas tecnológicas en procesos de diseño curricular incrementa la pertinencia y empleabilidad de la formación profesional (European Centre for the Development of Vocational Training [CEDEFOP], 2021). En el caso español, experiencias como los Centros de Excelencia en Formación Profesional o los Nodos de Talento y Ciberseguridad impulsados por los clústeres autonómicos demuestran la efectividad de estas alianzas para la innovación educativa. Estos espacios de cooperación permiten identificar brechas formativas reales y adaptar los contenidos curriculares a los estándares de seguridad más recientes (López & García, 2023).

El diseño del módulo *Metodologías Aplicadas de Ciberseguridad* se nutre precisamente de esta lógica colaborativa. A lo largo de 2024, el *Cluster TIC Asturias* articuló un proceso participativo con centros de excelencia en Formación Profesional (IES Valle del Jerte y CIFP Avilés) y empresas especializadas en desarrollo web y ciberseguridad (Inetum, DXC Technology, Futuver, Ricoh, Asac, entre otras). La metodología incluyó reuniones iniciales, grupos focales y entrevistas individualizadas, orientadas a identificar las carencias formativas percibidas por el sector y los ámbitos prioritarios para la capacitación en desarrollo seguro de software.

Este enfoque se alinea con investigaciones previas sobre diseño participativo de currículos técnicos (Reyes et al., 2022; Sch-

midt et al., 2020), que destacan el valor de la cocreación *educativa* como estrategia de pertinencia, innovación y sostenibilidad. En tales modelos, el conocimiento experto de los docentes se complementa con la visión práctica del sector productivo, favoreciendo un currículo dinámico, contextualizado y orientado a la empleabilidad.

Asimismo, la integración de la inteligencia artificial (IA) en los procesos de desarrollo de software plantea nuevos retos para la formación profesional. La literatura reciente enfatiza la importancia de abordar los riesgos asociados a la automatización y a los sesgos algorítmicos desde la perspectiva de la seguridad (Goodman & Flaxman, 2023; Brundage et al., 2022). Por ello, el diseño del módulo incorpora la IA como tema de estudio transversal, en su doble dimensión: herramienta de detección de vulnerabilidades y objeto de análisis ético y técnico.

2.3. Síntesis del marco conceptual

De la revisión realizada se desprenden cuatro fundamentos conceptuales que orientan el diseño curricular del módulo:

1. Ciberseguridad como competencia transversal: más allá del conocimiento técnico, implica pensamiento crítico, responsabilidad ética y ciudadanía digital.
2. Aprendizaje basado en competencias profesionales: la formación debe integrar saberes técnicos, procedimentales y actitudinales, orientados a la resolución de problemas reales.
3. Colaboración interinstitucional como motor de innovación: la co-creación entre educación y empresa fortalece la pertinencia curricular.
4. Integración tecnológica y adaptación continua: los marcos internacionales (ESSA, DigComp, OWASP) orientan la actualización constante de los contenidos y metodologías.

Estos pilares configuran el marco teórico-empírico sobre el cual se estructura el diseño del módulo de Metodologías Aplicadas de Ciberseguridad, cuya descripción metodológica se desarrolla en el siguiente apartado.

3. Diseño de la investigación / innovación educativa

3.1. Enfoque metodológico general

El diseño del módulo *Metodologías Aplicadas de Ciberseguridad* se concibe como una innovación educativa de carácter colaborativo, orientada a la construcción de un currículo relevante, contextualizado y alineado con las necesidades del sector productivo. Se enmarca en la tradición de la investigación-acción participativa (IAP) (Kemmis & McTaggart, 1988; Elliott, 1993), aplicada al ámbito del diseño curricular en Formación Profesional. Esta elección metodológica responde a la doble finalidad del proyecto: generar conocimiento educativo y producir una propuesta formativa que responda a demandas reales del entorno laboral.

Desde esta perspectiva, la investigación no se limita a un análisis descriptivo, sino que constituye un proceso cíclico y reflexivo de diagnóstico, diseño, validación y mejora. El enfoque combina métodos cualitativos —entrevistas, grupos focales, análisis documental— con una sistematización de información proveniente de fuentes institucionales y normativas. El resultado no es un producto cerrado, sino un diseño susceptible de evolución y actualización conforme a los cambios tecnológicos y formativos.

El proyecto se articula en torno a cuatro fases metodológicas:

1. Diagnóstico y contextualización: identificación de necesidades formativas y revisión de referentes europeos y nacionales.
2. Diseño curricular participativo: elaboración de la estructura del módulo a partir de reuniones con agentes educativos y empresariales.
3. Validación experta: contraste del diseño con profesionales y especialistas en ciberseguridad y desarrollo web.
4. Sistematización y formalización del módulo final, ajustado a los marcos normativos del sistema de Formación Profesional español y europeo.

3.2. Participantes

El proceso de diseño involucró tres grupos principales de actores:

- Centros de Excelencia de Formación Profesional en Ciberseguridad:
  - *CIFP Avilés (Asturias)*, coordinado por Luis Miguel Lestón y Noelia Barreiro Braña.
  - *IES Valle del Jerte (Extremadura)*, con la participación de César Fernández Obaya, Carlos [Coordinador General], y otros responsables de proyectos de excelencia.

  Estos centros aportaron el conocimiento pedagógico y didáctico necesario para la definición de los resultados de aprendizaje, las metodologías y los criterios de evaluación del módulo.
- Cluster TIC Asturias y Nodo de Ciberseguridad:
- Representados por Enrique Jáimez (Director General), Roberto Bayón (responsable técnico del Nodo de Ciberseguridad) y Lucía Menéndez (responsable del Nodo de Talento). Su papel fue articular la colaboración con el tejido empresarial y facilitar la conexión con proyectos europeos como *ESSA*.
- Empresas participantes en el grupo focal:
  Se seleccionaron seis empresas con experiencia en el desarrollo de software seguro y sensibilidad hacia la formación de nuevos profesionales: Inetum, DXC Technology, Futuver Consulting, Ricoh España, Ewala y Asac Comunicaciones. En total, participaron 14 personas, entre directores de sistemas, desarrolladores senior, responsables de producto y gestores de proyectos.

Este conjunto de participantes conformó una comunidad de práctica interinstitucional, donde convergieron visiones educativas, técnicas y organizacionales. La heterogeneidad de perfiles fue esencial para garantizar una comprensión holística de las necesidades del sector.

3.3. Muestra y contexto

El contexto institucional de la investigación corresponde a la Formación Profesional de Grado Superior en Desarrollo de Aplicaciones Web (DAW), en el marco del sistema educativo español. El diseño del módulo se dirige al alumnado de segundo curso, en la fase final del itinerario formativo, y tiene una duración prevista de 80 horas lectivas. El carácter optativo del módulo permite introducir contenidos emergentes sin alterar el tronco común de los títulos oficiales.

La muestra informativa del proceso de diseño se conformó por:

- 2 centros educativos de excelencia en FP.
- 6 empresas tecnológicas.
- 14 expertos (académicos, formadores y técnicos en ciberseguridad).
- 1 entidad intermedia (Cluster TIC Asturias).

El ámbito geográfico abarca las comunidades de Asturias y Extremadura, representativas de dos ecosistemas de innovación en FP con fuerte orientación hacia la digitalización y el empleo tecnológico.

3.4. Instrumentos de recogida de información

Para la obtención de datos y opiniones se emplearon los siguientes instrumentos:

1. Análisis documental: revisión de currículums oficiales, cualificaciones del INCUAL relacionadas y marcos europeos de competencias digitales y de ciberseguridad.
2. Reuniones iniciales de planificación: celebradas en mayo de 2024 por videoconferencia, con los equipos de los Centros de Excelencia y el Cluster TIC. Se elaboró una ficha de contenidos estratégicos para orientar la consulta empresarial.
3. Focus Group con empresas del sector TIC: realizado el 22 de mayo de 2024 en las oficinas del Cluster TIC de Asturias. Se utilizó un panel colaborativo para sistematizar las aportaciones sobre las competencias necesarias, las tecnologías empleadas y las carencias detectadas en los titulados de Formación Profesional.
4. Entrevistas individuales con expertos empresariales: efectuadas entre el 31 de mayo y el 20 de junio de 2024, orientadas a validar el esquema preliminar del módulo y complementar la información del grupo focal.
5. Instrumento de validación curricular: cuestionario estructurado con ítems sobre la pertinencia, claridad, aplicabilidad y coherencia de los contenidos propuestos, administrado a los participantes en la validación final.

Estos instrumentos permitieron triangular la información obtenida, garantizando la fiabilidad y validez del proceso de diseño.

3.5. Procedimiento

El proceso se desarrolló en tres fases principales:

1. Fase 1: Diagnóstico inicial (abril–mayo 2024)
   Se revisaron documentos estratégicos europeos (ESSA, DigComp, CEDEFOP) y se definió el propósito del módulo: capacitar al alumnado de Formación Profesional en el desarrollo seguro de software. A partir de esta revisión se elaboró un primer mapa de competencias técnicas y transversales relacionadas con la ciberseguridad.
2. Fase 2: Diseño participativo del módulo (mayo 2024)
   A través del *focus group*, se identificaron las áreas clave que debía abordar el módulo: amenazas y vulnerabilidades, buenas prácticas de programación segura, cumplimiento normativo (GDPR, ENS), herramientas de *testing* de seguridad, y fundamentos de inteligencia artificial aplicada a la seguridad del software. Con estas aportaciones se construyó un borrador de programa formativo articulado en siete bloques temáticos.
3. Fase 3: Validación experta (junio 2024) Los borradores fueron revisados mediante reuniones con profesionales de DXC Technology, Inetum y Asac Comunicaciones. Estas validaciones permitieron ajustar el nivel de dificultad, eliminar contenidos demasiado avanzados (como seguridad en contenedores), e incorporar referencias a certificaciones y estándares reconocidos (AENOR, CCN-STIC).

3.6. Resultados del diseño curricular

El diseño final del módulo se estructuró con los siguientes componentes formativos:

- Título: *Metodologías Aplicadas de Ciberseguridad*
- Duración: 80 horas
- Tipo: Módulo optativo para el Ciclo Formativo de Grado Superior en Desarrollo de Aplicaciones Web
- Competencia general: Aplicar metodologías, herramientas y marcos de referencia de ciberseguridad en el proceso de desarrollo de aplicaciones web, garantizando la protección de datos, la integridad del software y la conformidad con las normativas vigentes.

Resultados de aprendizaje (RA) principales:

1. Comprender la importancia de la ciberseguridad en el desarrollo web.
2. Aplicar los principios de desarrollo seguro a lo largo del ciclo de vida del software.
3. Identificar vulnerabilidades y los riesgos habituales en las aplicaciones web.
4. Utilizar herramientas de análisis y validación de seguridad (p. ej., OWASP ZAP, SonarQube).
5. Emplear frameworks y estándares de seguridad (Spring Security, OAuth 2.0).
6. ntroducir la inteligencia artificial en el análisis y la detección de vulnerabilidades.
7. Realizar una práctica integradora de revisión de seguridad sobre un proyecto existente.

Metodología didáctica sugerida: aprendizaje basado en proyectos, análisis de casos, simulaciones de incidentes de seguridad y trabajo colaborativo. Evaluación: rúbricas de desempeño, portafolio técnico y pruebas prácticas.

3.7. Consideraciones éticas y de calidad

El proceso de diseño se desarrolló respetando principios éticos de transparencia, confidencialidad y participación voluntaria. Las aportaciones de los profesionales fueron utilizadas exclusivamente con fines de mejora educativa. El proyecto, al centrarse en el diseño y no en la implementación, no implicó intervención directa sobre el alumnado ni recogida de datos personales, por lo que no requirió autorización ética formal.

Se garantizó la trazabilidad y documentación de cada decisión curricular, conforme a los criterios de calidad educativa definidos por los Centros de Excelencia de FP y el *Cluster TIC Asturias*.

4. Análisis de datos

4.1. Estrategia de análisis

La información obtenida a través de reuniones, grupos focales, entrevistas y documentos fue analizada mediante un enfoque de análisis de contenido temático (Bardin, 2013), orientado a identificar las categorías conceptuales emergentes que dieron forma al diseño del módulo. La triangulación de fuentes —documentales, institucionales y testimoniales— permitió establecer convergencias y divergencias entre las percepciones del ámbito educativo y las demandas del sector empresarial.

El procedimiento analítico se desarrolló en tres fases:

1. Codificación inicial: segmentación de la información en unidades significativas relacionadas con competencias, necesidades formativas y prácticas de seguridad.
2. Agrupación temática: clasificación de las unidades en categorías conceptuales (por ejemplo, *competencias técnicas*, *normativas y estándares*, *aprendizaje práctico*, *ética y responsabilidad digital*).
3. Interpretación y síntesis: elaboración de matrices comparativas y mapas conceptuales que facilitaron la elaboración de conclusiones pedagógicas y curriculares.

Para la sistematización se utilizó una matriz de análisis que relacionaba los objetivos específicos del estudio con los resultados del trabajo de campo. La codificación fue revisada por dos investigadores del equipo de FP de excelencia, garantizando la fiabilidad entre evaluadores.

4.2. Categorías emergentes

Del análisis de la información se identificaron seis categorías principales que estructuraron los hallazgos del proceso de diseño:

a) Brecha competencial en ciberseguridad

Tanto los docentes como los representantes del sector TIC coincidieron en señalar que los titulados en *Desarrollo de Aplicaciones Web* poseen una sólida base en programación y gestión de bases de datos, pero carecen de formación específica en seguridad del software y análisis de riesgos. Esta carencia se manifiesta en prácticas poco seguras —validación deficiente de entradas, la ausencia de pruebas de penetración o el desconocimiento de los estándares OWASP—, lo cual genera dependencia de revisiones posteriores por parte de equipos especializados en ciberseguridad.

Esta constatación empírica refuerza la hipótesis inicial de la investigación: la necesidad de incorporar la ciberseguridad como competencia estructural y no como contenido complementario.

b) Relevancia del desarrollo seguro como práctica profesional

Las empresas participantes destacaron la urgencia de formar a futuros desarrolladores con una mentalidad *"secure by default"*. El concepto de desarrollo seguro fue recurrente en todos los discursos, vinculado al cumplimiento de normativas, la calidad del software y la reputación corporativa.

Los participantes mencionaron expresamente estándares y marcos de referencia como el OWASP Top 10, la ISO 27001, el Esquema Nacional de Seguridad (ENS) y las guías CCN-STIC, considerados pilares para la formación práctica.

c) Integración de la ciberseguridad en el ciclo de vida del software

De los análisis se desprende una fuerte convergencia entre los principios de DevSecOps y las metodologías ágiles de desarrollo. Las empresas señalaron que la seguridad debe estar presente desde la planificación hasta el mantenimiento del producto, fomentando una cultura de prevención continua.

Este enfoque se tradujo en la estructura modular del programa, donde cada bloque de contenidos responde a una fase del ciclo de vida del código (planificación, diseño, codificación, pruebas, despliegue y mantenimiento).

d) Importancia del aprendizaje experiencial y del trabajo con herramientas reales

El consenso entre todos los agentes fue que la enseñanza de la ciberseguridad requiere entornos prácticos simulados, que permitan experimentar con vulnerabilidades reales y emplear herramientas profesionales de análisis (p. ej., SonarQube, OWASP ZAP, Burp Suite).

Las estrategias de aprendizaje basadas en proyectos, retos y laboratorios virtuales fueron identificadas como las más eficaces para el desarrollo de competencias aplicadas.

e) Colaboración entre educación–empresa como estrategia de pertinencia

El análisis de las reuniones y entrevistas puso de relieve el valor del modelo de cooperación entre FP y el sector TIC. Los participantes resaltaron que esta interacción no solo mejora la pertinencia del currículo, sino que también favorece la actualización docente y la inserción laboral del alumnado.

Asimismo, la presencia del *Cluster TIC Asturias* como mediador institucional permitió estructurar la colaboración y generar confianza entre actores de distinta naturaleza (educativa y empresarial).

f) Nuevos retos asociados a la inteligencia artificial

La irrupción de la inteligencia artificial generativa fue identificada como un factor emergente con implicaciones directas en la seguridad del software.

Los participantes consideraron fundamental que los futuros desarrolladores comprendan los riesgos derivados del uso de IA en la programación automatizada, así como las posibilidades de su aplicación en la detección de vulnerabilidades. Esta categoría se incorporó como un bloque transversal dentro del diseño del módulo, destacando su dimensión técnica y ética.

4.3. Síntesis interpretativa

La convergencia entre las categorías permite identificar cuatro ejes de innovación que estructuran el diseño curricular del módulo:

1. Integración de la ciberseguridad en el currículo técnico de Formación Profesional, respondiendo a una necesidad detectada en la práctica empresarial y en las políticas europeas de cualificación digital.
2. Actualización metodológica del aprendizaje técnico, mediante estrategias activas centradas en la práctica, la resolución de problemas y la colaboración con el entorno profesional.
3. Vinculación institucional y corresponsabilidad educativa, que refuerza la cooperación entre escuelas de Formación Profesional, clústeres tecnológicos y empresas líderes.
4. Inclusión de perspectivas emergentes, como la inteligencia artificial y la ética digital, que amplían la visión tradicional de la ciberseguridad hacia un enfoque más integral y humano.

El análisis evidencia que el proceso de diseño no solo generó un programa curricular pertinente, sino también una comunidad de aprendizaje interinstitucional, capaz de producir conocimiento aplicado y transferible a otros contextos educativos.

4.4. Validación del diseño

La validación experta confirmó la solidez del enfoque adoptado. Los especialistas coincidieron en valorar positivamente:

- La claridad de los resultados de aprendizaje.
- La coherencia entre las competencias, los contenidos y los criterios de evaluación.
- La incorporación de referencias internacionales reconocidas (OWASP, AENOR, ENS).

Las sugerencias más significativas se centraron en:

- Reducir la complejidad de los contenidos sobre seguridad en contenedores, al considerarse demasiado avanzados para el alumnado en formación inicial.
- Incluir mayor énfasis en aspectos de comunicación y gestión de incidencias, considerados fundamentales para el trabajo en equipo.
- Potenciar la evaluación formativa mediante portafolios y autoevaluaciones, coherentes con las tendencias actuales en enseñanza técnica.

En conjunto, el proceso de análisis permitió depurar y afinar la propuesta, garantizando su viabilidad pedagógica y su relevancia profesional antes de pasar a las fases de aprobación e implementación.

5. Resultados más relevantes

5.1. Consolidación de un modelo de colaboración interinstitucional

Uno de los resultados más destacados del proceso de diseño ha sido la consolidación de una red colaborativa entre el ámbito educativo y el sector empresarial TIC. La participación activa de los Centros de Excelencia de Formación Profesional, junto con el *Cluster TIC Asturias* y las empresas tecnológicas, ha permitido construir un modelo de diseño curricular cooperativo, alineado con el paradigma de la *triple hélice* (Etzkowitz & Leydesdorff, 2000).

Este modelo ha demostrado que la innovación curricular no puede desarrollarse de manera aislada desde la institución educativa, sino que requiere una interacción continua con el entorno productivo, donde se generen espacios de diálogo, validación y transferencia de conocimiento.

La experiencia ha reforzado el papel del *Cluster TIC* como mediador entre ambos mundos, funcionando como un nodo de innovación educativa que traduce las necesidades del mercado en competencias formativas concretas.

Además, este enfoque colaborativo ha tenido un efecto multiplicador: los centros participantes han manifestado su intención de aplicar esta metodología de codiseño a otros módulos formativos, creando una cultura institucional de innovación compartida y aprendizaje organizacional.

5.2. Definición de un perfil de competencias actualizado

Otro resultado central ha sido la elaboración de un mapa de competencias en ciberseguridad adaptado al perfil profesional del *Técnico Superior en Desarrollo de Aplicaciones Web*. Este mapa integra competencias técnicas, metodológicas y actitudinales, organizadas en torno a cuatro dimensiones clave:

1. Competencias técnicas: manejo de herramientas de análisis y validación de seguridad, comprensión de estándares internacionales y aplicación de metodologías *DevSecOps*.
2. Competencias analíticas: capacidad para identificar riesgos, evaluar vulnerabilidades y priorizar medidas de mitigación.
3. Competencias ético-legales: comprensión del marco normativo de protección de datos (RGPD, LOPDGDD, ENS) y de los principios de responsabilidad digital.
4. Competencias transversales: trabajo en equipo, comunicación en entornos técnicos y toma de decisiones fundamentadas en la gestión de riesgos.

La construcción de este perfil competencial contribuye a reducir la brecha existente entre la formación académica y la práctica profesional, garantizando que los futuros egresados dispongan de los conocimientos y habilidades que demanda el sector tecnológico europeo.

5.3. Diseño curricular estructurado en bloques de aprendizaje

El producto final del proceso de diseño se tradujo en un currículo estructurado en seis bloques temáticos, articulados de forma progresiva y coherente con el ciclo de vida del software. Esta estructura favorece la comprensión secuencial de los contenidos y su aplicación práctica en entornos de desarrollo real.

Bloque	Eje formativo principal	Contenidos y enfoques destacados
1	Fundamentos de ciberseguridad en el desarrollo web	Principios de confidencialidad, integridad y disponibilidad; análisis de riesgos y modelos organizativos de seguridad.
2	Desarrollo seguro en el ciclo de vida del código	Metodologías de referencia (*Secure SDLC*, *DevSecOps*), prácticas de codificación segura y revisión de código.
3	Gestión y mitigación de vulnerabilidades	Estudio del *OWASP Top 10*, estrategias de detección y mitigación, y pruebas de penetración básicas.
4	Herramientas de análisis y validación de seguridad	Uso de SonarQube, OWASP ZAP y otras herramientas de pruebas de seguridad.
5	Frameworks y estándares de seguridad	Implementación de Spring Security, OAuth 2.0, y referencias a ISO 27001 y ENS.
6	Inteligencia artificial y seguridad	Aplicaciones de IA en la detección de vulnerabilidades, sesgos y riesgos éticos de la automatización.

Tabla 1. Bloques, ejes y contenidosdel curriculo

Cada bloque está asociado a resultados de aprendizaje verificables y criterios de evaluación claros, orientados a la adquisición de competencias demostrables.

El diseño enfatiza el aprendizaje activo mediante proyectos, retos y resolución de casos reales, coherente con la tendencia europea hacia la *work-based learning* (CEDEFOP, 2022).

5.4. Innovación metodológica: aprendizaje basado en retos

El proceso de análisis y consulta llevó a consensuar una metodología de enseñanza centrada en el aprendizaje basado en retos (ABR) y el aprendizaje colaborativo. Estas metodologías permiten conectar los contenidos de ciberseguridad con contextos reales de desarrollo web, donde el alumnado debe analizar problemas, tomar decisiones técnicas y justificar sus soluciones de manera argumentada.

El ABR facilita, además, la integración de las dimensiones técnica y ética de la ciberseguridad, al plantear dilemas y situaciones en las que deben considerarse las consecuencias sociales y legales de las decisiones tecnológicas.

Los participantes del sector empresarial valoraron especialmente esta orientación, al considerarla coherente con los entornos laborales donde la resolución de incidentes exige no solo conocimiento técnico, sino también juicio crítico y trabajo en equipo.

5.5. Sistematización de un procedimiento replicable

El trabajo conjunto permitió definir una metodología replicable para el diseño curricular en Formación Profesional, aplicable a otros ámbitos tecnológicos. Este procedimiento incluye:

1. Análisis documental y diagnóstico de necesidades del sector.
2. Consulta participativa con empresas y expertos.
3. Diseño preliminar del currículo basado en competencias.
4. Validación técnica y pedagógica por agentes externos.
5. Elaboración de la versión final del módulo conforme a estándares nacionales (INCUAL) y europeos (EQF).

Este procedimiento se constituye como una buena práctica en innovación educativa, alineada con los principios del *European Quality Assurance in Vocational Education and Training (EQAVET)*, que promueve la calidad mediante la participación de los agentes interesados.

5.6. Contribución al desarrollo profesional docente

Otro resultado relevante, aunque indirecto, ha sido el fortalecimiento de las competencias pedagógicas y digitales del profesorado participante.

Los equipos docentes de los Centros de Excelencia señalaron que el trabajo conjunto con expertos en ciberseguridad les permitió actualizar sus conocimientos técnicos, acceder a documentación profesional y mejorar sus estrategias didácticas.

En este sentido, el proyecto ha actuado como un espacio de formación docente continua y de construcción de conocimiento compartido, coherente con las recomendaciones europeas sobre *teacher digital competence* (Redecker & Punie, 2017).

5.7. Resultados de validación experta

La validación realizada por las empresas y especialistas permitió confirmar que el módulo diseñado responde adecuadamente a las competencias y perfiles demandados en el ámbito del desarrollo web seguro.

Las valoraciones cualitativas más destacadas fueron:

- "El esquema propuesto refleja con precisión los desafíos reales del desarrollo web seguro y las herramientas empleadas en la industria." (*J. Asenjo, DXC Technology*).
- "La integración de la IA y la reflexión ética es muy oportuna. "No solo necesitamos técnicos competentes, sino también desarrolladores responsables." (*J. S. Vázquez, Inetum*).
- "El enfoque práctico y modular permitirá una incorporación gradual del alumnado sin sobrecargar el currículo." (*A. Menéndez, Asac Comunicaciones*).

Estos testimonios evidencian la aceptación y legitimidad social del diseño, así como su potencial para ser adoptado en otros centros educativos o contextos formativos.

5.8. Impacto esperado

Aunque el módulo aún no haya sido implementado, el proceso de diseño anticipa varios impactos a corto y medio plazo:

- Mejora de la pertinencia curricular de la FP en el ámbito del desarrollo web.
- Creación de sinergias sostenibles entre educación y empresa.
- Potenciación de la empleabilidad del alumnado mediante competencias actualizadas.
- Fortalecimiento del ecosistema de innovación educativa regional, vinculado a la transformación digital y la seguridad tecnológica.

Estos resultados posicionan al proyecto como una experiencia pionera dentro de la red de Centros de Excelencia en FP y un modelo de referencia para políticas educativas orientadas a la digitalización segura.

6. Debate / Conclusiones

6.1. Reflexión general sobre el proceso de diseño

El proceso de diseño del módulo Metodologías Aplicadas de Ciberseguridad permite situar la innovación curricular en la Formación Profesional (FP) como una práctica de investigación aplicada y colaborativa, más que como una mera actualización técnica.

El análisis del proceso evidencia que la ciberseguridad, lejos de ser un área marginal o complementaria, debe constituirse en el eje estructural del currículo técnico, especialmente en los programas vinculados al desarrollo de software y la gestión de datos.

En coherencia con las políticas europeas (ESSA, DigComp, EQAVET), la experiencia demuestra que la formación en ciberseguridad requiere un enfoque sistémico que articule tres dimensiones:

- la pedagógica, que se centra en el desarrollo de competencias;
- la tecnológica, que garantiza la actualización de los contenidos; y
- la institucional, que impulsa la cooperación entre los distintos agentes.

Este triple enfoque genera un nuevo modelo de formación técnica que responde no sólo a la demanda de empleo, sino tam-

bién a la necesidad de una ciudadanía digital responsable, capaz de actuar éticamente en entornos digitales complejos.

6.2. La innovación curricular como proceso de co-creación

Uno de los principales aportes de este proyecto es la demostración empírica de que la innovación curricular puede concebirse como un proceso de co-creación interinstitucional.

El diseño del módulo no se limitó a incorporar contenidos técnicos de ciberseguridad, sino que integró una metodología de participación activa de empresas, docentes y expertos, consolidando un modelo que supera la lógica vertical de "currículo prescrito" y la sustituye por una lógica horizontal de "currículo construido".

Este cambio de paradigma es coherente con los planteamientos de Fullan (2020) sobre las alianzas para el cambio sistémico, donde la innovación educativa surge del diálogo entre contextos de conocimiento distintos.

La participación de las empresas en el diseño curricular no debe entenderse como subordinación del ámbito educativo al productivo, sino como una oportunidad para articular pertinencia y calidad. En este sentido, la colaboración con el Cluster TIC Asturias se constituye como una práctica de gobernanza compartida y como modelo transferible a otros sectores formativos.

6.3. Los desafíos epistemológicos y pedagógicos

El debate académico derivado de esta experiencia revelan varios retos que trascienden el ámbito de la ciberseguridad:

Integrar la seguridad como pensamiento y no solo como contenido.

La ciberseguridad implica un modo de pensar el desarrollo tecnológico, basado en la anticipación, la prevención y la ética. Enseñarla requiere, por tanto, fomentar el pensamiento sistémico y la toma de decisiones responsable.

Equilibrar la complejidad técnica y la accesibilidad didáctica.

Diseñar un módulo en un ámbito tan especializado exige encontrar un equilibrio entre la profundidad conceptual y la comprensibilidad para estudiantes de Formación Profesional, evitando tanto la superficialidad como la sobrecarga cognitiva.

Desarrollar competencias docentes en seguridad digital.

El papel del profesorado es central en este proceso. No basta con dotar de materiales y guías: es necesario fortalecer la competencia digital docente (Redecker & Punie, 2017), especialmente en los ámbitos de programación segura, análisis de riesgos y ética tecnológica.

Evaluar la innovación más allá del rendimiento.

En coherencia con los principios de EQAVET, la evaluación de la innovación curricular debe incorporar indicadores de relevancia, impacto y sostenibilidad, más allá de los resultados inmediatos del aprendizaje.

6.4. Contribución al debate sobre la educación técnica y la sociedad digital

El diseño del módulo aporta evidencias relevantes para el debate sobre el papel de la educación técnica en la sociedad digital.

Primero, muestra que la Formación Profesional puede ser un espacio de investigación educativa aplicada, capaz de generar conocimiento y modelos exportables.

Segundo, refuerza la idea de que la educación en ciberseguridad es también educación en valores democráticos, al promover la protección de datos, la integridad digital y la responsabilidad profesional.

Tercero, consolida la noción de competencia digital ampliada, donde la seguridad no es un contenido aislado, sino una competencia integrada en la práctica profesional y la ciudadanía.

De este modo, la ciberseguridad se presenta como un constructo educativo multidimensional: técnico, ético, jurídico y social. Su enseñanza requiere una pedagogía que combine el saber hacer con el saber ser y el saber convivir, en línea con los principios de la UNESCO sobre la educación para el desarrollo sostenible (UNESCO, 2022).

6.5. Limitaciones del estudio

Este trabajo reconoce varias limitaciones derivadas de su naturaleza y alcance:

- El proceso se circunscribe a la fase de diseño, sin haberse implementado ni evaluado el módulo en un entorno real de aprendizaje.
- La muestra de participantes, aunque diversa, se concentra en un número limitado de empresas y centros educativos, por lo que los resultados deben interpretarse con cautela.
- La rápida evolución tecnológica puede requerir actualizaciones periódicas del contenido y de las herramientas propuestas.

Estas limitaciones no menoscaban el valor del estudio, sino que señalan las líneas futuras de investigación y mejora, orientadas a la validación empírica del módulo mediante su implementación piloto y la medición de su impacto formativo.

6.6. Conclusiones finales

A partir del análisis realizado, pueden extraerse las siguientes conclusiones principales:

- El diseño del módulo de Metodologías Aplicadas de Ciberseguridad constituye una innovación curricular significativa en la Formación Profesional española, al integrar la seguridad como competencia estructural y transversal del desarrollo web.
- El modelo de co-creación interinstitucional demuestra que la colaboración entre centros educativos, clústeres tecnológicos y empresas incrementa la pertinencia y la calidad del currículo.
- La formación en ciberseguridad debe concebirse como una educación para la ciudadanía digital, articulando conocimientos técnicos con responsabilidad ética y social.
- El proceso de diseño ha permitido generar un modelo metodológico replicable en otros ámbitos de la Formación Profesional, basado en la investigación participativa, la validación experta y la mejora continua.
- La experiencia confirma que la innovación educativa sostenible surge de la alianza entre el conocimiento pedagógico y la práctica profesional, en coherencia con los principios de la educación superior como referente cultural y científico del siglo XXI (RIAICES, 2025).

Fuentes documentales

Álvarez-Arregui, E. (2017). *Proyecto Docente de Didáctica y Organización.* Inédito. Universidad de Oviedo.

Álvarez-Arregui, E. (2021). *Ecosistemas de innovación educativa y desarrollo sostenible*. CIDIPA.

Álvarez-Arregui, E. (2022). Avances en investigación transdisciplinar. *Revista Riaices, 4, 1*, 1-4.

Álvarez-Arregui, E. y Menéndez-Menéndez, L. (2023). Teoría y práctica de la innovación educativa. *Riaices, 5.* https://doi.org/10.17811/ria.5.1.2023

Álvarez-Arregui, E., Menéndez-Menéndez, L., Álvarez Martínez-Cué, M.M. y Arreguit, X. (2022). Continuing Education as a Universal Right to Adapt to a Working Environment in Accelerated Change. *Revista Derechos Humanos y Educación. 5*, 45-68

Álvarez-Arregui, E.; Rodríguez-Fernández, C.; González-Melgar, C. y Rodríguez-Martín, A. (2024). *El ADN del desarrollo personal, profesional, institucional y comunitario. La formación continua.* Ediuno.

Álvarez-Arregui, E.Rodríguez-Martín, A. y Rodríguez-Fernández, C. (2024). *¿Innovar para adaptarse? O ¿Innovar para mejorar? Instituciones socioeducativas sostenibles que aprenden a aprender emprendiendo.* Ediuno.

Álvarez-Arregui, E. y Arreguit, X. (2022). La universidad en evolución: Construyendo alianzas interinstitucionales y multidisciplinares a través de proyectos sostenibles y responsables. *International Journal of Human Sciences Research, 2*, 1-17

Bardin, L. (2013). *Análisis de contenido* (2.ª ed.). Akal.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2022). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv preprint. https://arxiv.org/abs/1802.07228

Bynum, T. W. (2019). *Computer and information ethics*. Cambridge University Press. https://doi.org/10.1017/9781108681161

CEDEFOP. (2022). *Work-based learning: Relevance and quality in vocational education and training*. Publications Office of the European Union. https://www.cedefop.europa.eu/en/publications/4208

Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From National Systems and "Mode 2" to a Triple Helix of university–industry–government relations. *Research Policy, 29*(2), 109–123. https://doi.org/10.1016/S0048-7333(99)00055-4

European Commission. (2020). *European Skills Agenda for sustainable competitiveness, social fairness and resilience*. Publications Office of the European Union. https://ec.europa.eu/social/main.jsp?catId=1223

European Commission, Joint Research Centre. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes* (JRC128415). Publications Office of the European Union. https://doi.org/10.2760/115376

Floridi, L. (2016). *The ethics of information*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199641321.001.0001

Fullan, M. (2020). *All systems go: The change imperative for whole system reform*. Corwin Press.

Goodman, B., & Flaxman, S. (2023). European and UK frameworks for AI governance: A review of executive frameworks. *AI & Society, 38*(3), 897–910. https://doi.org/10.1007/s00146-022-01523-1

Goues, C., Devanbu, P., & Ko, A. J. (2022). Integrating security into agile development: A DevSecOps approach. *Software Quality Journal, 30*(1), 67–85. https://doi.org/10.1007/s11219-021-09562-5

Kemmis, S., & McTaggart, R. (1988). *The action research planner* (3rd ed.). Deakin University Press.

López, M., & García, P. (2023). Buenas prácticas en la formación profesional para la ciberseguridad: el papel de los *clusters* tecnológicos. *Revista de Innovación Educativa Técnica, 12*(3), 45–60.

OECD. (2021). *Skills for a digital world: Policy directions and evidence*. OECD Publishing. https://doi.org/10.1787/9789264279583-en

Open Web Application Security Project (OWASP). (2021). *OWASP Top 10 – 2021: The ten most critical web application security risks*. https://owasp.org/Top10/

Redecker, C., & Punie, Y. (2017). *European framework for the digital competence of educators (DigCompEdu)*. Publications Office of the European Union. https://doi.org/10.2760/159770

Reyes, J., Martínez, A., & Sánchez, R. (2022). Diseño participativo de currículos técnicos en la formación profesional: estudio de caso. *Educación Técnica y FP, 6*(1), 23–41. https://revistas.um.es/educacion-tecnica/article/view/526721

Tobón, S. (2013). *Formación basada en competencias: Pensamiento complejo, diseño curricular y didáctica*. ECOE Ediciones. https://www.ecoeediciones.com/libro/formacion-basada-en-competencias

UNESCO. (2022). *Reimagining our futures together: A new social contract for education*. UNESCO Publishing. https://unesdoc.unesco.org/ark:/48223/pf0000379707

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2 Annex 2: Citizens interacting with AI systems*. Publications Office of the European Union. https://data.europa.eu/doi/10.2760/115376

Zabalza, M. A. (2021). *Las competencias profesionales en la formación profesional: Innovación curricular y retos pedagógicos*. Octaedro. https://octaedro.com/libro/las-competencias-profesionales-en-la-formacion-profesional