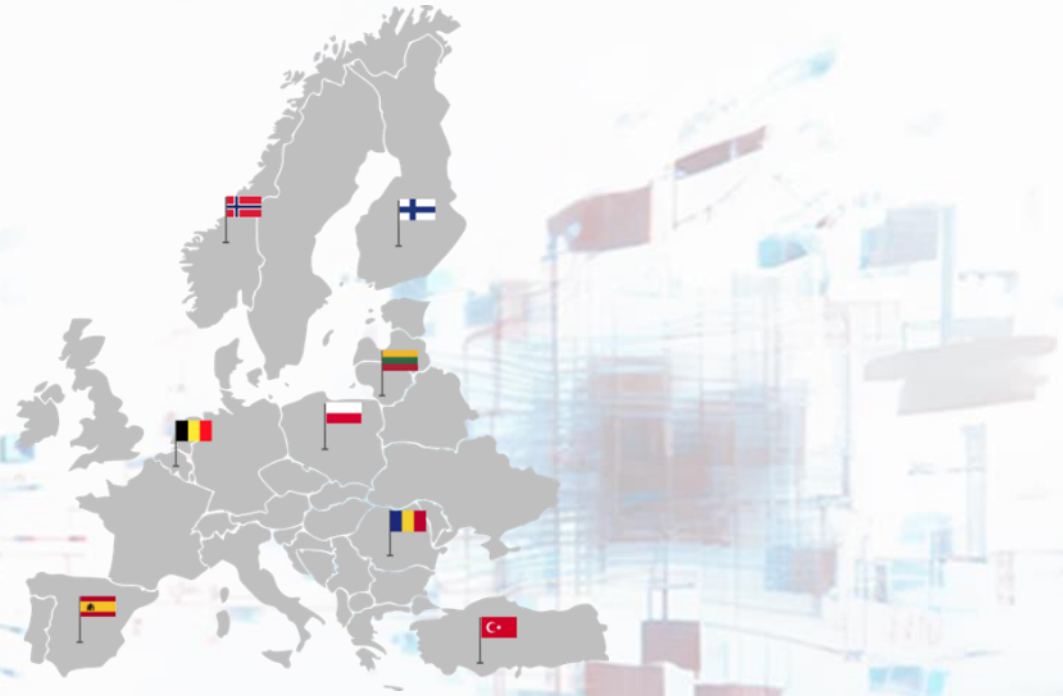
Co-funded by the European Union

ESTRUCTURA DEL ITINERARIO DE APRENDIZAJE DE LOS Y LAS AGENTES DEL CAMBIO EN LA CIBERSEGURIDAD DE LAS PYMES

CIBERAGENTE 06.2024

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Financiado por la Unión Europea. Las opiniones y puntos de vista expresados solo comprometen a su(s) autor(es) y no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea ni la EACEA pueden ser considerados responsables de ellos.



Paquete de trabajo 2: Enfoque y diseño de la estructura de CyberAgent

Entregable 2.3: Estructura del itinerario de aprendizaje de los y las agentes del cambio en la ciberseguridad para las PYMES

Líder del WP2 - Olemisen Balanssia ry
Responsable del paquete de trabajo 2.3: Universidad de Vilnius

CONTENIDO

ABREVIATURAS

CBL - Modelo de aprendizaje basado en retos

CL - Modelo de aprendizaje cooperativo

CE - Comisión Europea

ECTS - Sistema Europeo de Transferencia y Acumulación de Créditos

MEC - Marco Europeo de Cualificaciones

GICL - Modelo de aprendizaje colaborativo de investigación guiada

IES - Instituciones de Educación Superior

PBL - Modelo de aprendizaje basado en proyectos

POGIL - Modelo de aprendizaje por investigación guiada orientado a procesos

PYMES - Pequeñas y medianas empresas

EFP - Instituciones de Formación Profesional

LISTA DE CIFRAS

LISTA DE CUADROS

INTRODUCCIÓN

El objetivo general de este informe es desarrollar y describir nuevos itinerarios de aprendizaje profesional para mejorar las competencias en ciberseguridad de las personas empleadas en las PYMES (pequeñas y medianas empresas) europeas.

Sobre la base de los resultados del mapeo de las necesidades de formación de los y las Agentes de Cambio de la Ciberseguridad de las PYMES, se identificaron recursos externos para el análisis de los resultados del aprendizaje en términos de conocimientos, habilidades y competencias. Tras el análisis de los resultados de aprendizaje identificados, este informe proporciona orientación sobre dos tipos de planes de estudios de formación de nivel 4 a 6 del MEC (Marco Europeo de Cualificaciones) para cubrir la gama de habilidades y conocimientos necesarios para los grupos destinatarios del proyecto, personas empleadas de PYMES y estudiantes, y adaptar los resultados de la formación a los diferentes antecedentes y perfiles del alumnado.

- El nivel 4-5 del MEC se aplicará a las personas empleadas de las PYMES que no tengan formación de enseñanza superior, así como a los estudios de EFP (educación y formación profesional). Este nivel proporcionará las competencias y conocimientos básicos en ciberseguridad con una ligera especialización en algunos módulos.
- El nivel 5-6 del MEC, que será una oferta para las personas empleadas de las PYME que también tengan la formación adecuada para seguirlo y para los y las estudiantes de las IES (Instituciones de Educación Superior). En ese nivel se realizarán actividades de formación más avanzadas y complejas.

Se decidió actualizar los niveles del MEC a 4-6 no sólo para cubrir una amplia gama de resultados de aprendizaje, como se ha mencionado anteriormente, sino también para permitir una pasarela entre los planes de estudios y la mejora de las cualificaciones para las personas estudiantes de EFP y empleadas, poder pasar del nivel 4 para alcanzar el nivel 6.

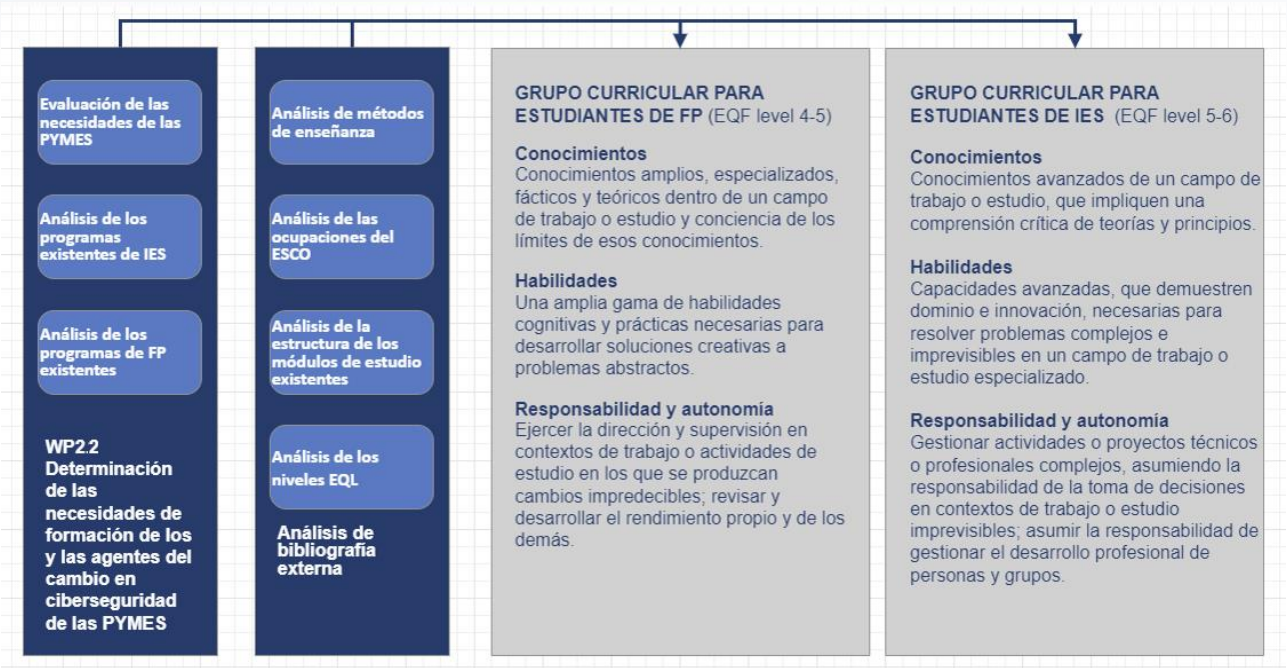


Figura 1. Un diagrama ilustrativo, que sigue las directrices de la CE, muestra los ocho niveles del MEC, proporcionando una representación visual del marco educativo.[1]

El plan de estudios aborda los resultados del aprendizaje y la necesidad de formar a las personas empleadas de las PYMES para que adquieran las competencias necesarias para desempeñar el papel de agentes del cambio en la ciberseguridad de las PYMES y de educar a los y las estudiantes de IES y FP para que desempeñen este papel una vez finalizados sus estudios. Cada plan de estudios consta de ocho módulos que abarcan cuatro subtemas:

- Conocimientos técnicos - Conocimientos actualizados sobre las amenazas a la ciberseguridad y las cuestiones jurídicas relacionadas - Conocimientos prácticos sobre cómo hacer frente a las amenazas a la ciberseguridad.
- Capacidad analítica - Mentalidad de pensamiento crítico - Capacidad para analizar y comprender las amenazas locales, cómo se producen, las personas en situación de riesgo, etc.
- Gestión de riesgos - Aprender a dotar a los lugares de trabajo de las PYMES de rutinas de ciberseguridad y a describirlas - Crear su propio manual de ciberseguridad para PYMES en el lugar de trabajo y cómo realizar su seguimiento.
- Habilidades organizativas - Cómo implantar nuevas rutinas y formas de trabajar en ciberseguridad en los centros de trabajo de las PYMES; Cómo llevar a cabo el apoyo a los y las líderes en ciberseguridad.

Además, una parte fundamental de la creación de los itinerarios de aprendizaje para mejorar las competencias en ciberseguridad de las PYMES europeas es cómo se aplicarán las

[1] https://europa.eu/europass/en/description-eight-eqf-levels

microcredenciales. Deben hacer referencia a los resultados del aprendizaje (conocimientos, habilidades y competencias), el contenido del curso, la formación (conocimientos, habilidades y competencias), los elementos de gamificación, la duración y el número de ECTS (Sistema Europeo de Transferencia y Acumulación de Créditos). Para ajustarse a su finalidad, deben impartirse mediante el establecimiento de asociaciones entre las HEI con proveedores de EFP y empresas privadas del sector de la ciberseguridad.

Las microsecciones ofrecen a al alumnado más libertad para elegir módulos o partes de módulos y decidir qué nivel de certificado necesitan: certificados de participación o certificado de finalización de curso con prueba de certificación, es decir, prueba de que se ha completado el curso con la adquisición de una competencia específica. Los certificados de finalización de curso se expiden por superar la prueba final con una puntuación mínima del 75%, y los certificados de participación se expiden por asistir a formación presencial, semipresencial o en línea sobre temas/módulos específicos. Esta práctica no sólo aumenta la aplicabilidad y eficacia de la formación, sino que también estimula la motivación para el aprendizaje, proporcionando una clara perspectiva de valor para la carrera profesional y el desarrollo posterior de los y las participantes.

En general, este informe esboza unas guías detalladas para el desarrollo de módulos de Ciberagente, que incluyen el esquema de contenidos de los itinerarios de estudio y de carrera, las metodologías de formación y evaluación, y la hoja de ruta para la elaboración de planes de estudios.

1. VÍA DE ESTUDIO

Un itinerario de aprendizaje es un viaje completo que la persona participante realiza desde el momento en que se da cuenta de que necesita mejorar sus capacidades, iniciar y completar la formación, hasta el momento en que termina de aprender y empieza a aplicar los conocimientos recibidos. Hay 3 etapas en un itinerario de aprendizaje:

- Aprendizaje previo,
- Aprender,
- Post-aprendizaje.

La etapa de preaprendizaje se ilustra en la siguiente figura.

Figura 2. Itinerario de aprendizaje antes del inicio de los estudios

En el contexto de las PYMES, se puede seguir esta vía de aprendizaje/estudio. En la figura, la persona participante decide formarse o se ve influido por una campaña de sensibilización y adquiere una comprensión de los beneficios de la formación, las oportunidades y las carreras que puede adquirir tras la formación.

También se ha propuesto un itinerario de aprendizaje como módulo típico a través de la estructura EVA (Entornos Virtuales de Aprendizaje). Tras un análisis bibliográfico y varios proyectos en los que se aplica el principio de las microcredenciales [2], [3], [4] se propone que cada módulo de Ciberagente tenga una duración de 1-5 ECTS (cada ECTS equivale a 25-30 horas de

[2] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Hacia adelante y más allá en la educación: Concept of FLEXIBLE LEARNING PATHWAYS. En KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[3] https://argus-alliance.eu/call/argus-microcredential-development-f2f-workshop/

[4] **https://www.youtube.com/watch?v=ECH0VvHIyRI, https://ndma.lt/alta2023/**

carga de trabajo) y comience con una introducción para dividirse a continuación en temas, que son subtemas.

Al final de los temas, se ofrece un test de autoevaluación compuesto por varias preguntas. El material didáctico del módulo debe apoyar el estudio de 6-8 temas, en cada uno de los cuales hay 4-6 subtemas. El curso puede concluir con una prueba de conocimientos, que no es obligatoria. Esto ofrece a las personas empleadas de las PYMES y a las personas estudiantes de los centros de formación la posibilidad de adquirir y demostrar las competencias aprendidas en un módulo o parte de la formación específicos.

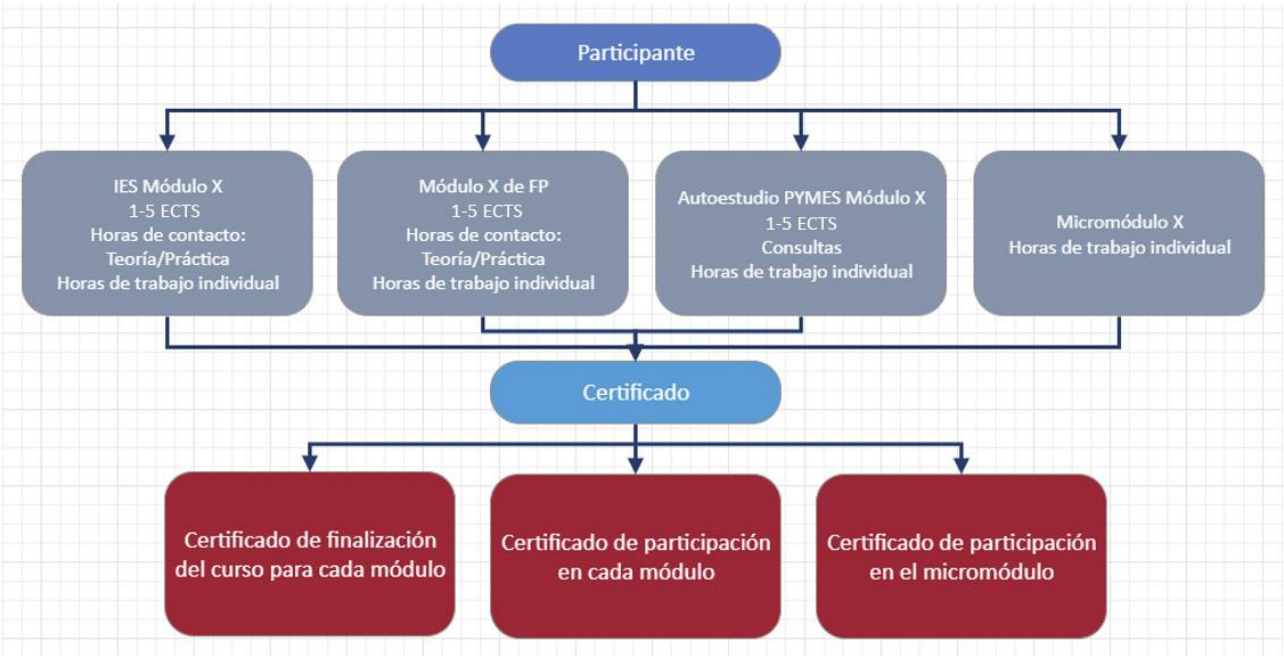


Figura 3. Estructura de los estudios

Las microcredenciales se integran en el proceso de aprendizaje a través de las siguientes actividades clave:

- Desarrollo de módulos de formación: cada módulo debe formularse cuidadosamente teniendo en cuenta los conocimientos y competencias específicos requeridos en el sector de las PYMES, con objetivos claros, resultados del aprendizaje, métodos de enseñanza y aprendizaje y duración del curso.
- Tareas prácticas y proyectos: el alumnado realiza tareas prácticas y desarrolla proyectos que se evalúan y proporciona pruebas claras de las competencias adquiridas.
- Estrategia de evaluación de conocimientos y criterios de evaluación claramente descritos: al final de cada módulo, se organiza una evaluación de conocimientos para determinar si la persona participante ha alcanzado los resultados de aprendizaje requeridos y si puede optar a un certificado que lo demuestre.

Como el grupo destinatario del proyecto son las personas empleadas de PYMES y las personas estudiantes de IES y FP, se ofrecen cuatro tipos de estudios, según las posibilidades y necesidades del alumnado:

- Estudios de IES: 8 módulos, cada uno de 1-5 ECTS, donde hay horas de contacto (teoría y práctica) y horas de trabajo individual;
- Estudios de FP: 8 módulos, cada uno de 1-5 ECTS, en los que hay horas de contacto (teoría y práctica) y horas de trabajo individual;
- Autoestudios (para PYMES): 8 módulos, cada uno de 1-5 ECTS, en los que hay consultas (si son necesarias) y horas de trabajo individual;
- Micromódulos: hora de trabajo individual en función del número de temas elegidos.

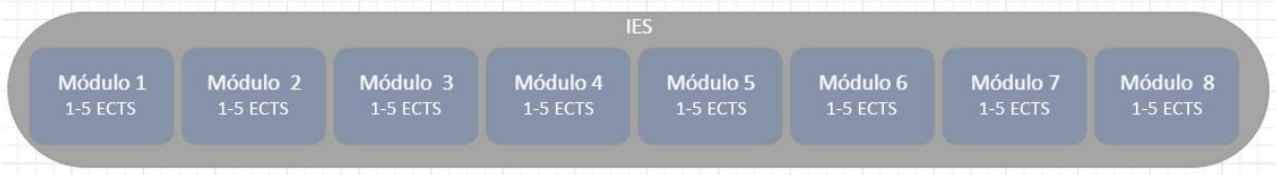


Figura 4. Estructura de estudios del IES

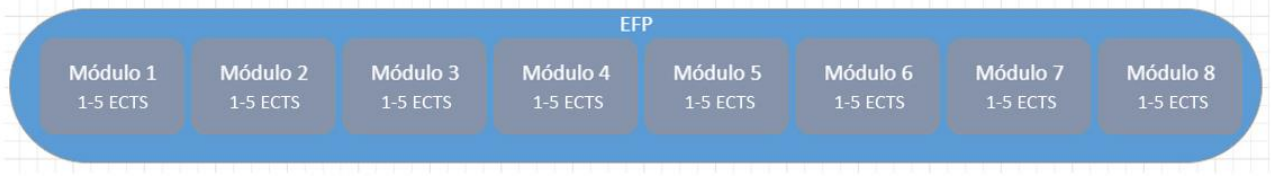


Figura 5. Estructura de los estudios de EFP

Figura 6. Estructura de estudios para Autoestudio

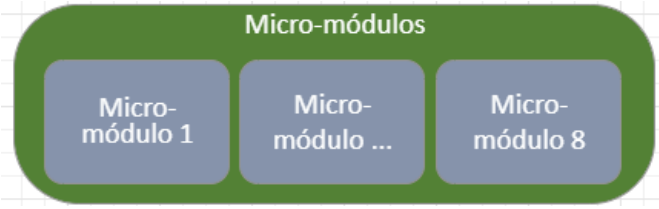


Figura 7. Estructura de estudios del micromódulo

El alumnado de IES y FP podrá estudiar un módulo de 1-5 créditos cada uno. Las personas trabajadoras en PYMES podrán cursar un módulo cada vez, o podremos ofrecer microsecciones como parte del curso.

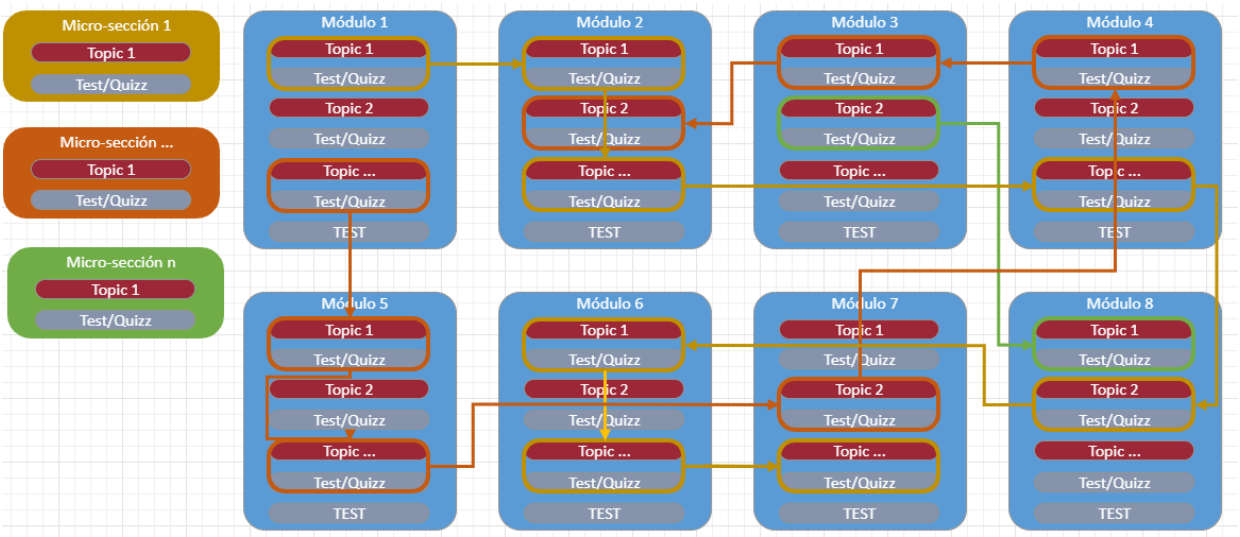


Figura 8. Vínculos entre los itinerarios de aprendizaje

En los tres tipos de aprendizaje (IES, FP y PYMES), el alumno o la alumna estudia 8 módulos. En el caso de los micromódulos, el o la estudiante elige los módulos por su cuenta.

Los micromódulos son experiencias de aprendizaje cortas o largas que se evalúan de forma transparente. La persona participante puede cursarlos junto con la prueba final o por separado. Cada micromódulo se valora con una cantidad diferente de la carga de trabajo de aprendizaje (como ECTS) y finaliza con una evaluación. La finalización con éxito de la evaluación del micromódulo recompensa al alumnado con microcredenciales.

La propuesta es que cada módulo del programa IES pueda modularse en un micromódulo, cada uno con tareas especializadas y un plan detallado de ejecución. Los resultados de las pruebas pueden evaluarse mediante insignias, que se basan en imágenes y son universalmente legibles por ordenador. Estas imágenes incorporan metadatos que detallan las competencias asociadas a cada insignia e información sobre la persona participante que la posee.

Por microcredencial se entiende el registro de los resultados de aprendizaje que una persona participante ha adquirido tras un pequeño volumen de aprendizaje. Estos resultados de aprendizaje se habrán evaluado con arreglo a criterios transparentes y claramente definidos. Las experiencias de aprendizaje conducentes a microcredenciales están diseñadas para

proporcionar al participante conocimientos, aptitudes y competencias específicos que respondan a necesidades sociales, personales, culturales o del mercado laboral.[5], [6] .

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Hacia adelante y más allá en la educación: Concept of FLEXIBLE LEARNING PATHWAYS. En KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[6] Recomendación del Consejo, de 16 de junio de 2022, relativa a un enfoque europeo sobre microcredenciales para el aprendizaje permanente y la empleabilidad". Diario Oficial de la Unión Europea, vol. 2022/C, 16 de junio de 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN

2. TRAYECTORIA PROFESIONAL

El itinerario de postaprendizaje podría denominarse trayectoria profesional o plan de carrera. Al principio del proyecto se realizó el análisis de investigación de las ocupaciones de ESCO (Descrito en el informe: D2.2 - The SME Cyber Security Change Agents Training needs mapping report). El análisis realizado en tres fases tenía como objetivo investigar varias ocupaciones de ciberseguridad enumeradas en el marco ESCO. En la primera fase, se identificaron y documentaron las ocupaciones relacionadas con la ciberseguridad a partir del **portal** ESCO, destacando sus respectivas habilidades, competencias y conocimientos. Estas ocupaciones incluían funciones como jefe de seguridad de las TIC, experto en forense digital, ingeniero de seguridad de sistemas integrados, hacker ético, gestor de resiliencia de las TIC, administrador de seguridad de las TIC, ingeniero de seguridad de las TIC, gestor de seguridad de las TIC e ingeniero del conocimiento. Cada profesión se definió por sus responsabilidades específicas y áreas de interés dentro del campo de la ciberseguridad, que van desde funciones de seguridad corporativa hasta análisis forense digital, hacking ético y planificación de la resiliencia.

En la segunda fase, se rellenó una tabla para cada ocupación de la ESCO revisada, detallando su título y responsabilidades principales. Entre ellas figuraban tareas como la planificación y aplicación de medidas de seguridad, la realización de evaluaciones de vulnerabilidad, el desarrollo de modelos de resiliencia y recuperación en caso de catástrofe y la integración de conocimientos en sistemas informáticos.

Además, la tercera fase consistió en mapear las ocupaciones de la ESCO con los resultados de aprendizaje asociados, clasificándolos en conocimientos, habilidades y competencias. Este proceso facilitó una comprensión exhaustiva de los requisitos educativos y las competencias esperadas para cada función de ciberseguridad, garantizando la alineación con las normas y las mejores prácticas del sector. A través de estas fases, el análisis proporcionó valiosas perspectivas para la investigación posterior.

Figura 9. Ocupaciones de la ESCO definidas en el informe anterior

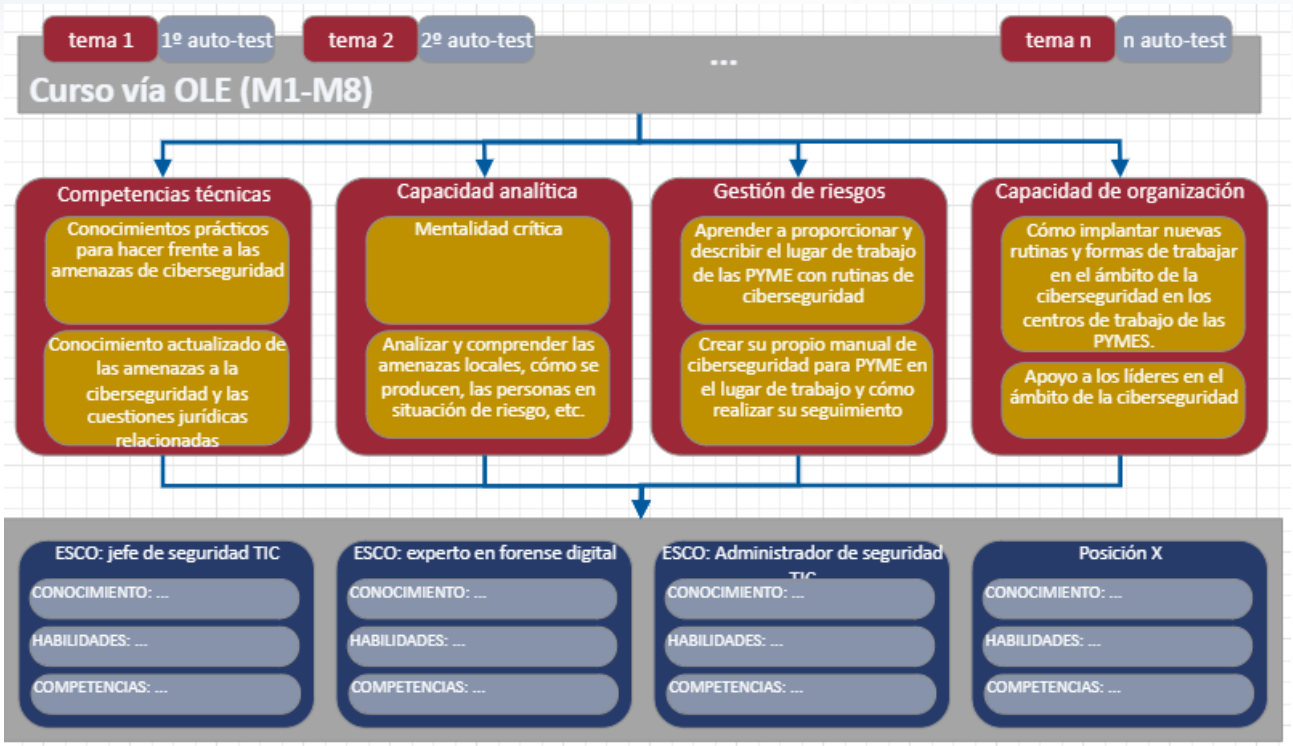


Figura 10. Posibles itinerarios post-aprendizaje

La figura 10 ilustra las posibles trayectorias profesionales que pueden seguirse una vez finalizados los estudios a través de un entorno de aprendizaje en línea (IES, EFP, PYMES) y la adquisición de competencias, en consonancia con las ocupaciones de la ESCO.

Con un conocimiento más claro de las salidas profesionales, los estudiantes de IES y EFP que estudien ciberseguridad comprenderán mejor las opciones profesionales y podrán elegir otro campo de estudio o trabajar en empresas en puestos específicos, mientras que los estudiantes de TI y de otros ámbitos podrán elegir módulos de CyberAgent como módulos de estudio individuales, mejorando así sus competencias en su campo de estudio, como las capacidades organizativas y de gestión de riesgos, etc.

El personal de las PYMES tendrá la oportunidad de actualizarse y desarrollar sus competencias en el lugar de trabajo. Sobre la base de la trayectoria profesional que se ha desarrollado y con claras oportunidades de carrera, el personal de PYMES podrá reciclarse en el ámbito de la ciberseguridad.

Está prevista una mayor participación tanto de estudiantes como del personal de las PYMES mediante la integración de sistemas de tutoría, la organización de actos de difusión, talleres (el proyecto incluye 6 talleres conjuntos organizados por todos los socios, así como campañas de difusión organizadas por cada uno de ellos), la invitación a representantes del mundo empresarial y de la ciberseguridad, la cooperación con los interlocutores sociales y la red CyberAgent, la oferta de prácticas a estudiantes, etc. Además, nuestras iniciativas en materia de diversidad, que

incluyen programas específicos de divulgación y apoyo, pretenden reforzar la participación de las mujeres, fomentando una mano de obra inclusiva en el ámbito de la ciberseguridad.

Al asignar de forma exhaustiva las ocupaciones de la ESCO a nuestros módulos de formación de Ciberagente, los participantes pueden pasar sin problemas de los entornos de aprendizaje a funciones de gran repercusión en el ámbito de la ciberseguridad. Con el fin de seguir el desarrollo profesional del alumnado de Ciberagente, está previsto organizar encuestas previas a la formación, inmediato después a la formación y a tres meses después para averiguar cómo contribuyen sus competencias a la ciberseguridad de las organizaciones en las que trabajan. Las encuestas se integrarán en la plataforma de formación y se ofrecerán automáticamente al alumnado antes del inicio del curso y al final de este para medir el progreso y evaluar el curso y la calidad de la formación. Una tercera encuesta servirá para averiguar si se han producido cambios en la carrera profesional de las personas participantes.

3. MÉTODOS DE ENSEÑANZA

El análisis de los métodos pedagógicos del programa de estudios de Sistemas de Información y Ciberseguridad de la Universidad de Vilnius (VU), de los programas de estudios Timtal y Moisil Buzau y de la bibliografía externa nos permite recomendar varias combinaciones innovadoras de métodos pedagógicos. Estas combinaciones podrían incluirse en los módulos de estudio, teniendo en cuenta la estructura de cada módulo.[7]

Tabla 1. Métodos pedagógicos recomendados

Categoría	Información detallada
Conferencia e instrucción directa	- **Conferencias teóricas:** conceptos y teorías fundamentales. - **Ponentes invitados** (especialistas certificados en: Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+, Certified Ethical Hacker (CEH), GIAC Security Essentials Certification (GSEC), Systems Security Certified Practitioner (SSCP), CompTIA Advanced Security Practitioner (CASP+), GIAC Certified Incident Handler (GCIH), Offensive Security Certified Professional (OSCP)).

Aprendizaje práctico	- **Tareas prácticas/Laboratorios:** experimentos prácticos y ejercicios prácticos.
	- **Actividades prácticas**: aplicaciones reales y tareas interactivas.
	- **Análisis técnico de vídeos:** análisis de contenidos de vídeo para el aprendizaje de habilidades técnicas.
	- **Entornos simulados**:
	  o Máquinas alojadas para entornos en nube.
	  o Lanzar ataques contra una máquina objetivo.
	  o Máquina para planificar y realizar ataques: una caja de ataque.

[7] Enseñanza de la ciberseguridad: Un enfoque de aprendizaje colaborativo basado en proyectos e investigación guiada https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

Categoría	Información detallada
Valoración y evaluación	- **Pruebas, juegos, lo que se debe y lo que no se debe hacer**: Evaluaciones atractivas e interactivas. - **Pruebas de autoevaluación**: Para la autoevaluación del alumnado al final de los temas.
Autoestudios	- **Aprendizaje autoguiado:** este método admite itinerarios de aprendizaje personalizados y puede mejorarse con recursos digitales y contenidos modulares a los que el alumnado puede acceder según sus necesidades.
Aprendizaje colaborativo y entre iguales	- **Aprendizaje colaborativo, trabajo en equipo**: proyectos de grupo y tareas colaborativas. - **Enseñanza y aprendizaje entre iguales**: las personas alumnas enseñan y aprenden unas de otras. - **Tutoría de grupo y/o tutoría individual**: orientación proporcionada por personas con más experiencia.
Aprendizaje potenciado por la tecnología	- **Utilización de una plataforma de aprendizaje de ciberseguridad gamificada**: captación de alumnado mediante elementos similares a juegos en plataformas de aprendizaje. - **Concursos de captura la bandera**: eventos competitivos para mejorar las competencias en ciberseguridad. - **Concursos**: los concursos ponen a prueba las habilidades y conocimientos de las personas estudiantes en un entorno práctico y aplicado, y proporcionan una medida de sus competencias en un formato competitivo.
Compromiso público y comunitario	- **Actos educativos:** actos especiales durante iniciativas como el Mes de la Ciberseguridad. - **Presentaciones públicas**: seminarios, conferencias y seminarios web.

Categoría	Información detallada
	- **Redes sociales**: uso de medios y redes sociales para el aprendizaje y el compromiso. - **Campus de un día**: suele consistir en eventos de inmersión en el campus que pueden incluir talleres, conferencias y oportunidades para establecer contactos.
Modelos de aprendizaje innovadores	- **BSCS 5E Instructional Model (5Es)** - el 5Es se centra en las siguientes 5 fases: Compromiso, Exploración, Explicación, Elaboración y Evaluación. - **Modelo de aprendizaje basado en retos (Challenge-Based Learning - CBL)**: una aplicación temprana del CBL proporciona un marco que consta de seis fases: Describir el reto, Generación y lluvia de ideas, Revisar múltiples perspectivas que cuestionan y apoyan, Investigar y revisar para encontrar las mejores soluciones, Probar hipótesis, Compartir los resultados y conclusiones. - **Modelo de aprendizaje cooperativo (CL)** - similar a los modelos 5E y CBL, el aprendizaje cooperativo promueve el aprendizaje activo en pequeños grupos y el alumnado recibe una recompensa basada en su rendimiento que puede incluir una nota, una recompensa tangible como un certificado o una beca, o la aprobación de un docente. - **Modelo de Aprendizaje Basado en Proyectos (ABP)** - el Aprendizaje Basado en Proyectos y el Aprendizaje Basado en Problemas utilizan la misma abreviatura de ABP y ambos se centran en mejorar la resolución de problemas, el pensamiento crítico, el trabajo en equipo, la comunicación y las habilidades creativas; sin embargo, constan de fases diferentes., Investigación independiente y en grupo, Desarrollar y presentar, Analizar y evaluar el proceso. - **Modelo de aprendizaje guiado por procesos (Process Oriented Guided Inquiry Learning -**

Categoría	Información detallada
	POGIL) - este enfoque guía a estudiantes a través de la exploración de un concepto; seguido de la invención del concepto donde el alumnado sintetiza y explica el concepto; y cierra el ciclo de aprendizaje con la aplicación del concepto teórico. - **Modelo de aprendizaje de la colaboración en la investigación guiada (Guided Inquiry Collaborative Learning Model - GICL)**: se trata de un nuevo enfoque basado en gran medida en el modelo POGIL.

Con el fin de garantizar que las diversas estrategias de formación ofrecidas tengan el mejor impacto posible, cada enfoque se seleccionará y alineará con los objetivos de aprendizaje específicos de los módulos de ciberseguridad en el desarrollo de un programa de módulo completo y materiales de formación. El personal docente/mentores que impartirán la formación de Ciberagente también podrán elegir métodos adicionales. Durante la fase de desarrollo de los materiales de formación, se impartirá formación al personal instructor de las formaciones piloto para informarles sobre los objetivos, el proceso y las responsabilidades de la formación, y prepararlos para impartir eficazmente el plan de estudios de Ciberagente. El proceso de formación piloto también incluye la recogida de comentarios del alumnado y formadores con el fin de supervisar la eficacia de los métodos de formación utilizados y realizar los ajustes necesarios.

Los módulos se impartirán en diferentes formatos pedagógicos:

- en **formato remoto**,
- en el **aprendizaje sincrónico** (apoyo total del docente),
- y en el **aprendizaje asíncrono** (apoyo del docente cuando es necesario), el aprendizaje combinado y el autoaprendizaje.

Dado que se prevén diferentes maneras de impartir la formación, los métodos de formación se presentan en esta fase como directrices.

4. ESTRUCTURA DE LOS MÓDULOS

El análisis de la estructura de módulos del programa de estudios de Ciberseguridad de la VU, el análisis de la estructura de módulos de los proyectos internacionales (**CyberPhish**, **FuseIT**, **dComFra**), y el análisis de la estructura de módulos de plataformas comerciales, como **Udemy** y **Coursera**, ha llevado a la creación de una estructura de módulos típica que podría aplicarse tanto a módulos de IES como de EFP.

El objetivo principal es desarrollar 8 módulos, de los cuales 8 serían para estudiantes de IES (nivel EQF 5-- 6), para estudiantes de EFP y PYMEs (nivel EQF 4-5) y micromódulos para todo tipo de estudiantes.

Figura 11. Estructura del módulo

* Se recomienda que cada subtema vaya seguido de preguntas de autocomprobación (autorreflexión). No obstante, en la fase de desarrollo del módulo, puede elegirse un método u opción de evaluación diferente en función del tipo de estudio elegido; por ejemplo, se pueden plantear al alumnado ejercicios prácticos, simulaciones, etc., mientras que las preguntas de autocomprobación se ofrecen al alumnado independiente.

** La prueba de evaluación de conocimientos es opcional. Si la persona desea obtener un certificado de finalización del curso que ateste los conocimientos adquiridos, esta prueba es obligatoria. Sin embargo, el alumno o la alumna tiene la opción de obtener un certificado de asistencia al curso para demostrar que ha asistido a la formación, en cuyo caso esta prueba es opcional.

Para garantizar que cada módulo de formación está directamente vinculado a la aplicabilidad práctica, la descripción de cada módulo proporcionará ejemplos claros de cómo se aplica la teoría en la práctica. Esto incluye no sólo escenarios detallados de la aplicabilidad de los módulos, sino también tareas específicas que el alumnado realizará para consolidar los conocimientos teóricos en situaciones reales de ciberseguridad.

Cada módulo debe proporcionar competencias técnicas, analíticas, de gestión de riesgos y organizativas en diferentes proporciones. Se ofrece una prueba de autoevaluación para comprobar los conocimientos del alumnado al final de cualquier parte del módulo (tema). Esto no sólo permite valorar o evaluar los conocimientos adquiridos, sino que también se registra el progreso del alumno o de la alumna y el participante acumula puntos e insignias, lo que le permite implicarse más en el proceso de aprendizaje.

Siguiendo las formalidades ECTS donde cada ECTS son 25-30 horas de carga de trabajo. Según esto, cada módulo podría equivaler a 5 ECTS. Las horas de carga de trabajo podrían distribuirse de esta manera:

Tabla 2. Horas de carga de trabajo

	Número de módulos	Total de ECTS	Horas a distancia para competencias teóricas	Horas a distancia para competencias prácticas	Horas de trabajo individuales	Horas totales de carga de trabajo
Módulos para estudiantes de IES (nivel 5-6 del MEC)	8	8-40	20%	20%	60%	200-1200
Módulos para estudiantes de EFP (nivel 4-5 del MEC)	8	8-40	15%	25%	60%	200-1200
Autoaprendizaje (semipresencial)	8	8-40	10%		90%	200-1080
Autoestudio (en línea)	8	8-40				200-1200
Micromódulos	1-8	1-40				25-1200

Cuadro 3. Carga de trabajo de los módulos recomendados

Módulo	ECTS	Total de horas	Horas de contacto	Horas de contacto (teoría)	Horas de contacto (prácticas)	Horas de trabajo individual
IES Título del módulo	1-5	25-150	40%	20%	20%	60%
FP Título del módulo	1-5	25-150	40%	15%	25%	60%
Autoestudio (formación semipresencial)	1-5	25-150	10%			90%
Autoestudio (en línea)	1-5	25-150				100%
Microsecciones						10%-100%

Cada módulo debería tener su propia descripción. Tras el análisis de la VU, Timtal y otros programas que utilizan microcredenciales, se propone una estructura de módulo típica para

cada módulo de Ciberagente (en el anexo 1 se ofrece un ejemplo de estructura de módulo típica).

Cuadro 4. Estructura típica de los módulos de Ciberagente

Categoría	Información detallada
Identificación del módulo (información básica sobre el módulo)	- Título del módulo - Código del módulo - Docente - Institución o departamento donde se imparte el módulo - Modelo de entrega - Idioma - Requisitos previos
Duración y carga de trabajo del módulo (compromiso de tiempo claro y esquema de la estructura)	- Duración total (número de ECTS) - Carga de trabajo del alumando en horas - Horas de trabajo de contacto - Horas de trabajo individual

Objetivos educativos y resultados del aprendizaje (detalles sobre lo que pretende conseguir el módulo y lo que aprenderá el alumnado)	- Finalidad y resultados del módulo
	- Resultados del aprendizaje
	  o Competencias técnicas
	  o Capacidad de análisis
	  o Habilidades de riesgo
	  o Capacidad de organización

Métodos de enseñanza y aprendizaje	- Métodos de enseñanza y aprendizaje
Evaluación (explicación de cómo se evaluará al alumnado)	- Métodos de evaluación - Tareas (laboratorios, proyectos, presentaciones, informes, etc.) - Estrategia de evaluación, criterios de evaluación
Facilitar recursos	- Equipamiento, software y tecnología
Contenido del curso	- Temas y subtemas del módulo
Recursos	- Lista de fuentes - Otras fuentes

Cada ECTS se considera de 25 a 30 horas (horas de contacto o en línea + estudio individual).

El módulo debe tener al menos una jerarquía de dos niveles:

- **El primer nivel de la jerarquía - temas**. En este nivel, los principales elementos del módulo podrían ser introducción, prueba de acceso, prueba final y el elemento base - tema.
- **El segundo nivel de la jerarquía** - subtemas, los principales elementos educativos del módulo.

Cada módulo del primer nivel de la jerarquía debe incluir:

- **INTRODUCCIÓN** al módulo (descripción textual, introducción en vídeo): relevancia y ventajas del módulo, objetivos y resultados básicos del módulo, software y hardware necesarios, requisitos para las personas participantes.
- **TEMAS** - temas principales del curso, material teórico y métodos teóricos de enseñanza.
- **SUBTEMA** - subtema de cada tema, análisis y tareas prácticas y analíticas, métodos de enseñanza prácticos y analíticos. Los temas y subtemas pueden incluir información textual, vídeos, clips de audio, presentaciones, enlaces a lecturas complementarias.
- **MÓDULO Prueba introductoria** (si es necesario). La prueba introductoria de los niveles intermedio y avanzado debe confirmar que la persona candidata domina suficientes conocimientos y habilidades en los niveles anteriores.
- **Pruebas de reconocimiento** del **MÓDULO**. Las pruebas de reconocimiento deben proporcionar una verificación objetiva de las habilidades de la persona estudiante y demostrar su competencia con los requisitos del módulo.
- **DIRECTRICES para mentores / docentes**. Este documento debe contener recomendaciones metodológicas para tutores / docentes sobre el uso de los elementos educativos del módulo.

Cada TEMA en el segundo nivel de la jerarquía debe incluir:

- **INTRODUCCIÓN** a los objetivos y resultados del tema, breve contenido.
- **SUBTEMA**: todos los elementos educativos necesarios para ayudar al alumno a dominar las competencias pertinentes.
- **Prueba del TEMA**: breves recomendaciones para mentores / docentes sobre la implementación y aplicación del módulo. Cada SUBTEMA debe constar de elementos educativos cuyo contenido corresponda a las tareas de la descripción del módulo. Cada subtema puede (debe) incluir una PRUEBA DE SUBTEMA, que confirme que la persona estudiante ha dominado las destrezas relevantes a un nivel suficientemente alto.

Los materiales didácticos del módulo deben apoyar el estudio de 6-8 temas, en cada uno de los cuales hay 4-6 subtemas y, como mínimo, una prueba temática. Por lo tanto, el módulo debe contener (aproximadamente) 30-40 elementos educativos (métodos descritos en la sección de métodos de enseñanza) y 6-8 pruebas y una prueba de reconocimiento final del módulo.

5. PLAN DE ESTUDIOS Y PROGRAMA DE FORMACIÓN PARA CIBERAGENTES

Hoja de ruta para la elaboración de planes de estudios

El plan de estudios y el programa de formación de Ciberagente siguen las Directrices curriculares para programas de postgrado en ciberseguridad, desarrolladas por el grupo de trabajo conjunto de ACM, IEEE, AIS SIGSEC e IFIP (2017)[8] (en adelante, **Directrices**). Más concretamente, dado que el objetivo general del proyecto CyberAgent es aumentar las competencias internas en ciberseguridad de las PYMES europeas, el plan de estudios sigue el marco del área de conocimiento de Seguridad Organizacional, según las recomendaciones de estas Directrices.

Dicho esto, el primer paso en la elaboración del plan de estudios consiste en establecer una correspondencia entre los subtemas y módulos predefinidos en el proyecto CyberAgent y las unidades de conocimiento y los temas clave, recomendados y descritos en las Directrices (p. 59-70). El mapeo se basa en la correlación lógica entre estos dos pilares, según lo discutido y acordado por los socios del proyecto.

El segundo paso consiste en asignar resultados de aprendizaje específicos, identificados y descritos en el documento D2.2 "Mapping the training needs for SME Cyber Security Change Agents" con la unidad de conocimiento y los temas clave, descritos anteriormente. Cabe señalar que las diferentes ocupaciones relacionadas con la ciberseguridad pueden tener una variedad de diferentes conocimientos, habilidades y competencias, como elocuentemente se indica en la mencionada D2.2. No obstante, la propuesta que figura a continuación refleja el conjunto de conocimientos, aptitudes y competencias que se espera del Ciberagente, que puede adaptarse a las necesidades específicas de determinadas ocupaciones o grupos de alumnos.

Dicho esto, los resultados de este ejercicio de elaboración de planes de estudios figuran en el cuadro 5.

[8] The Joint Task Force on Cybersecurity Education . (2017). Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity: A Report in the Computing Curricula Series. Association for Computing Machinery, 31 de diciembre de 2017. Disponible en: **https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf** [Consultado el 3 de marzo de 2024].

Cuadro 5. Hoja de ruta para la elaboración de planes de estudios

Subtemas y módulos	Unidad de conocimiento y temas clave	Resultados del aprendizaje IES	Resultados del aprendizaje EFP
Competencias técnicas			
- Conocimiento actualizado de las amenazas a la ciberseguridad y cuestiones jurídicas relacionadas	**Gestión de programas de seguridad** - Gestión de proyectos - Gestión de recursos - Métricas de seguridad - Garantía y control de calidad	**Conocimientos**: El alumnado obtendrá un conocimiento avanzado de los principios de ciberseguridad avanzada, incluidas las ciberamenazas sofisticadas y los vectores de ataque, la legislación nacional e internacional sobre ciberseguridad, las normas y los requisitos de cumplimiento pertinentes para su sector. **Habilidades**: El alumnado será capaz de diseñar y aplicar estrategias avanzadas de evaluación y gestión de riesgos para mitigar los riesgos identificados, utilizando metodologías y herramientas avanzadas. **Competencias**: El alumnado será competente para dirigir y gestionar proyectos y equipos de ciberseguridad implementando políticas y marcos estratégicos de ciberseguridad alineados con los objetivos y obligaciones de cumplimiento de la organización.	**Conocimientos**: El alumnado adquirirá conocimientos prácticos sobre las últimas amenazas a la ciberseguridad, incluidos el phishing, el ransomware y los ataques DDoS, y sobre cómo gestionarlas mediante una gestión eficaz de proyectos y recursos, y la aplicación de medidas de control y garantía de calidad. **Habilidades**: El alumnado estará capacitado para utilizar herramientas y software de protección contra las ciberamenazas en evolución, y aplicar prácticas de seguridad sólidas en la gestión de proyectos y recursos para mejorar las métricas generales de seguridad y el control de calidad dentro de sus organizaciones. **Competencias**: El alumnado será competente para evaluar y mitigar las posibles amenazas a la seguridad, comunicar eficazmente los problemas de ciberseguridad y notificar con precisión las amenazas y violaciones a través de los

			canales adecuados dentro de su organización.
- Conocimientos prácticos para hacer frente a las amenazas de ciberseguridad	**Administración de sistemas** - Administración de sistemas operativos - Administración de sistemas de bases de datos - Administración de redes - Administración de la nube - Administración de sistemas ciberfísicos - Endurecimiento del sistema - Disponibilidad	**Conocimientos**: El alumnado adquirirá conocimientos avanzados en administración de sistemas operativos, de bases de datos, de redes, en la nube y ciberfísicos, entre otros, que les permitirá endurecer eficazmente los sistemas y garantizar su disponibilidad, al tiempo que aplican los últimos mecanismos de defensa de la ciberseguridad. **Habilidades**: Las personas alumnas estarán capacitadas para utilizar metodologías y herramientas avanzadas para diseñar e implementar arquitecturas de sistemas seguras, incluidos sistemas operativos, bases de datos, redes e infraestructuras en la nube **Competencias**: El alumnado será competente para desarrollar e implementar marcos estratégicos de ciberseguridad para la administración de sistemas, liderar proyectos y equipos para mejorar el endurecimiento y la disponibilidad de los sistemas, y tomar decisiones éticas en el mantenimiento	**Conocimientos**: El alumnado obtendrá conocimientos prácticos sobre cómo administrar y proteger sistemas operativos, bases de datos, redes, nubes y sistemas ciberfísicos contra ciberamenazas comunes como phishing, ransomware y ataques DDoS, al tiempo que implementan políticas eficaces de gestión de riesgos. **Habilidades**: El alumando estará capacitado para identificar posibles riesgos y vulnerabilidades de ciberseguridad en diversas plataformas de sistemas, utilizar herramientas y software especializados para mejorar el refuerzo y la disponibilidad de los sistemas, y aplicar prácticas básicas de ciberseguridad como la creación de contraseñas seguras, la navegación segura y el manejo seguro de datos confidenciales. **Competencias**: El alumnado será competente para evaluar y mitigar las amenazas a la seguridad en la administración de sistemas, comunicar eficazmente los problemas de ciberseguridad e informar con prontitud

		de prácticas sólidas de ciberseguridad en varios dominios administrativos.	de cualquier amenaza y brecha a los canales organizativos adecuados.
Capacidad de análisis			
- Mentalidad crítica	**Herramientas analíticas** - Medidas de rendimiento (métricas) - Análisis de datos - Inteligencia en materia de seguridad	**Conocimientos**: El alumnado adquirirá conocimiento avanzado sobre la legislación, las normas y los requisitos de cumplimiento en materia de ciberseguridad nacionales e internacionales, así como otros pertinentes para su sector específico. **Habilidades**: El alumnado estará capacitado para utilizar mediciones de rendimiento, análisis de datos e inteligencia de seguridad para diseñar y aplicar estrategias eficaces de gestión de riesgos. **Competencias**: El alumnado será competente en el uso de herramientas analíticas para desarrollar políticas estratégicas de ciberseguridad con una mentalidad de pensamiento crítico, y tomar decisiones en prácticas de ciberseguridad alineadas con los objetivos de la organización y las obligaciones de cumplimiento.	**Conocimientos**:El alumnado adquirirá conocimientos prácticos sobre cómo aplicar mediciones de rendimiento, análisis de datos e inteligencia de seguridad para proteger los activos de la organización. **Habilidades**: El alumnado será capaz de utilizar herramientas analíticas para identificar posibles riesgos y vulnerabilidades de ciberseguridad, aplicar conocimientos basados en datos para reforzar las prácticas de ciberseguridad y utilizar métricas de rendimiento para evaluar y mejorar la seguridad de las contraseñas, la navegación, el correo electrónico y el manejo de datos. **Competencias**: La persona alumna será competente para evaluar y mitigar las posibles amenazas a la seguridad utilizando herramientas analíticas, informando con precisión sobre amenazas y violaciones a los canales apropiados dentro de su organización.

- Analizar y comprender las amenazas locales, cómo se producen, las personas en situación de riesgo, etc.	**Operaciones de seguridad** - Convergencia de la seguridad - Centros mundiales de operaciones de seguridad (GSOC)	**Conocimientos**: El alumnado adquirirá conocimientos avanzados sobre las ciberamenazas locales, utilizando los conocimientos de los centros de operaciones de seguridad globales y las tendencias actuales en estrategias de defensa de la ciberseguridad. **Habilidades**: El alumnado estará capacitado para utilizar metodologías y herramientas avanzadas dentro de los centros de operaciones de seguridad globales para diseñar estrategias eficaces de gestión de riesgos y desarrollar planes para mitigar eficazmente las amenazas locales a la ciberseguridad. **Competencias**: Las personas alumnas serán competentes en el desarrollo y la aplicación de políticas estratégicas de ciberseguridad que aborden las amenazas locales mediante el uso de centros de operaciones de seguridad globales.	**Conocimientos**: El alumnado adquirirá conocimientos prácticos sobre las ciberamenazas locales y sus orígenes, y evaluará cómo afectan estas amenazas a los activos de la organización. **Habilidades**: El alumnado estará capacitado para identificar los riesgos y vulnerabilidades locales en materia de ciberseguridad, utilizando herramientas y programas informáticos como la creación de contraseñas seguras, la navegación segura y el manejo seguro de datos adaptados a sus entornos específicos. **Competencias**: Las personas alumnas serán capaces de evaluar y mitigar las amenazas a la seguridad local utilizando la información procedente de los centros de operaciones de seguridad globales, comunicar eficazmente los problemas de ciberseguridad e informar con precisión de las amenazas y las infracciones a los canales adecuados dentro de su organización.
Gestión de riesgos			
- Aprender a proporcionar y describir el lugar de trabajo de las PYMES con rutinas de ciberseguridad	**Gestión de riesgos** - Identificación de riesgos	**Conocimientos**: El alumnado adquirirá conocimientos avanzados sobre los procesos de gestión de riesgos, incluida su identificación, evaluación y control,	**Conocimientos**:El alumnado adquirirá conocimientos prácticos sobre los procesos de identificación, evaluación y control de riesgos, y las estrategias de

	- Evaluación y análisis de riesgos - Amenazas internas - Modelos y metodologías de medición y evaluación de riesgos - Control de riesgos	lo que le permitirá establecer y describir rutinas eficaces de ciberseguridad adaptadas a las necesidades específicas de los lugares de trabajo de las PYMES, de conformidad con las normas nacionales e internacionales. **Habilidades**: El alumnado estará capacitado para aplicar metodologías y herramientas avanzadas para llevar a cabo evaluaciones exhaustivas de riesgos, diseñar y aplicar estrategias eficaces de gestión de riesgos y desarrollar rutinas sólidas de ciberseguridad adaptadas específicamente a los lugares de trabajo de las PYME. **Competencias**: La persona alumna será competente en la elaboración y aplicación de políticas estratégicas de ciberseguridad para los centros de trabajo de las PYME.	gestión de riesgos para salvaguardar eficazmente los lugares de trabajo de las PYME. **Habilidades**: El alumnado estará capacitado para identificar y analizar los posibles riesgos de ciberseguridad en los entornos de las PYME, utilizar las herramientas y el software adecuados para mitigar las amenazas, y promover y aplicar prácticas esenciales de ciberseguridad, como la creación de contraseñas seguras, la navegación segura y el manejo seguro de datos confidenciales. **Competencias**: La persona alumna será capaz de evaluar y mitigar las amenazas a la seguridad en el lugar de trabajo de una PYME, de comunicar eficazmente los problemas y procedimientos de ciberseguridad, y de informar con precisión de las amenazas y violaciones pertinentes a los canales organizativos apropiados.
- Crear su propio manual de ciberseguridad para PYMES en el lugar de trabajo y cómo realizar su seguimiento	**Continuidad de las actividades, recuperación en caso de catástrofe y gestión de incidentes y seguridad del personal** - Respuesta a incidentes	**Conocimientos**: El alumnado adquirirá conocimientos avanzados sobre cómo crear y aplicar un manual completo de ciberseguridad en el lugar de trabajo de las PYMES, que incorpore principios avanzados de ciberseguridad, los	**Conocimientos**: El alumnado adquirirá conocimientos prácticos sobre cómo crear un manual completo de ciberseguridad en el lugar de trabajo de las PYMES que incorpore estrategias para la respuesta ante incidentes, la recuperación ante

	- Recuperación en caso de catástrofe - Continuidad de las actividades - Concienciación, formación y educación en materia de seguridad - Prácticas de contratación en materia de seguridad - Prácticas de rescisión de seguridad - Seguridad de terceros - Seguridad en los procesos de revisión - Especial sobre la privacidad de los datos personales de las personas trabajadoras	últimos mecanismos de defensa y el cumplimiento de la legislación y las normas nacionales e internacionales en materia de gestión de incidentes, continuidad de las actividades y seguridad del personal. **Habilidades**: El alumnado estará capacitado para crear y mantener un manual de ciberseguridad en el lugar de trabajo de la PYMES, utilizando metodologías avanzadas para evaluar riesgos, diseñar estrategias eficaces de gestión de riesgos y respuesta a incidentes, y desarrollar planes integrales de continuidad de la actividad adaptados a las necesidades de su organización. **Competencias**: La persona alumna será competente en el desarrollo e implementación de un manual de ciberseguridad para PYMES, liderando proyectos y equipos de seguridad de forma eficaz, asegurando la alineación con los objetivos de la organización y las obligaciones de cumplimiento.	desastres, la continuidad empresarial y la seguridad del personal, protegiendo los activos de la organización y los datos confidenciales. **Habilidades**: El alumnado estará capacitado para identificar posibles riesgos de ciberseguridad, utilizando herramientas y software para protegerse de las amenazas, y aplicando las mejores prácticas en ciberseguridad para desarrollar y mantener un manual de PYME que aborde la creación de contraseñas seguras, la navegación, la seguridad del correo electrónico y la protección de datos. **Competencias**: El alumnado será competente para evaluar y mitigar las amenazas a la seguridad, comunicar eficazmente las políticas y prácticas de ciberseguridad y notificar sistemáticamente los incidentes de seguridad dentro de su PYME, como se indica en su manual de ciberseguridad personalizado.
Capacidad de organización			
- Cómo implantar nuevas rutinas y formas de	**Gobernanza y política de seguridad**	**Conocimientos**: El alumnado adquirirá conocimientos avanzados sobre cómo	**Conocimientos**: El alumnado adquirirá conocimientos prácticos sobre cómo

trabajar en el ámbito de la ciberseguridad en los centros de trabajo de las PYMES.	- Contexto organizativo - Privacidad - Legislación, ética y cumplimiento - Gobernanza de la seguridad - Comunicación a nivel ejecutivo y directivo - Política de gestión	implantar nuevas rutinas y flujos de trabajo de ciberseguridad en los lugares de trabajo de las PYMES, incorporando los principios actuales de ciberseguridad, las tendencias y el cumplimiento de la legislación nacional e internacional pertinente para su sector. **Habilidades**: El alumnado estará capacitados para utilizar metodologías avanzadas para realizar evaluaciones de riesgos, diseñar e implantar nuevas rutinas de ciberseguridad y preparar estrategias de respuesta, garantizando una gobernanza y un cumplimiento eficaces en los lugares de trabajo de las PYME. **Competencias**: El alumnado será competente en el desarrollo e implementación de políticas estratégicas de ciberseguridad, liderando iniciativas para establecer nuevas rutinas y flujos de trabajo en los lugares de trabajo de las PYMES, y tomando decisiones éticas que se alineen con los objetivos de la organización y los requisitos de cumplimiento.	integrar nuevas rutinas y prácticas de ciberseguridad en los lugares de trabajo de las PYMES, de conformidad con la legislación, las normas, las estrategias y las políticas de ciberseguridad para la seguridad de la información, la gestión de riesgos y la protección de datos. **Habilidades**: El alumnado estará capacitado para aplicar herramientas y programas informáticos de ciberseguridad para implantar nuevas rutinas de seguridad, identificar y mitigar riesgos y promover prácticas esenciales de ciberseguridad como la creación de contraseñas seguras, la navegación y el manejo de datos dentro del marco de gobernanza de los lugares de trabajo de las PYMES. **Competencias**: El alumno será competente para evaluar y mitigar las posibles amenazas a la seguridad, comunicar eficazmente los cambios y las políticas de ciberseguridad y notificar con precisión los incidentes de seguridad en las PYME de acuerdo con los requisitos de gobernanza y cumplimiento.

- Dirigir el apoyo a los y las líderes en el ámbito de la ciberseguridad.	**Planificación de la ciberseguridad** - Planificación estratégica - Gestión operativa y táctica	**Conocimientos**: El alumnado adquirirá conocimientos avanzados sobre cómo integrar principios avanzados de ciberseguridad y tendencias actuales en la planificación estratégica y la gestión operativa. **Habilidades**: El alumnado estará capacitado para la planificación estratégica y la gestión operativa, lo que les permitirá diseñar y aplicar eficazmente estrategias de ciberseguridad que aborden los riesgos emergentes y garanticen respuestas tácticas sólidas. **Competencias**: El alumnado será competente en el desarrollo e implementación de marcos estratégicos de ciberseguridad, liderando y gestionando iniciativas de ciberseguridad.	**Conocimientos**: El alumnado adquirirá conocimientos prácticos sobre cómo integrar la planificación estratégica y la gestión operativa en ciberseguridad para proteger los activos de la organización, cumplir la legislación y las normas pertinentes y aplicar estrategias eficaces de seguridad de la información y políticas de gestión de riesgos. **Habilidades**: El alumnado estará capacitado para identificar los riesgos de ciberseguridad, utilizar herramientas de planificación estratégica y gestión operativa para protegerse de las amenazas y promover la aplicación de prácticas fundamentales de ciberseguridad dentro de sus funciones de apoyo a la dirección. **Competencias**: El alumnado será competente para evaluar y mitigar las amenazas a la seguridad, comunicar eficazmente las estrategias y los problemas de ciberseguridad, y notificar de forma fiable los incidentes y las vulnerabilidades a los canales adecuados dentro de sus organizaciones.

6. ESTRATEGIA DE EVALUACIÓN DEL CURSO

La evaluación de los conocimientos es parte integrante del proceso de aprendizaje y promueve un aprendizaje más profundo. En este capítulo se describe el enfoque de la evaluación del curso necesario para garantizar que todas las personas participantes en los cursos de Ciberagente alcancen los resultados de aprendizaje y las competencias requeridas. El proceso de evaluación del curso se divide en dos partes principales: la autoevaluación y las pruebas de evaluación de conocimientos, que se adaptan tanto a las personas estudiantes de Enseñanza Superior (IES) como a los de Formación Profesional (EFP), teniendo en cuenta sus diferentes necesidades y objetivos de aprendizaje.

Dado que los temas de los módulos podrían ser los mismos tanto para las IES como para la EFP, algunas de las preguntas podrían ser adecuadas tanto para los cursos de las IES como para los de la EFP. Por lo tanto, al diseñar las preguntas, será posible especificar si la pregunta está destinada únicamente a la EFP, a las IES o a ambas. Esta forma de marcar sólo se utilizará al diseñar las preguntas, ya que facilitará el diseño de las mismas. Una vez importadas las preguntas a la plataforma, las bases de datos serán diferentes para EFP e IES.

Figura 12. Bases de datos de autoevaluación y evaluación de conocimientos

1. Pruebas de autoevaluación: Tras la finalización de cada tema del curso, las personas estudiantes realizarán pruebas de autoevaluación. Estas evaluaciones están diseñadas para proporcionar una retroalimentación inmediata, ayudando a las personas estudiantes a evaluar su comprensión del material recientemente cubierto. Esta etapa fomenta la autorreflexión y ayuda a reforzar los objetivos de aprendizaje de cada tema. Además, permite a al alumnado identificar las áreas en las que podrían necesitar más estudio o aclaración, promoviendo un enfoque proactivo en su viaje de aprendizaje.

Mediante pruebas de autoevaluación, las personas participantes en el curso pudieron determinar su nivel inicial de conocimientos y comprobar sus progresos después de cada tema de formación.

Se recomienda un cuestionario de autoevaluación de 3-5 preguntas, con una mezcla de preguntas de verdadero/falso, de emparejamiento y/o de elección múltiple. Sólo se desbloqueará otro tema después de responder correctamente a todas las preguntas. No debe haber límites de tiempo ni restricciones en los intentos. Los intentos deben seleccionar aleatoriamente preguntas de la base de datos correspondiente.

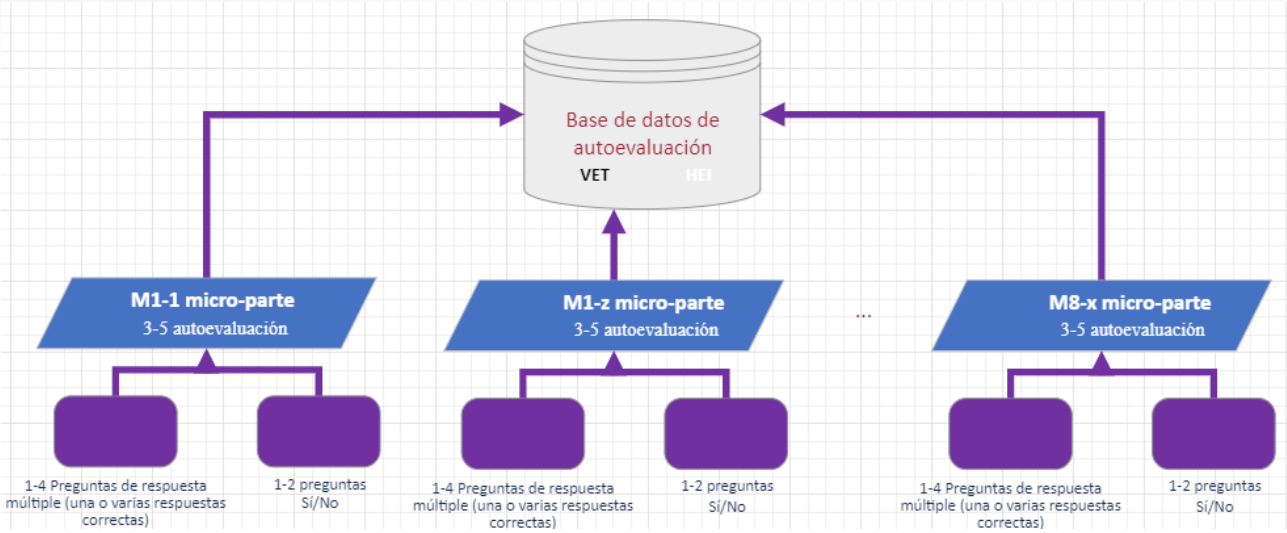


Figura 13. Estructura de la base de datos de autoevaluación

2. Prueba de evaluación de conocimientos*: Una vez completados todos los temas del curso, las personas estudiantes deberán realizar una prueba final para obtener el certificado de finalización del curso. Esta evaluación global evalúa su comprensión y dominio generales del contenido del curso. La prueba final evalúa la retención del material por parte de las personas estudiantes e identifica hasta qué punto pueden aplicar sus conocimientos en un contexto más amplio.

* Durante el desarrollo del plan de estudios y los materiales, se considerarán otras metodologías para evaluar la realización del curso y la evaluación de los conocimientos, como estudios de casos, ejercicios prácticos e informes reflexivos, que permitirán una evaluación más exhaustiva de las capacidades de pensamiento analítico y crítico de las personas participantes. Este enfoque también estará a disposición del personal docente de los centros de enseñanza superior y EFP durante el proceso de impartir el curso.

Mediante una prueba de evaluación de conocimientos, las personas participantes en el curso podían identificar su nivel final de conocimientos y, si lo superaban, recibir una insignia (certificado) de finalización del curso.

Se recomienda una prueba de evaluación de conocimientos de 36 preguntas, con una mezcla de preguntas de verdadero/falso, de emparejamiento y de opción múltiple. Debe haber un límite de tiempo de 45 minutos y sólo se permite un intento. La prueba debe administrarse seleccionando al azar preguntas de una base de datos.

Además, la evaluación también debe tener en cuenta la prevención del engaño y, por lo tanto, deben desarrollarse unos cuatro conjuntos de preguntas. Algunas de las preguntas de la prueba de conocimientos tanto para EFP como para IES pueden solaparse, por lo que tendremos tres atributos en el momento del desarrollo: EFP, IES o EFP e IES.

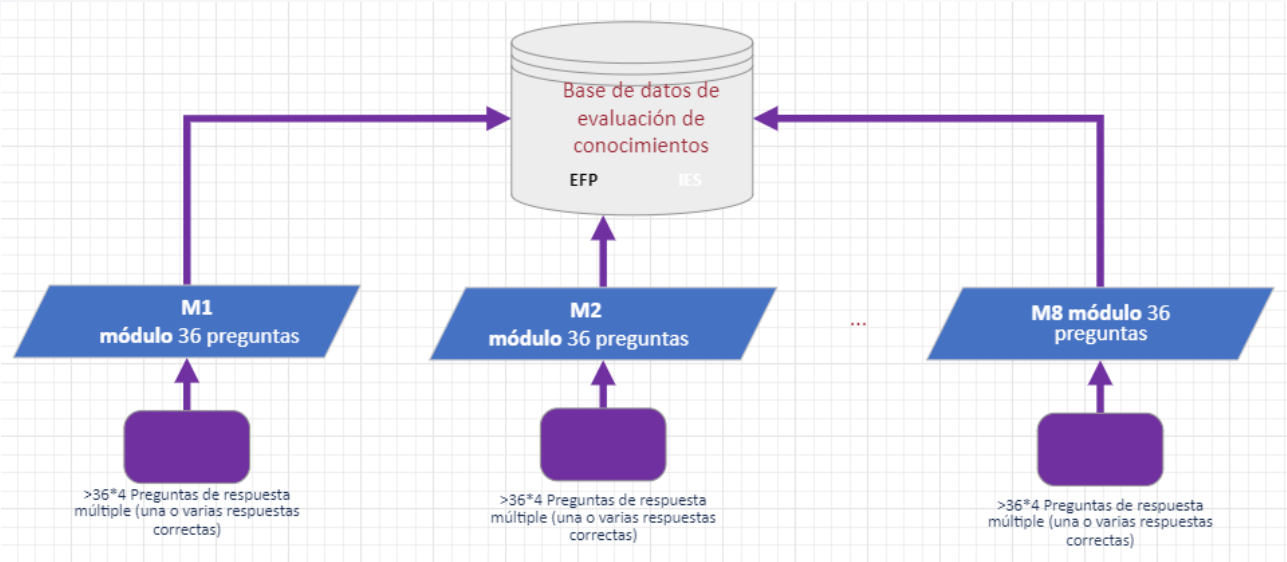


Figura 14. Estructura de la base de datos de evaluación de conocimientos

Esta estrategia de evaluación en dos fases no sólo favorece el aprendizaje eficaz al proporcionar múltiples circuitos de retroalimentación, sino que también capacita a al alumnado para asumir un papel activo en su formación.

Se elaborarán pruebas de autoevaluación y pruebas para la evaluación de los conocimientos siguiendo el programa de los cursos y basándose en los resultados y las recomendaciones elaboradas en este proyecto.

COMPOSICIÓN DE LA BASE DE DATOS DE PREGUNTAS

Para garantizar una base de preguntas suficientemente amplia y equilibrada, se crearán al menos 5 preguntas de verdadero/falso o de emparejamiento y 5 preguntas de opción múltiple para cada tema del curso de EFP o de IES.

Suponiendo que haya al menos 10 temas en cada curso, la base general de cada curso de EFP o IES debería contener al menos un 10-20% de preguntas de verdadero/falso o de emparejamiento, y un 90-80% de preguntas de opción múltiple. Se trata de una orientación general, pero el personal docente tendrá la posibilidad de elegir la estructura de las preguntas en función del tema del curso.

Teniendo en cuenta las diferencias en los objetivos y resultados de aprendizaje de EFP / IES, la composición general de la base de datos de preguntas para un solo curso debería contener lo que se muestra en la tabla siguiente.

Tabla 6. Tipos de preguntas

	Preguntas de verdadero/falso o de emparejamiento	Preguntas de respuesta múltiple
Parte general del curso	20%	80%
Parte específica de EFP del curso	20%	80%
Parte del curso específica para la IES	20%	80%
Total para un curso de FP y un curso de IES	20%	80%

DIRECTRICES PARA LA ELABORACIÓN DE PREGUNTAS

Las preguntas de las pruebas de autoevaluación y de evaluación de conocimientos deben prepararse en inglés y luego localizarse a las lenguas de los socios.

A la hora de elaborar las preguntas de las pruebas, tanto para la autoevaluación como para la evaluación de conocimientos dentro del curso, es esencial asegurarse de que las preguntas sean claras, concisas y accesibles para todas las personas candidatas, independientemente de su formación. Este enfoque garantiza que las evaluaciones reflejen con precisión la comprensión por parte de del alumnado del contenido del curso y su capacidad para alcanzar las competencias y objetivos establecidos en el programa del curso.

Directrices generales para la elaboración de preguntas:

Se aplicarán directrices claras en la elaboración de las preguntas de la prueba: las preguntas deben ser comprensibles y estar directamente relacionadas con los objetivos de aprendizaje del curso, sin utilizar terminología compleja ni una redacción confusa. También se evitarán las preguntas culturalmente específicas o confusas para garantizar la equidad y la accesibilidad de todos las personas participantes en el curso. A continuación se ofrecen más orientaciones sobre el diseño de las preguntas.

Claridad y sencillez: las preguntas deben ser directas, evitando el uso de lenguaje complejo o jerga que pueda confundir o inducir a error a las personas candidatas. El objetivo es evaluar los conocimientos y la comprensión del tema por parte de las personas candidatas, no su capacidad para descifrar preguntas complicadas.

Directa y pertinente: cada pregunta debe estar directamente relacionada con las competencias clave y los objetivos del programa del curso. Deben evitarse los contenidos irrelevantes o tangenciales para mantener la atención en la evaluación de los resultados de aprendizaje previstos.

Sensibilidad cultural y de fondo: asegúrese de que las preguntas no presuponen conocimientos o experiencias culturales específicos, haciéndolas accesibles y justas para candidatos de diversos orígenes.

Sin preguntas trampa: la intención de cada pregunta debe ser clara, sin ningún intento de engañar a las personas candidatas. Las preguntas diseñadas para sorprender a las personas candidatas o para poner a prueba su capacidad de detectar engaños no evalúan eficazmente su comprensión del tema.

Presentación inequívoca y concisa: las preguntas deben formularse de forma que no dejen lugar a interpretaciones, garantizando que todos las personas candidatos entiendan la pregunta de la misma manera. Las preguntas deben ser concisas, evitando una extensión innecesaria que pueda ocultar el punto principal.

Redacción positiva: evite utilizar frases negativas en las preguntas (por ejemplo, "¿Cuál de las siguientes NO es..."). Las frases negativas pueden dar lugar a confusiones y malas interpretaciones, sobre todo en situaciones de examen. En su lugar, formula todas las preguntas de forma positiva para fomentar la claridad.

Directrices específicas para la elaboración de preguntas:

Preguntas de opción múltiple: asegúrese de que todas las opciones son plausibles y pertinentes para la pregunta. La respuesta correcta debe ser indiscutiblemente correcta, mientras que las alternativas deben ser claramente incorrectas para alguien que entienda el material.

Preguntas de verdadero/falso: presentan afirmaciones claras y objetivas que se relacionan directamente con el contenido del curso, garantizando que no haya ambigüedad sobre su valor de verdad.

Preguntas de emparejamiento: asegúrese de que ambas listas (por ejemplo, los términos en un lado y las definiciones en el otro) están claramente relacionadas y de que existe una base clara para realizar cada emparejamiento. Evite las listas desiguales en las que el número de elementos no coincida, a menos que se indique explícitamente que algunos elementos no se utilizarán o pueden utilizarse varias veces.

En la formación piloto se analizará la información sobre las metodologías de evaluación de los conocimientos y el proceso de evaluación mediante la recogida de opiniones tanto del alumnado como del personal docente. Esto permitirá evaluar la idoneidad de los métodos de evaluación de conocimientos y, en caso necesario, complementar o mejorar el enfoque de evaluación.

GAMIFICACIÓN

Esta sección presenta la descripción de los elementos de gamificación implementados en los cursos de Ciberagente. La gamificación es el proceso de incorporar los principios de la gamificación a las actividades de aprendizaje tradicionales con el fin de aumentar la motivación y el compromiso de las personas participantes. Estos elementos se han seleccionado basándose

en las últimas investigaciones sobre tecnología educativa, que demuestran que la gamificación puede mejorar significativamente el rendimiento del aprendizaje, aumentar la motivación de las personas estudiantes para aprender y potenciar su compromiso en el proceso de aprendizaje.

Los elementos de gamificación que se integrarán en los cursos incluyen insignias, puntos, rangos y apodos codificados por colores que reflejan la experiencia y los logros de la persona participante.

- Se concederán insignias por:

- **Finalización del módulo**.
- **Por superar una prueba en función del porcentaje de aprobados**. Por ejemplo, una persona participante recibirá una insignia de bronce por una puntuación mínima de aprobado en la prueba final, una insignia de plata por una puntuación mínima de aprobado del 75%, una insignia de oro por una puntuación de aprobado del 76%-90% y una insignia de platino por una puntuación de aprobado del 90%-100%. En este caso, una persona participante puede tener 8 insignias de este tipo.
- **Completando tema**.
- **Entrar en el sistema todos los días durante diez días**.
- El/ la tutor/docente del curso también concederá **una insignia de actividad especial** para cada tema.

- Puntos y puntuaciones calculados sobre la base de las puntuaciones de la prueba de autoevaluación + las puntuaciones de la prueba final con multiplicador.

Las personas participantes en el curso Ciberagente no podrán ver sus progresos individualmente, sino que podrán competir con otras personas participantes en grupos o equipos (en función del mayor número de puntos obtenidos, pero también en función del mayor número de insignias). Esto fomenta no sólo la competición y la cooperación individual, sino también en equipo, lo cual es importante para desarrollar habilidades de cooperación.

Cada participante verá su apodo cuando se conecte al curso, que tendrá un código de colores según el progreso del curso y la experiencia acumulada (cursos completados/registrados).

Esto ayudará a las personas participantes del curso a implicarse mejor en el proceso de formación. Las personas participantes en el curso pueden repetir la misma prueba varias veces para mejorar su puntuación (se conceden puntos por el mayor número de pruebas de autoevaluación realizadas correctamente).

Un algoritmo especial calculará la puntuación de cada participante teniendo en cuenta el tiempo empleado en responder, el número de veces que se repite la prueba y otros parámetros, minimizando así la posibilidad de hacer trampas.

Todas las reglas de gamificación se describirán y comunicarán claramente a las personas participantes para entender fácilmente cómo se pueden alcanzar los distintos niveles de gamificación y cómo se calculan.

7. PROCESO DE APRENDIZAJE/ENSEÑANZA DE CIBERAGENTE

Esta sección resume la información de todos los capítulos de este documento y describe en detalle el proceso de aprendizaje/enseñanza, empezando por la inscripción en un curso de Ciberagente en la plataforma de aprendizaje y terminando con la finalización del curso o la expedición de un certificado.

Los cursos Ciberagente están diseñados para atender a una amplia gama de alumnado, incluidos estudiantes de instituciones de educación superior (IES), estudiantes de educación y formación profesional (EFP), así como personal de PYMES. Nuestro objetivo es dar a cada participante la oportunidad de elegir la forma de aprendizaje que más le convenga, teniendo en cuenta sus circunstancias personales y las políticas organizativas de la institución de formación.

Independientemente del método de aprendizaje/formación elegido, las personas participantes se registran en la plataforma Ciberagente y la utilizan durante la formación.

Inscripción

Las posibles personas interesadas en inscribirse en el curso Ciberagente deben rellenar un formulario de inscripción, seleccionando los módulos que deseen y el método de aprendizaje que prefieran. Se proporciona un diagrama conceptual para guiar a las personas participantes a través del itinerario de aprendizaje desde el primero hasta el octavo módulo de Ciberagente.

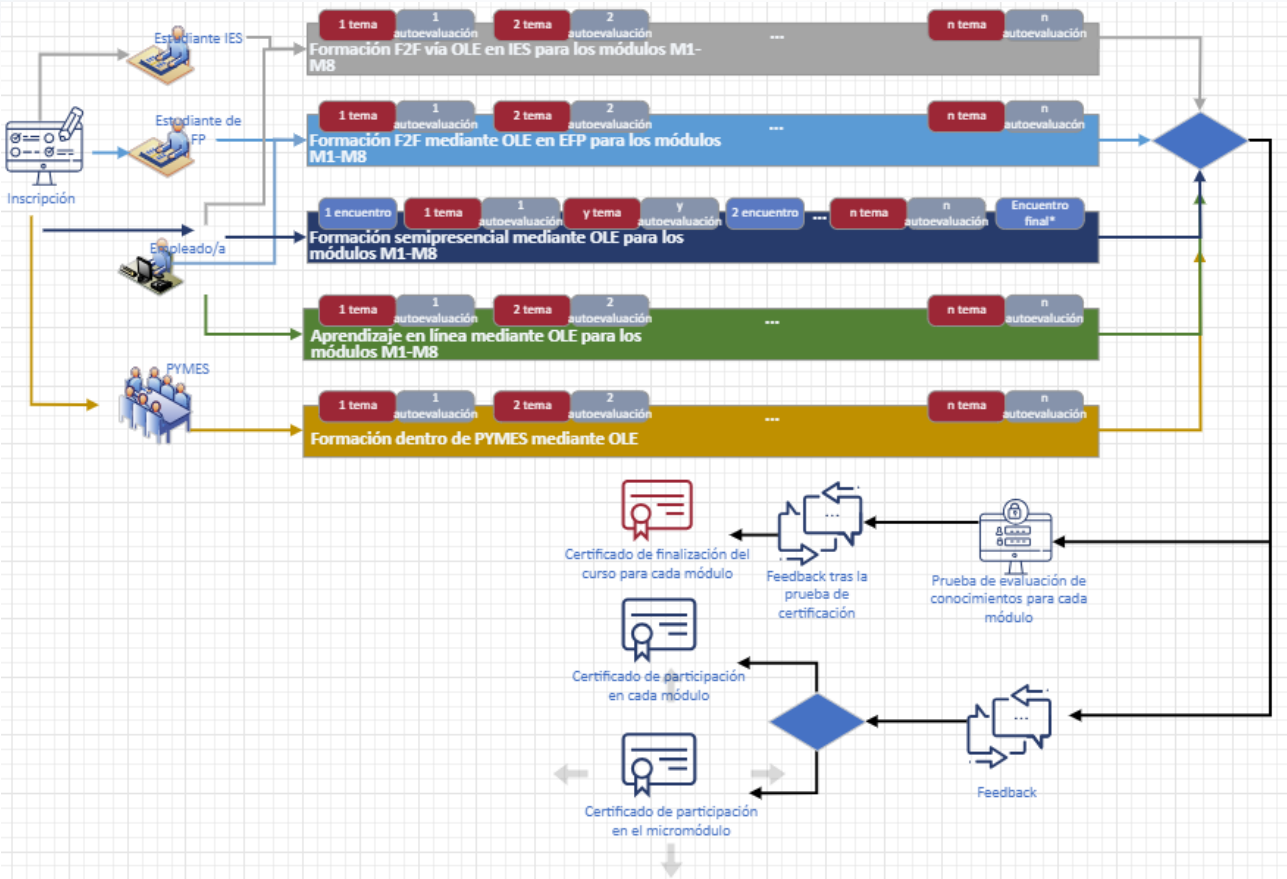


Figura 15. Itinerario de aprendizaje/enseñanza de Ciberagente

Durante el proceso de inscripción se garantizará la confidencialidad de la información de las personas participantes, en particular en lo que respecta a los requisitos del GDPR. Durante la inscripción, las personas participantes tendrán la oportunidad de familiarizarse con las normas de la plataforma de formación, la privacidad y las normas de protección de datos.

Los datos de registro de las personas participantes sólo son accesibles para las personas designadas dentro de la organización de los socios, en cumplimiento de las políticas internas de la organización. Durante las sesiones de formación piloto, los datos de las personas participantes de los socios del proyecto podrán ser accesibles al coordinador del proyecto CyberAgent, y los demás socios no podrán ver los datos de las personas participantes de los demás. Una vez finalizado el proyecto, el coordinador sólo podrá acceder a los datos anonimizados de los demás socios para supervisar los resultados del proyecto, tal y como se especifica en la solicitud del proyecto, hasta 5 años después de su conclusión.

Ofrecemos opciones de formación a medida para satisfacer las necesidades de nuestros diversos grupos destinatarios. Las personas estudiantes de IES y EFP pueden participar en la formación a través de sesiones de contacto con la universidad. El personal de las PYMES pueden elegir el método de aprendizaje que mejor se adapte a sus necesidades: aprendizaje combinado, solo en línea o, con menos frecuencia, asistiendo a clases de IES o EFP.

También se puede ofrecer formación a empresas más grandes con varios empleados. En tales casos, el método de formación se personalizará para satisfacer necesidades específicas, sin dejar de incorporar los cursos del módulo Ciberagente.

Al registrarse en la plataforma, las personas participantes seleccionan su método de aprendizaje y comienzan sus estudios. Tras completar un módulo o parte de un módulo, pueden optar a un Certificado de Participación o a un Certificado de Finalización del Curso, este último expedido si la persona participante supera la prueba del módulo con una puntuación mínima del 75%.

Por último, las personas participantes deben rellenar un formulario de evaluación antes de recibir cualquier certificado. Esta información es crucial para la mejora continua de nuestra oferta de formación y para garantizar la satisfacción de las personas participantes.

Formas de aprendizaje/formación

Las personas empleadas tienen varias opciones para comprometerse con el contenido del curso:

- Si las IES o los centros de EFP permiten al personal empleado asistir como participantes invitados, el empleado o la empleada puede participar en las clases junto con las personas estudiantes matriculadas. Estas sesiones de participantes externos pueden organizarse 1-2 veces al año, en función del calendario de conferencias publicado.
- Las personas empleadas pueden optar por un enfoque de formación semipresencial, en el que las sesiones de formación se imparten en fechas concretas con una duración recomendada de 2 a 4 meses. Se aconsejan grupos de al menos 10 participantes, con un máximo de 30 participantes por grupo. La formación semipresencial incluye consultas presenciales y en línea al principio, durante y al final del curso para facilitar la retroalimentación directa y la preparación de la evaluación final.
- Las personas empleadas pueden elegir la modalidad de aprendizaje en línea para aprender a su propio ritmo, sin una duración determinada para completar el curso.
- En la Sección 1. Vía de estudio se ofrecen más detalles sobre los módulos de Ciberagente.

Participación de las personas estudiantes

Las personas estudiantes matriculadas en el programa de estudios de ciberseguridad pueden encontrar diferentes vías en función de la normativa de su institución académica. Pueden estar obligados a completar algunos o todos los módulos de Ciberagente o, en función de las políticas internas de la universidad, los estudiantes que cumplan los criterios pueden optar por estudiar uno o varios módulos de Ciberagente. Las personas estudiantes de IES o de EFP suelen dedicarse a las asignaturas a través de la enseñanza presencial tradicional impartida por su institución o pueden optar por métodos de autoaprendizaje para prepararse para la prueba final de evaluación de conocimientos.

Participación de las PYMES

En las organizaciones en las que se considere necesaria una formación en ciberseguridad, un representante de la empresa podrá inscribir a la organización en sesiones de formación interna. En tales casos, previo acuerdo por separado con la universidad y/o el personal docente, el método de formación, el calendario y la expedición de certificados podrán adaptarse a las necesidades específicas de la organización basándose en los módulos existentes.

Recogida de comentarios

Una vez finalizado el módulo, las personas participantes deben rellenar un formulario de opinión anónimo accesible en línea. Solo el personal autorizado de la organización asociada puede acceder a los datos de las opiniones, y se aplican medidas de confidencialidad similares durante las sesiones de formación piloto y el uso de datos posterior al proyecto.

Se recogerá principalmente la opinión de las personas participantes en el curso, pero también la de mentores/docentes. El feedback recogido evaluará el nivel de satisfacción organizativa de las personas participantes, aspectos de la organización del curso, el proceso de aprendizaje, el uso de las competencias adquiridas en la práctica, el contenido del curso, las estrategias de evaluación, la inclusión de elementos de gamificación, áreas de mejora, etc.

Los resultados del feedback se revisarán periódicamente y se presentarán al equipo de gestión del proyecto para reaccionar con rapidez y mejorar las estrategias de formación en función de las necesidades reales y los cambios del mercado.

Sólo si rellenan este formulario, las personas participantes podrán obtener un certificado de participación o un certificado de finalización del curso.

Certificado de finalización del curso

La superación de la prueba de evaluación da lugar a la generación de un certificado de finalización del curso para la persona participante. Hay una prueba final por módulo.

Certificado de participación

Las personas participantes que opten por no realizar la prueba de evaluación de conocimientos podrán recibir un certificado de participación. Este reconocimiento puede expedirse al finalizar un único módulo o varias micropartes dentro del curso.

CONCLUSIONES Y RESUMEN

Este informe ha desarrollado con éxito itinerarios de aprendizaje estructurados para los y las agentes del cambio en la ciberseguridad de las PYMES, adaptados para abordar las necesidades específicas en varios niveles educativos y profesionales, desde la enseñanza superior a la formación profesional y la formación directa de las personas empleadas en PYMES. El plan de estudios ideado, que consta de ocho módulos completos, integra competencias técnicas, analíticas, organizativas y de gestión de riesgos que son cruciales para la capacitación efectiva de futuros profesionales de la ciberseguridad.

El enfoque estructurado de los itinerarios de aprendizaje garantiza un itinerario educativo completo para las personas empleadas en las PYMES. A través de las etapas de Preaprendizaje, Aprendizaje y Postaprendizaje, favorece la retención de conocimientos y la aplicación práctica. Los micromódulos ofrecen flexibilidad y adaptabilidad a las necesidades individuales, mejorando el aprendizaje con microcredenciales que proporcionan cualificaciones reconocidas. Esta alineación con los estándares de la industria contribuye significativamente a fortalecer las capacidades de ciberseguridad dentro de las PYMES, preparando a las personas empleadas para afrontar los retos actuales y los avances futuros. El siguiente análisis de Carrera Profesional ha trazado la progresión de las funciones de ciberseguridad definidas por el marco ESCO, facilitando un enfoque educativo específico que prepara a las personas para su integración efectiva en la mano de obra de la ciberseguridad, mejorando en última instancia sus perspectivas de carrera y su desarrollo profesional.

La diversidad explorada de enfoques pedagógicos dentro del plan de estudios de ciberseguridad debe permitir un entorno de aprendizaje dinámico y flexible que se adapte a los diferentes estilos y necesidades de aprendizaje. La incorporación de varios métodos de enseñanza, como clases teóricas, laboratorios prácticos, gamificación y proyectos colaborativos, garantiza que las personas estudiantes no sean solo receptores de conocimientos, sino participantes activos en su viaje de aprendizaje. Esta estrategia global debería aumentar el compromiso y la comprensión y preparar mejor a las personas estudiantes para los retos de ciberseguridad del mundo real. La adaptabilidad de los métodos de enseñanza a los requisitos específicos del módulo debería personalizar aún más la experiencia de aprendizaje, garantizando que los resultados educativos se maximicen para cada estudiante.

Al asignar sistemáticamente los subtemas y módulos del proyecto Ciberagente a unidades de conocimiento reconocidas internacionalmente, el plan de estudios no sólo cumple los requisitos dinámicos del campo de la ciberseguridad, sino que se anticipa a ellos. Este enfoque metódico garantiza que cada resultado del aprendizaje esté estratégicamente vinculado a competencias del mundo real que son cruciales para la gestión eficaz de las amenazas a la ciberseguridad. La adaptabilidad del plan de estudios le permite desempeñar diversas funciones profesionales dentro del sector, preparando al alumnado no sólo para los retos inmediatos, sino también para el desarrollo profesional a largo plazo en el ámbito de la ciberseguridad.

La estrategia de evaluación de cursos descrita ofrece un marco para evaluar la competencia y el progreso de las personas estudiantes en programas de ciberseguridad. El enfoque en dos fases, que combina pruebas de autoevaluación y pruebas exhaustivas de evaluación de conocimientos, permite a las personas estudiantes comprometerse activamente con el material, evaluar continuamente su comprensión y ajustar en consecuencia sus estrategias de aprendizaje. Al diseñar la evaluación para adaptarse tanto a las IES como a estudiantes de EFP con preguntas a medida, la estrategia garantiza la pertinencia y adecuación a cada nivel educativo, mejorando la experiencia de aprendizaje. Este método permite medir claramente el dominio y la preparación de las personas estudiantes para aplicar sus conocimientos en la práctica. Además, la introducción de elementos de gamificación, como insignias y sistemas de puntuación, no sólo motiva a las personas estudiantes, sino que también fomenta un entorno de aprendizaje competitivo pero colaborativo.

Por último, el proceso de aprendizaje y enseñanza de Ciberagente proporciona un marco educativo completo y adaptable adecuado para una amplia gama de alumnos de centros de enseñanza superior, centros de formación profesional y PYMES. Este sistema permite diversos métodos participativos, como el aprendizaje presencial, semipresencial y en línea, garantizando la flexibilidad en la forma de impartir y acceder a la formación en ciberseguridad. La inscripción en la plataforma Ciberagente inicia un itinerario en el que las personas participantes seleccionan los módulos y métodos de aprendizaje preferidos, que culmina con la expedición de certificados una vez completados y evaluados con éxito. Esta estructura no sólo apoya las trayectorias de aprendizaje personalizadas, sino que también se alinea con las rigurosas normas de privacidad esenciales para mantener la confidencialidad de las personas participantes durante todo el proceso de formación.

Las recomendaciones y orientaciones proporcionadas en este documento se utilizarán en la siguiente fase para desarrollar los planes de formación completos de Ciberagente, los materiales de formación, las pruebas y evaluaciones de conocimientos, los ejercicios prácticos y otros contenidos de formación, que se integrarán en la plataforma de formación de Ciberagente.

ANEXO 1. DESCRIPCIÓN DEL MÓDULO

DESCRIPCIÓN DEL MÓDULO

Título del módulo	Código del módulo
...	

Docente(s)	Institución o departamento donde se imparte el módulo
...	...

Modo de entrega	Idioma
Consultas presenciales, en línea, mixtas	*Inglés, ...*

Requisitos previos
...

Número de créditos ECTS asignados	Carga de trabajo del estudiante	Horas de trabajo de contacto	Horas de trabajo individual
5	...	...	...

Finalidad y resultados del módulo		
...		
Resultados de aprendizaje del módulo	**Métodos de enseñanza y aprendizaje**	**Métodos de evaluación**
Competencias técnicas		
Capacidad de análisis		
Habilidades de riesgo		
Capacidad de organización		

Facilitar recursos (equipos, programas informáticos, tecnología)
...

Contenido del módulo: desglose de los temas	Horas de trabajo de contacto					Horas de trabajo y tareas individuales	
	Conferencias (IES/EFP)	Consultas (PYMES)	Prácticas (IES/EFP)	Pruebas	**Todo el trabajo de contacto**	**Trabajo individual**	**Tarea**
1							
…							
n							
Total							

Estrategia de evaluación	Porcentaje en peso comparativo	Criterios de evaluación
Autocomprobación I		…
…		…
Autocomprobación n		…
Prueba de evaluación de conocimientos		…
Certificación IES/EFP -> Autocomprobación I + …+ Autocomprobación n + Prueba de evaluación de conocimientos		
Certificación PYMES/ Certificación de autoaprendizaje -> Autocomprobación I + …+ Autocomprobación n + Prueba de evaluación de conocimientos		
Micromódulos, microsección -> Autocomprobación I (opcional), Autocomprobación n (opcional)		

Material de estudios *(Apellido, Inicial del nombre. (Año, Mes Día). Título del artículo. Título de la revista/periódico/periódico, número de volumen (número de número), números de página de todo el artículo, editorial, URL)*
Lecturas obligatorias
…
Lecturas recomendadas
…

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau