DATOS GENERALES

Curso académico	Curso 2025/2026
Tipo de curso	Microcredencial Universitario
Número de créditos	3,00 Créditos ECTS
Matrícula	135 euros (importe precio público) Preu general
Requisitos de acceso	Dirigida a personas mayores de 24 años y menores de 65. El perfil engloba a todas aquellas personas interesadas en adquirir o actualizar competencias digitales esenciales para su desarrollo personal, académico o profesional. Se recomienda especialmente a quienes desempeñan o aspiran a desempeñar funciones en entornos donde el uso seguro y eficaz de tecnologías digitales, la colaboración en línea y la protección de la información resultan fundamentales. No se requieren conocimientos técnicos específicos previos, aunque sí se valora un manejo básico de dispositivos digitales.
Modalidad	Semipresencial
Lugar de impartición	Aula Virtual ADEIT-UV e Instalaciones ADEIT
Horario	Online

Dirección

Organizador	0
Dirección	Máximo Cobos Serrano Catedrático/a de Universidad. Departament d'Informàtica. Universitat de València

Plazos

Preinscripción al curso	Hasta 16/11/2025
Fecha inicio	Diciembre 2025
Fecha fin	Diciembre 2025

Más información

Teléfono	961 603 000
E-mail	formacion@adeituv.es

PROGRAMA

Competencias digitales y ciberseguridad

Módulo 1: Alfabetización digital e IA aplicada al trabajo digital
Este módulo ofrece una introducción estructurada a los fundamentos del entorno digital y al uso inicial de la inteligencia artificial (IA) aplicada en contextos profesionales. Se abordarán los principios básicos que permiten desenvolverse con solvencia en entornos tecnológicos actuales, así como las herramientas que facilitan el trabajo colaborativo, la organización personal y la gestión de la información en línea. Además, se presentarán aplicaciones prácticas de la IA generativa y los criterios necesarios para su uso responsable y eficaz.
Contenidos:
- Principios básicos del entorno digital: sistemas operativos, navegadores web, correo electrónico, gestores de archivos, calendarios digitales y plataformas de videoconferencia.
- Estrategias para la búsqueda y selección de información fiable; uso del almacenamiento en la nube y evaluación crítica de fuentes digitales.
- Introducción a herramientas colaborativas en línea para la gestión y el desarrollo de tareas compartidas.
- Fundamentos del uso de IA aplicada en el entorno laboral: redacción asistida, asistentes conversacionales y productividad aumentada.
- Buenas prácticas en el uso de herramientas basadas en IA: criterios éticos, limitaciones, responsabilidad y toma de decisiones informadas en entornos profesionales.

Módulo 2: Ciberseguridad básica y protección de datos
Este módulo introduce los fundamentos de la ciberseguridad y la protección de datos desde una perspectiva práctica y crítica. El objetivo es capacitar al alumnado para identificar riesgos digitales habituales y adoptar medidas preventivas que refuercen la seguridad de la información en el uso cotidiano de las tecnologías. Se abordarán también los principios básicos del marco normativo vigente en materia de privacidad, así como los dilemas éticos asociados a la vigilancia digital, el tratamiento de datos personales y el uso de IA con fines tanto defensivos como maliciosos.
Contenidos:- Principales amenazas en entornos digitales: phishing, malware, ransomware y errores humanos vinculados al

factor humano.
- Medidas básicas de protección: gestión de contraseñas, sistemas de autenticación, navegación segura y prácticas recomendadas de autoprotección.
- Introducción al Reglamento General de Protección de Datos (RGPD): derechos del usuario, consentimiento informado, privacidad y tratamiento responsable de la información personal.
- Impacto ético y social de la ciberseguridad: vigilancia digital, sesgos algorítmicos y responsabilidad en la toma de decisiones automatizadas.
- IA y ciberseguridad: análisis de usos ofensivos (como los deepfakes) y defensivos (como la detección de patrones de ataque o actividad sospechosa).

Módulo 3: Ciberseguridad aplicada (prevención y actuación ante incidentes)
Este módulo profundiza en la dimensión aplicada de la ciberseguridad, centrándose en la prevención activa de riesgos y en la capacidad de respuesta ante incidentes digitales en contextos reales. A partir del análisis de situaciones concretas, el alumnado desarrollará criterios y herramientas para detectar amenazas, adoptar medidas preventivas eficaces y actuar de forma responsable ante posibles vulneraciones de seguridad. Asimismo, se promoverá una reflexión crítica sobre los dilemas éticos asociados al uso de datos personales, la privacidad digital y la inteligencia artificial en el marco de la cultura de la ciberseguridad.
Contenidos:
- Análisis de casos reales y simulación de amenazas comunes (phishing, suplantación de identidad, accesos no autorizados, entre otros).
- Recomendaciones prácticas para la prevención: hábitos digitales seguros, herramientas de protección y protocolos de mejora continua.
- Respuesta ante incidentes de ciberseguridad: pautas de actuación, recursos disponibles y canales institucionales de ayuda.
- Debate y reflexión crítica: dilemas éticos actuales relacionados con la privacidad, la inteligencia artificial y el uso de datos personales.

PROFESORADO

Régis Cazenave

Autónomo

Máximo Cobos Serrano

Catedrático/a de Universidad. Departament d'Informàtica. Universitat de València

Miguel García Pineda

Profesor/a Titular de Universidad. Departament d'Informàtica. Universitat de València

OBJETIVOS

Las salidas profesionales que tiene el curso son:

Esta microcredencial mejora la empleabilidad en múltiples sectores al fortalecer competencias digitales clave demandadas en el mercado laboral actual. Resulta especialmente útil para profesionales de cualquier ámbito que deseen desenvolverse con mayor seguridad y eficacia en entornos digitales, así como para quienes trabajan en contextos donde la protección de datos, la ciberseguridad o el uso ético de la inteligencia artificial tienen un papel relevante. También aporta valor añadido a perfiles administrativos, técnicos, educativos y de gestión que requieran actualizar sus habilidades digitales en el marco de la transformación tecnológica.

El objetivo principal de esta microcredencial es capacitar a los participantes para desenvolverse de forma competente, segura y responsable en entornos digitales, tanto personales como profesionales. A través de un enfoque aplicado y transversal, el curso permite desarrollar habilidades fundamentales en alfabetización digital, colaboración en línea, protección de datos y ciberseguridad, integrando además nociones prácticas sobre el uso de la inteligencia artificial como parte del ecosistema tecnológico actual. Se busca no solo la adquisición de competencias técnicas, sino también la comprensión crítica del impacto social, ético y normativo asociado al uso de tecnologías digitales en la vida cotidiana y en el ejercicio profesional.

METODOLOGÍA

La metodología del curso combina aprendizaje online asincrónico, actividades de interacción guiada y una sesión final especializada, en modalidad presencial o síncrona en línea. Se fundamenta en principios de aprendizaje activo, significativo y orientado a la práctica profesional, con un enfoque centrado en la resolución de situaciones reales, el desarrollo de competencias aplicadas y la reflexión crítica sobre el uso de tecnologías digitales.
La docencia online se estructura a partir de materiales multimedia interactivos, incluyendo vídeos breves, lecturas estructuradas, infografías y simulaciones prácticas, que permiten al estudiante avanzar de forma autónoma y flexible. Esta

dimensión se complementa con foros de discusión y tutorías supervisadas, concebidos como espacios de acompañamiento, intercambio de experiencias y análisis de buenas prácticas digitales.
A lo largo del curso, los participantes tendrán acceso a cuestionarios de autoevaluación y retos aplicados que favorecen la consolidación del aprendizaje y permiten evidenciar de forma progresiva la adquisición de competencias. De manera opcional, se ofrecerán sesiones síncronas centradas en demostraciones prácticas, resolución de dudas y orientación para el proceso de evaluación.
La microcredencial culmina con una sesión final impartida por una persona experta en ciberseguridad, orientada a la resolución colaborativa de incidentes simulados, el análisis crítico de casos reales y la reflexión compartida sobre la cultura de la seguridad digital en contextos profesionales. Esta propuesta metodológica garantiza un equilibrio entre flexibilidad, aplicabilidad y exigencia formativa, permitiendo al estudiante adaptar su ritmo de aprendizaje sin renunciar al acompañamiento docente ni a la profundidad en los contenidos.