

DADES GENERALS

Curs acadèmic	Curs 2025/2026
Tipus de curs	Microcredencial Universitari
Nombre de crèdits	3,00 Crèdits ECTS
Matrícula	135 euros (import preu públic)
Requisits d'accés	Dirigida a persones majors de 24 anys i menors de 65. El perfil engloba a totes aquelles persones interessades a adquirir o actualitzar competències digitals essencials per al seu desenvolupament personal, acadèmic o professional. Es recomana especialment als qui exerceixen o aspiren a exercir funcions en entorns on l'ús segur i eficaç de tecnologies digitals, la col·laboració en línia i la protecció de la informació resulten fonamentals. No es requereixen coneixements tècnics específics previs, encara que sí que es valora un maneig bàsic de dispositius digitals.
Modalitat	Semipresencial
Lloc d'impartició	Aula Virtual ADEIT-UV e Instalaciones ADEIT
Horari	Online
Direcció	
Organitzador	0
Direcció	Máximo Cobos Serrano Catedrático/a de Universidad. Departament d'Informàtica. Universitat de València
Terminis	
Preinscripció al curs	Fins a 16/11/2025
Data inici	Desembre 2025
Data fi	Desembre 2025
Més informació	
Telèfon	961 603 000
E-mail	formacion@adeituv.es

PROGRAMA

Mòdul 1: Alfabetització digital i IA aplicada al treball digital

Aquest mòdul ofereix una introducció estructurada als fonaments de l'entorn digital i a l'ús inicial de la intel·ligència artificial (IA) aplicada en contextos professionals. S'abordan els principis bàsics que permeten desembolicar-se amb solvència en entorns tecnològics actuals, així com les eines que faciliten el treball col·laboratiu, l'organització personal i la gestió de la informació en línia. A més, es presentaran aplicacions pràctiques de la IA generativa i els criteris necessaris per al seu ús responsable i eficaç.

Continguts:

- Principis bàsics de l'entorn digital: sistemes operatius, navegadors web, correu electrònic, gestors d'arxius, calendaris digitals i plataformes de videoconferència.
- Estratègies per a la cerca i selecció d'informació fiable; ús de l'emmagatzematge en el núvol i avaluació crítica de fonts digitals.
- Introducció a eines col·laboratives en línia per a la gestió i el desenvolupament de tasques compartides.
- Fonaments de l'ús d'IA aplicada en l'entorn laboral: redacció assistida, assistents conversacionals i productivitat augmentada.
- Bones pràctiques en l'ús d'eines basades en IA: criteris ètics, limitacions, responsabilitat i presa de decisions informades en entorns professionals.

Mòdul 2: Ciberseguretat bàsica i protecció de dades

Aquest mòdul introdueix els fonaments de la ciberseguretat i la protecció de dades des d'una perspectiva pràctica i crítica.

L'objectiu és capacitar a l'alumnat per a identificar riscos digitals habituals i adoptar mesures preventives que reforcen la seguretat de la informació en l'ús quotidià de les tecnologies. S'abordan també els principis bàsics del marc normatiu vigent en matèria de privacitat, així com els dilemes ètics associats a la vigilància digital, el tractament de dades personals i l'ús d'IA amb finalitats tant defensius com maliciosos.

Continguts:- 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.

PROFESSORAT

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

OBJECTIUS

Les sortides professionals que té el curs són:

Aquesta microcredencial millora l'ocupabilitat en múltiples sectors en enfortir competències digitals clau demandades en el mercat laboral actual. Resulta especialment útil per a professionals de qualsevol àmbit que desitgen desembolicar-se amb major seguretat i eficàcia en entorns digitals, així com per als qui treballen en contextos on la protecció de dades, la ciberseguretat o l'ús ètic de la intel·ligència artificial tenen un paper rellevant. També aporta valor afegit a perfils administratius, tècnics, educatius i de gestió que requereixen actualitzar les seues habilitats digitals en el marc de la transformació tecnològica.

L'objectiu principal d'aquesta microcredencial és capacitar als participants per a desembolicar-se de manera competent, segura i responsable en entorns digitals, tant personals com professionals. A través d'un enfocament aplicat i transversal, el curs permet desenvolupar habilitats fonamentals en alfabetització digital, col·laboració en línia, protecció de dades i ciberseguretat, integrant a més nocions pràctiques sobre l'ús de la intel·ligència artificial com a part de l'ecosistema tecnològic actual. Se cerca no sols l'adquisició de competències tècniques, sinó també la comprensió crítica de l'impacte social, ètic i normatiu associat a l'ús de tecnologies digitals en la vida quotidiana i en l'exercici professional

METODOLOGÍA

La metodologia del curs combina aprenentatge en línia asincrònic, activitats d'interacció guiada i una sessió final especialitzada, en modalitat presencial o síncrona en línia. Es fonamenta en principis d'aprenentatge actiu, significatiu i orientat a la pràctica professional, amb un enfocament centrat en la resolució de situacions reals, el desenvolupament de competències aplicades i la reflexió crítica sobre l'ús de tecnologies digitals.

La docència en línia s'estructura a partir de materials multimèdia interactius, incloent-hi vídeos breus, lectures estructurades, infografies i simulacions pràctiques, que permeten a l'estudiant avançar de manera autònoma i flexible. Aquesta dimensió es complementa amb fòrums de discussió i tutories supervisades, concebuts com a espais d'acompanyament, intercanvi d'experiències i anàlisis de bones pràctiques digitals.

Al llarg del curs, els participants tindran accés a qüestionaris d'autoavaluació i reptes aplicats que afavoreixen la consolidació de l'aprenentatge i permeten evidenciar de manera progressiva l'adquisició de competències. De manera opcional, s'oferiran sessions síncrones centrades en demostracions pràctiques, resolució de dubtes i orientació per al procés d'avaluació.

La microcredencial culmina amb una sessió final impartida per una persona experta en ciberseguretat, orientada a la resolució col·laborativa d'incidents simulats, l'anàlisi crítica de casos reals i la reflexió compartida sobre la cultura de la seguretat digital en contextos professionals. Aquesta proposta metodològica garanteix un equilibri entre flexibilitat, aplicabilitat i exigència formativa, permetent a l'estudiant adaptar el seu ritme d'aprenentatge sense renunciar a l'acompanyament docent ni a la profunditat en els continguts.