

Desarrollo
profesional y personal

Curso académico 2025-2026

Forense digital

del 13 de enero al 24 de abril de 2026

8 créditos ECTS

MICROCREDENCIAL

Características: prácticas y visitas, material impreso, material multimedia, página web, curso virtual y guía didáctica.

Departamento

Sistemas de Comunicación y Control

E.t.s. de Ingeniería Informática



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA, INNOVACIÓN
Y UNIVERSIDADES



Plan de Recuperación,
Transformación
y Resiliencia



upgrade hub

Destinatarios

Edad: 25-64 (obligatorio según normativa gubernamental para el Plan Microcred) No requiere titulación previa

1. Título del resultado de aprendizaje: Comprender y aplicar los fundamentos legales y conceptuales del análisis forense digital en el contexto de la ciberseguridad
2. Tipo: Conocimiento 3. Capacidades ESCO relacionadas: Ciberseguridad 1. Título del resultado de aprendizaje: Evidenciar y documentar incidentes de ciberseguridad 2. Tipo: Capacidad 3. Capacidades ESCO relacionadas: Gestionar incidentes de ciberseguridad 1. Título del resultado de aprendizaje: Evaluar la seguridad de la información en un entorno TIC 2. Tipo: Capacidad 3. Capacidades ESCO relacionadas: Identificar riesgos de seguridad de las TIC 1. Título del resultado de aprendizaje: Proponer soluciones técnicas para la mejora de la seguridad en la información de cualquier organización 2. Tipo: Conocimiento 3. Capacidades ESCO relacionadas: contramedidas frente a ataques informáticos 1. Título del resultado de aprendizaje: Marco jurídico profesional del forense digital
2. Tipo: Conocimiento 3. Capacidades ESCO relacionadas: legislación sobre seguridad de las TIC Los estudiantes que se gradúen en esta microcredencial serán capaces de identificar, preservar y evidenciar un incidente de ciberseguridad en diferentes entornos como son los dispositivos IoT, entornos cloud, dispositivos móviles, PC o Servidores, utilizando herramientas técnicas profesionales de uso extendido y reconocido en el mercado laboral. La labor pericial va más allá del aspecto puramente técnico, y debe materializarse sabiendo construir un informe técnico profesional que se pueda argumentar y defender como perito judicial ante un tribunal o ante responsables de seguridad en la información de cualquier organización, lo que es por tanto igualmente importante en la formación adquirida por los estudiantes que cursen esta microcredencial.

Este curso oferta únicamente 42 plazas.

Este curso está subvencionado con Fondos de Recuperación Next Generation de la UE, por lo que el **precio de matrícula que abonará el alumno es de 373.68 €**

1. Objetivos

Esta microcredencial está destinada a dotar de capacidades técnicas y metodologías profesionales en el ámbito forense y pericial de profesionales relacionados con el ámbito de las tecnologías de la información y las comunicaciones o del ámbito judicial, para ello facilitará sensiblemente tener conocimientos previos en sistemas operativos, redes de comunicaciones y bases de datos relacionales. Esta formación permitirá a estos profesionales poder desarrollarse dentro del sector de la ciberseguridad en uno de los entornos más específicos y de mayor demanda profesional actual como es el ámbito pericial y forense y del compliance.

Resultados de aprendizaje (máximo 5 por logro)

1. Título del resultado de aprendizaje: Comprender y aplicar los fundamentos legales y conceptuales del análisis forense digital en el contexto de la ciberseguridad

2. Tipo: Conocimiento

3. Capacidades ESCO relacionadas: Ciberseguridad

1. Título del resultado de aprendizaje: Evidenciar y documentar incidentes de ciberseguridad

2. Tipo: Capacidad

3. Capacidades ESCO relacionadas: Gestionar incidentes de ciberseguridad

1. Título del resultado de aprendizaje: Evaluar la seguridad de la información en un entorno TIC

2. Tipo: Capacidad

3. Capacidades ESCO relacionadas: Identificar riesgos de seguridad de las

TIC

1. Título del resultado de aprendizaje: Proponer soluciones técnicas para la mejora de la seguridad en la información de cualquier organización

2. Tipo: Conocimiento

3. Capacidades ESCO relacionadas: contramedidas frente a ataques informáticos

1. Título del resultado de aprendizaje: Marco jurídico profesional del forense digital

2. Tipo: Conocimiento

3. Capacidades ESCO relacionadas: legislación sobre seguridad de las TIC

Los estudiantes que se gradúen en esta microcredencial serán capaces de identificar, preservar y evidenciar un incidente de ciberseguridad en diferentes entornos como son los dispositivos IoT, entornos cloud, dispositivos móviles, PC o Servidores, utilizando herramientas técnicas profesionales de uso extendido y reconocido en el mercado laboral.

La labor pericial va más allá del aspecto puramente técnico, y debe materializarse sabiendo construir un informe técnico profesional que se pueda argumentar y defender como perito judicial ante un tribunal o ante responsables de seguridad en la información de cualquier organización, lo que es por tanto igualmente importante en la formación adquirida por los estudiantes que cursen esta microcredencial.

2. Contenidos

Módulo 1: Introducción al Forense Digital

Módulo 2. Creación de entornos virtuales para la labor pericial

Módulo 3: Aplicación de la técnica forense en el entorno digital

Módulo 4: Metodología profesional de la práctica forense digital

Módulo 5: Proyecto Final

3. Metodología y actividades

El curso se impartirá con la metodología Habitual de la UNED. A través de su plataforma, los estudiantes tendrán acceso a los contenidos. De especial importancia en este curso son la Prácticas y Laboratorios ya que es una microcredencial totalmente práctica. Por ello, la metodología de evaluación será personal, síncrona online y grabadas.

Asimismo, la trayectoria de Upgrade Hub en el ámbito de la formación tecnológica intensiva aporta un valor añadido a esta microcredencial. La entidad ha contribuido a la incorporación o mejora profesional de más de 3.000 personas en el sector digital, gracias a metodologías orientadas a resultados, colaboración con empresas del ecosistema y acompañamiento personalizado del alumnado. La integración de esta experiencia práctica y conexión con el tejido empresarial en el diseño y ejecución de la microcredencial supone una garantía adicional para la empleabilidad de sus participantes.

4. Nivel del curso

5. Duración y dedicación

Duración: del martes 13 de enero al viernes 24 de abril de 2026.

Dedicación: 200 horas.

6. Equipo docente

Director/a

Director - UNED

HERNANDEZ BERLINCHES, ROBERTO

Directores adjuntos

Director adjunto - Externo

BRIONES BERMEJO, JOAQUÍN

Colaboradores externos

Colaborador - Externo

ARIZA CÍVICO, DIEGO

Colaborador - Externo

BLANCO ARÉVALO, MANUEL

Colaborador - Externo

BRIONES BERMEJO, JOAQUÍN

Colaborador - Externo

SANDOVAL, ANGEL

Colaborador - Externo

VELASCO HERNANDEZ, ANDRES

7. Material didáctico para el seguimiento del curso

7.1 Material obligatorio

7.1.1 Material en Plataforma Virtual

Todos los pdf, vídeos y guías para los laboratorios

7.1.2 Material enviado por el equipo docente (apuntes, pruebas de evaluación, memorias externas, DVDs,)

Licencias de los programas propietarios

8. Información adicional sobre titulaciones ofertadas sometidas al SAIC

Para la oferta de esta microcredencial se han valorado los siguientes aspectos:

- La coherencia del plan de estudios con los objetivos formativos definidos.
- La adecuación de la estructura del Plan de Estudios a la duración prevista.
- La idoneidad del equipo docente propuesto, con experiencia acreditada tanto en docencia como en investigación en el área de conocimiento correspondiente.
- La disponibilidad de los recursos humanos y materiales suficientes para garantizar su impartición con calidad.

- La existencia de una demanda social y/o profesional que justifique la oferta de la microcredencial.
- El cumplimiento con los criterios de calidad establecidos en la normativa vigente de la universidad (SAICU-P03-C2-v01-e01) [Proceso para el aseguramiento de la calidad de los Másteres de Formación Permanente, microcredenciales y otros títulos propios de la UNED] y en el Real Decreto 822/2021, en lo que respecta a las enseñanzas de formación permanente.

La microcredencial a la que da acceso la presente acción formativa es impartida en español, de forma virtual por las entidades UNED y Upgrade-hub entre los días 13 de enero de 2026 y 24 de abril de 2026, siendo asimilable a un nivel MECU 2 correspondiente a Certificación de superación de 2º de la ESO. Certificado de Formación Profesional de Grado Básico..

El logro resultante de la consecución de la microcredencial implica la acreditación de los siguientes resultados de aprendizaje y competencias asociadas:

Resultado de aprendizaje	Tipo	Competencias ESCO
Comprender y aplicar los fundamentos legales y conceptuales del análisis forense digital en el contexto de la ciberseguridad	Conocimiento	Ciberseguridad: Los métodos y las mejores prácticas de protección de sistemas TIC, redes, ordenadores, dispositivos, servicios, procesos y personas contra accesos o modificaciones no autorizados o contra la denegación de servicio de los activos.
Evidenciar y documentar incidentes de ciberseguridad	Capacidad	Gestionar incidentes de ciberseguridad: Detectar, identificar, analizar y responder a incidentes de ciberseguridad en los sistemas o redes de una organización. Implica adoptar planes de respuesta a incidentes, como sistemas de detección de intrusiones, análisis de registros y documentación detallada sobre posibles incidentes.
Evaluar la seguridad de la información en un entorno TIC	Capacidad	Identificar riesgos de seguridad de las TIC: Aplicar métodos y técnicas para identificar posibles amenazas de seguridad, violaciones de seguridad y factores de riesgo con el empleo de herramientas de TIC para inspeccionar los sistemas de TIC, analizar riesgos, vulnerabilidades y amenazas y evaluar planes de contingencia.
Proponer soluciones técnicas para la mejora de la seguridad en la información de cualquier organización	Conocimiento	Contra medidas frente a ataques informáticos: Métodos, tecnologías y técnicas utilizados en la defensa (detección, supervisión y recuperación) contra ciberataques. Estos ciberataques incluyen varios vectores de ataque, como programas maliciosos, ataques de denegación de servicio (DoS) y suplantación de identidad («phishing»). Algunos ejemplos de métodos utilizados son los sistemas de prevención de intrusiones (IPS), los cortafuegos, los antivirus, los sistemas de detección de intrusos (IDS), la formación en ciberseguridad, las copias de seguridad, el sistema de gestión de la seguridad de la información (SGSI), la autenticación multifactor y tomar conciencia de los riesgos.
Marco jurídico profesional del forense digital	Conocimiento	Legislación sobre seguridad de las TIC: El conjunto de normas legislativas que protegen la tecnología de la información, las redes de TIC y los sistemas informáticos, así como las consecuencias jurídicas resultantes de su uso indebido. Entre las medidas reguladas figuran cortafuegos, detección de intrusiones, software antivirus y cifrado.

Los resultados de aprendizaje de esta microcredencial se alinean con la clasificación CINE-F (0719), que corresponde al ámbito de "Ingeniería y profesiones afines no contempladas en la clasificación".

La evaluación de los conocimientos y competencias adquiridos se realiza a través de una tarea puntuable denominada "". Esta se realiza de forma virtual, siendo la supervisión y verificación del estudiantado matriculado supervisada en línea con verificación de la identidad.

Esta formación permitirá a estos profesionales poder desarrollarse dentro del sector de la ciberseguridad en uno de los entornos más específicos y de mayor demanda profesional actual como es el ámbito pericial y forense y del compliance.

9. Atención al estudiante

ROBERTO HERNÁNDEZ roberto@scc.uned.es Martes de 15.00 a 19.00 h 913987196

10. Criterios de evaluación y calificación

La metodología de evaluación para los estudiantes de esta microcredencial se basará en 3 formatos diferenciados y que son obligatorios de realizar por parte de cada estudiante de forma individual: 1. Cuatro pruebas en formato de test 2. Siete pruebas de evaluación en forma de prácticas y laboratorios a completar por cada estudiante de forma individual, 3. Realización de un ejercicio final que incluirá la documentación y redacción de un informe forense ante un incidente de ciberseguridad y la posterior defensa del contenido y conclusiones de dicho informe forense ante un tribunal formado por el director académico y un docente por un tiempo no superior a los 15 minutos. Cada una de las pruebas de evaluación se realizará en fecha y hora específica de forma on line síncrona con la presencia de un profesor y utilizando las herramientas técnicas o plataforma de formación necesaria para poder realizar la prueba. Las evaluaciones serán grabadas. La defensa del ejercicio final de forma online síncrona se realizará de forma individual por parte de cada estudiante ante un tribunal formado por un profesor y el director académico por parte de Upgrade Hub en fecha y hora establecida. La defensa será grabada.

Sistema de calificación:

La ponderación de la nota final de estudiante será: Ø Test de evaluación 5% Ø Pruebas de evaluación 35% Ø Prueba y defensa del trabajo final: 60%

11. Descuentos

11.1 Ayudas al estudio y descuentos

Se puede encontrar información general sobre ayudas al estudio y descuentos en [este enlace](#).

Debe hacer la solicitud de matrícula marcando la opción correspondiente, y posteriormente enviar la documentación al correo: descuentos@fundacion.uned.es.

12. Matriculación

Del 20 de octubre de 2025 al 12 de enero de 2026.

Información de matrícula:

Fundación UNED

C/ Guzmán el Bueno, 133 - Edificio Germania, 9ª planta

28003 Madrid

Teléfonos: +34913867275/1592

lvillacorta@fundacion.uned.es

ATENCIÓN!!

En el momento de realización de la solicitud de matrícula debe marcar la subvención Fondos del plan de Recuperación, Transformación y Resiliencia Componente 21 Microcredenciales, de forma que, aunque el precio de la matrícula del curso es 1245,60 €, solo se le cobrará 30% del importe la de matrícula, es decir 373.68 €.

13. Responsable administrativo

Negociado de Institucionales.