IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

1. DATOS DE LA UNIVERSIDAD, CENTRO Y TÍTULO QUE PRESENTA LA SOLICITUD

De conformidad con el Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad.

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad Intercontinental de la Empresa	Facultad de Ingeniería y Tecnología Empresarial (Campus de A Coruña)	15028865
	Facultad de Ingeniería y Tecnología Empresarial (Campus de Vigo)	36020775

NIVEL	DENOMINACIÓN CORTA
Máster	Ciberseguridad

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Ciberseguridad por la Universidad Intercontinental de la Empresa

NIVEL MECES
3

RAMA DE CONOCIMIENTO	CAMPO DE ESTUDIO	CONJUNTO
Ingeniería y Arquitectura	Ingeniería informática y de sistemas	No

SOLICITANTE

NOMBRE Y APELLIDOS	CARGO
MIGUEL ÁNGEL ESCOTET ÁLVAREZ	Rector

REPRESENTANTE LEGAL

NOMBRE Y APELLIDOS	CARGO
MIGUEL ÁNGEL ESCOTET ÁLVAREZ	Rector

RESPONSABLE DEL TÍTULO

NOMBRE Y APELLIDOS	CARGO
BEATRIZ CHECCHIA COTTI	Coordinadora General Académica

2. DIRECCIÓN A EFECTOS DE NOTIFICACIÓN

A los efectos de la práctica de la NOTIFICACIÓN de todos los procedimientos relativos a la presente solicitud, las comunicaciones se dirigirán a la dirección que figure en el presente apartado.

DOMICILIO	CÓDIGO POSTAL	MUNICIPIO	TELÉFONO
Rúa Nova 33	15705	Santiago de Compostela	608295092
E-MAIL	**PROVINCIA**		**FAX**
notificaciones@uie.edu	A Coruña		

3. PROTECCIÓN DE DATOS PERSONALES

De acuerdo con lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley Orgánica 3/2018, de 5 de diciembre, sin perjuicio de lo dispuesto en otra normativa que ampare los derechos como cedentes de los datos de carácter personal.

El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

	En: A Coruña, AM 12 de septiembre de 2025
	Firma: Representante legal de la Universidad

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

1.1-1.3 DENOMINACIÓN, CAMPO DE ESTUDIO, MENCIONES/ESPECIALIDADES Y OTROS DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Ciberseguridad por la Universidad Intercontinental de la Empresa	No		Ver Apartado 1: Anexo 1.

RAMA
Ingeniería y Arquitectura
CAMPO DE ESTUDIO
Ingeniería informática y de sistemas
AGENCIA EVALUADORA
Axencia para a Calidade do Sistema Universitario de Galicia
LISTADO DE ESPECIALIDADES
No existen datos
MENCIÓN DUAL
No

1.4-1.9 UNIVERSIDADES, CENTROS, MODALIDADES, CRÉDITOS, IDIOMAS Y PLAZAS

UNIVERSIDAD SOLICITANTE
Universidad Intercontinental de la Empresa

LISTADO DE UNIVERSIDADES	
CÓDIGO	**UNIVERSIDAD**
097	Universidad Intercontinental de la Empresa

LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	**UNIVERSIDAD**
No existen datos	

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60		6
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
0	48	6

1.4-1.9 Universidad Intercontinental de la Empresa

1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS			
CÓDIGO	**CENTRO**	**CENTRO RESPONSABLE**	**CENTRO ACREDITADO INSTITUCIONALMENTE**
15028865	Facultad de Ingeniería y Tecnología Empresarial (Campus de A Coruña)	No	No
36020775	Facultad de Ingeniería y Tecnología Empresarial (Campus de Vigo)	Si	No

1.4-1.9.2 Facultad de Ingeniería y Tecnología Empresarial (Campus de Vigo)

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TITULO		
PRESENCIAL	**SEMIPRESENCIAL/HÍBRIDA**	**A DISTANCIA/VIRTUAL**
Sí	No	No
PLAZAS POR MODALIDAD		
30		

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

NÚMERO TOTAL DE PLAZAS	NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO	
30	30	
IDIOMAS EN LOS QUE SE IMPARTE		
CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	VALENCIANO	INGLÉS
Sí	No	No
FRANCÉS	ALEMÁN	PORTUGUÉS
No	No	No
ITALIANO	OTRAS	
No	No	

1.4-1.9.2 Facultad de Ingeniería y Tecnología Empresarial (Campus de A Coruña)

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TITULO		
PRESENCIAL	SEMIPRESENCIAL/HÍBRIDA	A DISTANCIA/VIRTUAL
Sí	No	No
PLAZAS POR MODALIDAD		
30		
NÚMERO TOTAL DE PLAZAS	NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO	
30	30	
IDIOMAS EN LOS QUE SE IMPARTE		
CASTELLANO	CATALÁN	EUSKERA
Sí	No	No
GALLEGO	VALENCIANO	INGLÉS
Sí	No	No
FRANCÉS	ALEMÁN	PORTUGUÉS
No	No	No
ITALIANO	OTRAS	
No	No	

1.10 JUSTIFICACIÓN

JUSTIFICACIÓN DEL INTERÉS DEL TÍTULO Y CONTEXTUALIZACIÓN
Ver Apartado 1: Anexo 6.

1.11-1.13 OBJETIVOS FORMATIVOS, ESTRUCTURAS CURRICULARES ESPECÍFICAS Y DE INNOVACIÓN DOCENTE

OBJETIVOS FORMATIVOS

1.11 Principales objetivos formativos del título.

El egresado o egresada de este Máster Universitario en Ciberseguridad de la UIE será un profesional altamente cualificado en la protección de datos y sistemas de información, con habilidades técnicas y el conocimiento de los requerimientos normativos y legales para liderar iniciativas de ciberseguridad en organizaciones de cualquier sector, tanto públicas como privadas.

Se trata, por tanto, de un egresado con un perfil que combina competencias técnicas avanzadas con una sólida comprensión del marco normativo y de gestión, y que estará capacitado para gestionar los nuevos riesgos cibernéticos en un entorno altamente complejo y cambiante, y en el que el uso de la Inteligencia Artificial va a desempeñar un papel cada vez más relevante tanto en las estrategias y técnicas defensivas como en el desarrollo de nuevas amenazas y tipos de ataques cada vez más sofisticados.

A los objetivos relativos a la adquisición de conocimientos específicos, se añaden los que se refieren a la obtención de habilidades de carácter transversal: búsqueda e interpretación de información, pensamiento crítico y creativo, resolución de problemas, manejo de plataformas digitales, dominio de la comunicación oral y escrita, etc.

El egresado o egresada del Máster Universitario en Ciberseguridad será capaz de:

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

1. Protección de sistemas y datos
- Diseñar, implementar y auditar medidas de seguridad para la protección de sistemas de información, redes y datos, aplicando estándares y buenas prácticas internacionales, como la ISO 27001, la Directiva NIS-2 o el ENS en España.
- Identificar vulnerabilidades en infraestructuras tecnológicas mediante herramientas de análisis, pruebas de penetración y técnicas de evaluación de riesgos.

2. Gestión de riesgos y gobernanza de la seguridad
- Analizar y gestionar riesgos de ciberseguridad en todo tipo de organizaciones privadas, definiendo planes de mitigación y de continuidad de negocio.
- Diseñar e implantar sistemas de gestión de la seguridad de la información (SGSI) alineados con los objetivos estratégicos de la organización.

3. Cumplimiento normativo y legal
- Interpretar y aplicar el marco normativo vigente en materia de ciberseguridad y protección de datos (incluyendo RGPD, NIS2 y normativa sectorial aplicable).
- Evaluar el impacto legal y regulatorio de incidentes de seguridad y definir medidas de cumplimiento.

4. Respuesta ante incidentes
- Detectar, analizar y responder a incidentes de ciberseguridad mediante técnicas de monitorización, análisis forense y gestión de crisis.
- Coordinar equipos y procedimientos de respuesta ante incidentes en entornos organizativos complejos.

5. Arquitecturas y tecnologías de seguridad
- Diseñar arquitecturas seguras en entornos cloud, híbridos y on-premise, incorporando mecanismos de autenticación, control de acceso y protección de datos.
- Evaluar e integrar herramientas y soluciones de ciberseguridad en función de las necesidades de la organización.
- Facilitar el desarrollo seguro de aplicaciones y la integración de soluciones adecuadas a través de la cadena de suministros.

6. Inteligencia Artificial aplicada a la ciberseguridad
- Aplicar técnicas de Inteligencia Artificial y análisis de datos para la detección de amenazas, anomalías y patrones de ataque.
- Evaluar los riesgos asociados al uso de IA en ciberseguridad, incluyendo ataques adversariales, automatización de amenazas y uso malicioso de modelos.

7. Competencias transversales aplicadas
- Analizar información técnica y estratégica para la toma de decisiones en ciberseguridad.
- Comunicar de forma clara y estructurada riesgos, incidentes y soluciones tanto a perfiles técnicos como no técnicos.
- Resolver problemas complejos en entornos inciertos mediante pensamiento crítico y creativo.
- Trabajar en equipos multidisciplinares y ser capaz de gestionar proyectos en el ámbito de la ciberseguridad.

1.12 Estructuras curriculares específicas y justificación de sus objetivos.

No procede.

1.13 Estrategias metodológicas de innovación docente específicas y justificación de sus objetivos.

La UIE está comprometida con brindar una educación diferenciada, con altos estándares de calidad y excelencia, en un entorno productivo y enriquecedor, en donde los miembros de la comunidad universitaria puedan crecer, desarrollarse y prosperar.

La Universidad pretende dotar a los estudiantes de rasgos distintivos propios que permitan su desarrollo humano integral como miembros de una sociedad, con valores, compromiso social y responsabilidad medioambiental, para lo cual incorpora en su modelo académico características como:

- Modelo comprehensivo y vanguardista.
- Competencias transversales interdisciplinares para la vida.
- Sistema centrado en el estudiante, flexible y personalizado.
- Aprendizaje experiencial dentro y fuera del aula.
- Experiencia multicultural.

ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO		
Especializado a nivel técnico y normativo en ciberseguridad, amenazas, tecnologías y estrategias de protección en redes, dispositivos y software.		
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	No	
NO ES CONDICIÓN DE ACCESO PARA TITULO PROFESIONAL		

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

RPFA-COMP-01 - Evaluar y gestionar riesgos aplicando las metodologías más extendidas. TIPO: Competencias
RPFA-COMP-02 - Gestionar procesos de auditoría y de certificación. TIPO: Competencias
RPFA-COMP-03 - Evaluar los distintos tipos de ciberdelitos y su tratamiento legal. TIPO: Competencias
RPFA-COMP-04 - Comprender y aplicar principios de criptografía para proteger la información. TIPO: Competencias
RPFA-COMP-05 - Diseñar e implementar medidas de seguridad en redes de ordenadores. TIPO: Competencias
RPFA-COMP-06 - Identificar y mitigar vulnerabilidades comunes en el código fuente (inyecciones SQL, XSS, CSRF, etc.). TIPO: Competencias
RPFA-COMP-07 - Ejecutar estrategias efectivas frente a los ciberincidentes. TIPO: Competencias
RPFA-COMP-08 - Diseñar planes de contención, erradicación y recuperación tras un incidente. TIPO: Competencias
RPFA-COMP-09 - Identificar vulnerabilidades y riesgos de ciberseguridad en sistemas de IA. TIPO: Competencias
RPFA-COMP-10 - Evaluar los riesgos éticos y regulatorios de la IA aplicada a la ciberseguridad. TIPO: Competencias
RPFA-COMP-11 - Desarrollar un trabajo profesional en un entorno laboral con responsabilidad, ética y eficiencia. TIPO: Competencias
RPFA-COMP-12 - Elaborar, redactar y defender un proyecto con rigor académico y científico, que resuelva un problema dentro del ámbito del conocimiento de la titulación y con una complejidad y alcance. TIPO: Competencias
RPFA-CONO-01 - Integrar y aplicar los principios de gobierno y gestión de la seguridad en una organización. TIPO: Conocimientos o contenidos
RPFA-CONO-02 - Analizar la complejidad del marco normativo en ciberseguridad. TIPO: Conocimientos o contenidos
RPFA-CONO-03 - Integrar normativas sectoriales específicas relacionadas con la ciberseguridad. TIPO: Conocimientos o contenidos
RPFA-CONO-04 - Analizar la regulación aplicable a la Inteligencia Artificial. TIPO: Conocimientos o contenidos
RPFA-CONO-05 - Interpretar los principios de la ingeniería social TIPO: Conocimientos o contenidos
RPFA-CONO-06 - Analizar el estado actual, las aplicaciones y las limitaciones de las técnicas biométricas. TIPO: Conocimientos o contenidos
RPFA-CONO-07 - Diagnosticar los problemas de seguridad que afectan a smartphones y dispositivos IoT. TIPO: Conocimientos o contenidos
RPFA-CONO-08 - Determinar los principios del desarrollo seguro y su importancia en el ciclo de vida del software. TIPO: Conocimientos o contenidos
RPFA-CONO-09 - Determinar los elementos clave para garantizar la continuidad de negocio. TIPO: Conocimientos o contenidos
RPFA-CONO-10 - Contrastar el impacto de la IA en el ámbito de la ciberseguridad, tanto en defensa como en ataques. TIPO: Conocimientos o contenidos
RPFA-CONO-11 - Analizar la estructura, el funcionamiento y las normas de un entorno laboral real. TIPO: Conocimientos o contenidos
RPFA-CONO-12 - Sintetizar y desarrollar las competencias de la titulación para desarrollar un proyecto dentro del ámbito de la profesión. TIPO: Conocimientos o contenidos
RPFA-HABI-01 - Diseñar y aplicar estrategias de cumplimiento para la obtención de certificaciones como la ISO 27001. TIPO: Habilidades o destrezas
RPFA-HABI-02 - Identificar y analizar amenazas y agentes maliciosos en el ciberespacio TIPO: Habilidades o destrezas
RPFA-HABI-03 - Ejecutar técnicas de ciberinteligencia OSINT y análisis de información pública. TIPO: Habilidades o destrezas
RPFA-HABI-04 - Diseñar estrategias para mitigar el riesgo ligado al factor humano. TIPO: Habilidades o destrezas
RPFA-HABI-05 - Implementar los principios básicos en materia de protección de datos. TIPO: Habilidades o destrezas
RPFA-HABI-06 - Implementar sistemas seguros de autenticación. TIPO: Habilidades o destrezas
RPFA-HABI-07 - Configurar las herramientas de protección en dispositivos y equipos de usuarios. TIPO: Habilidades o destrezas
RPFA-HABI-08 - Aplicar metodologías de desarrollo seguro (DevSecOps, OWASP, SDL de Microsoft) en proyectos reales. TIPO: Habilidades o destrezas
RPFA-HABI-09 - Implementar controles de seguridad en diferentes lenguajes de programación y frameworks. TIPO: Habilidades o destrezas

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

RPFA-HABI-10 - Analizar código y detectar vulnerabilidades mediante herramientas de análisis estático y dinámico. TIPO: Habilidades o destrezas
RPFA-HABI-11 - Detectar y analizar vulnerabilidades. TIPO: Habilidades o destrezas
RPFA-HABI-12 - Utilizar técnicas y herramientas avanzadas de monitorización y análisis forense. TIPO: Habilidades o destrezas
RPFA-HABI-13 - Aplicar técnicas de IA y Machine Learning en detección de amenazas y análisis forense digital. TIPO: Habilidades o destrezas
RPFA-HABI-14 - Analizar el uso de IA en la automatización de respuestas ante incidentes de seguridad. TIPO: Habilidades o destrezas
RPFA-HABI-15 - Aplicar la normativa laboral del entorno donde se desarrolla la práctica, utilizar las competencias adquiridas y seleccionar los conceptos y herramientas adecuadas para resolver problemas propios del ejercicio profesional. TIPO: Habilidades o destrezas
RPFA-HABI-16 - Utilizar con autonomía los recursos bibliográficos, documentales, la capacidad de análisis y seleccionar los conceptos, métodos y herramientas apropiadas para resolver un problema complejo. TIPO: Habilidades o destrezas

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

3.1 Admisión y Permanencia.

El procedimiento de acceso a las titulaciones de Posgrado de la UIE será el establecido en el artículo 38 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación y en el artículo 31 de la Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario. Asimismo, se estará a lo dispuesto en artículo 18 del Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad.

El Área de Admisiones es la encargada de gestionar y organizar el proceso de admisión de los estudiantes, velando por el cumplimiento tanto de la legislación referida al acceso a las enseñanzas de Posgrado como de la normativa de acceso interno de la UIE.

Respecto a la selección, se seguirán los principios de objetividad, imparcialidad, mérito y capacidad.

Respecto a las ponderaciones de los criterios de admisión, se incluyen las siguientes: Expediente Académico (30%), Curriculum Vitae (10%), Resultado de la Prueba Psicotécnica (10%), Valoración de la Entrevista Personal (40%) y Nivel de inglés (10%). Toda esta información estará disponible para los estudiantes en la página web de la universidad.

Una vez evaluado el expediente del candidato por el Área de Admisiones, si el candidato cumple con los requisitos establecidos y existen plazas disponibles, la admisión será concedida de forma inmediata.

La nota ponderada deberá alcanzar el 6 sin que exista un mínimo para cada una de las pruebas realizadas. Es decir, no se establece una puntuación mínima para cada criterio, sino para el promedio de las calificaciones resultantes de los cinco criterios de admisión.

La adjudicación de plazas se efectuará a medida que los candidatos cumplan con los requisitos de admisión, hasta completar el número total de plazas ofertadas.

Asimismo, aquellos estudiantes con talento, pero sin capacidad económica, dispondrán de un amplio sistema de becas que les permitan cursar sus estudios en la UIE.

Finalmente, en cumplimiento de lo establecido en el RD 822/2021, se recoge la reserva de un 5% de plazas para estudiantes que tengan reconocido un grado de discapacidad igual o superior al 33%, así como estudiantes con necesidades de apoyo educativo permanentes.

En el Anexo II puede consultarse la Normativa de Admisión y Permanencia.

Perfil de ingreso.

Si bien no constituyen requisitos indispensables, se recomienda que el estudiante que accede a la titulación reúna las siguientes cualidades:

- Haber cursado algún grado o licenciatura del área científico-tecnológica, entre los cuales se podrían incluir (de forma no exhaustiva):
  - Grado en Ingeniería Informática.
  - Grado en Ingeniería de Telecomunicación.
  - Grado en Ingeniería Industrial o similar con orientación TIC.
  - Grado en Matemáticas.
  - Grado en Físicas.
  - Grado en Ciencias de la Computación.
  - También podrían acceder otros titulados en áreas científicas o técnicas que acrediten competencias o experiencia profesional en entornos tecnológicos.
  - De manera excepcional se podrían admitidos titulados en otras áreas (ADE, Derecho, etc.) si acreditan experiencia profesional o formación complementaria suficiente en tecnologías de la información, y demuestran una clara motivación para el estudio de la ciberseguridad.
- El estudiante deberá contar con conocimientos básicos o intermedios en las siguientes áreas:
  - Sistemas operativos (Windows y Linux).
  - Redes de ordenadores y protocolos de comunicación.
  - Administración básica de sistemas.
  - Fundamentos de bases de datos.
  - Lenguajes de programación: Python, C/C++, Java, etc.

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

- También sería recomendable tener un nivel de inglés técnico intermedio-alto (para facilitar la lectura de documentación y normas internacionales), así como capacidad de trabajo en equipo, pensamiento analítico y actitud proactiva ante los retos tecnológicos.

El acceso al Máster Universitario en Ciberseguridad de la UIE se orienta prioritariamente a titulados universitarios del ámbito de las Tecnologías de la Información y las Comunicaciones (TIC), que dispongan de una base sólida en sistemas, redes y programación.

1. Perfiles de acceso prioritario (sin necesidad de complementos formativos)

Tendrán acceso directo, sin necesidad de cursar complementos formativos, los titulados en las siguientes titulaciones oficiales del sistema universitario español (lista no exhaustiva y abierta a las modificaciones del mapa de titulaciones de dicho sistema universitario):

- Grado en Ingeniería Informática.
- Grado en Ingeniería de Telecomunicación.
- Grado en Ingeniería Telemática.
- Grado en Ingeniería de Sistemas de Información.
- Grado en Ingeniería del Software.
- Grado en Ingeniería de Computadores.
- Grado en Ciencia de Datos / Data Science.
- Grado en Ciencias de la Computación.
- Grado en Ingeniería en Tecnologías de la Información

Asimismo, podrán acceder directamente titulados en programas equivalentes de universidades extranjeras que puedan acreditar resultados de aprendizaje análogos.

2. Perfiles de acceso afines (con posibles complementos formativos)

Podrán ser admitidos, condicionados a la realización de complementos formativos, los titulados en:

- Grado en Ingeniería Industrial.
- Grado en Ingeniería Electrónica Industrial y Automática.
- Grado en Ingeniería Eléctrica.
- Grado en Ingeniería Mecánica (con formación en automatización o sistemas digitales).
- Grado en Matemáticas.
- Grado en Física.
- Grado en Estadística.
- Otras ingenierías con contenidos relevantes en programación, sistemas o redes.

La necesidad de cursar complementos se determinará en función del expediente académico y/o experiencia profesional acreditada.

3. Perfiles de acceso no TIC (con complementos formativos obligatorios)

De forma excepcional, podrán ser admitidos titulados en otras áreas de conocimiento, tales como:

- Grado en Administración y Dirección de Empresas.
- Grado en Derecho.
- Grado en Economía.
- Otros grados del ámbito de las ciencias sociales.

En estos casos, la admisión estará condicionada a que la persona candidata pueda acreditar experiencia profesional en entornos tecnológicos o digitales.

Además, deberá superar obligatoriamente los complementos formativos definidos por el programa.

4. Conocimientos previos requeridos

Con carácter general, los estudiantes deberán poseer (o adquirir mediante complementos formativos) conocimientos en:

- Sistemas operativos (especialmente Linux).
- Redes de computadores (modelo OSI/TCP-IP, direccionamiento, protocolos).
- Programación (preferentemente Python o C/C++).
- Administración básica de sistemas.
- Fundamentos de bases de datos.

Asimismo, se recomienda un nivel de inglés equivalente a B2 que permita la comprensión de documentación técnica.

5. Complementos formativos

Con el objetivo de garantizar la adquisición de los resultados de aprendizaje del Máster, los estudiantes que no acrediten los conocimientos previos necesarios deberán cursar complementos formativos obligatorios, con una carga de hasta 12 ECTS, estructurados en los siguientes módulos:

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

- Fundamentos de Sistemas Operativos
  - Contenidos:
    - Arquitectura de sistemas operativos.
    - Administración básica de Linux.
    - Gestión de usuarios, procesos y permisos.
    - Introducción a scripting y manejo del intérprete de comandos (bash).
  - Resultados de aprendizaje:
  - Administrar sistemas Linux en entornos básicos.
  - Configurar servicios esenciales de un sistema operativo.
- Redes de Ordenadores y Fundamentos de Internet
- Contenidos:
  - Modelo OSI y TCP/IP.
  - Direccionamiento IP.
  - Protocolos básicos de red (HTTP, DNS, DHCP, etc.).
- Resultados de aprendizaje:
- Comprender y analizar el tráfico de red.
- Configurar redes básicas.
- Contenidos:
  - Programación estructurada y pensamiento computacional.
  - Introducción a Python.
  - Manipulación de estructuras de datos.
  - Conceptos básicos de algoritmos.
  - Introducción a Bases de Datos y al lenguaje de consulta SQL.
- Resultados de aprendizaje:
- Desarrollar scripts básicos para automatización de tareas.
- Comprender código y la implementación de los algoritmos.
- Configurar servicios básicos de bases de datos.
- Fundamentos de Ciencias de Computación y Bases de Datos

La Coordinación Académica del Máster determinará, en cada caso, los complementos a cursar en función del perfil del estudiante.

Normas de permanencia.

Se aplicará la normativa de permanencia de la UIE para los títulos de posgrado, de cuyo contenido los estudiantes serán adecuadamente informados, adoptándose las medidas precisas para dejar constancia de su conocimiento y aceptación.

Dicha normativa no será aplicable a estudiantes de intercambio procedentes de otras universidades, que se regirán en lo que compete a esta normativa, por el acuerdo, convenio o normativa que le afecte.

Disposiciones generales

La permanencia de los estudiantes estará condicionada por su aprovechamiento académico, así como por el cumplimiento de la normativa interna de la institución y los compromisos suscritos en los contratos de enseñanza-aprendizaje de cada asignatura y el Código Ético de la Universidad.

Asistencia a las actividades formativas del plan de estudios

Los estudiantes tienen la obligación de asistir a todas las actividades previstas para cada asignatura del plan de estudios, debiendo justificar su presencia en al menos el noventa por ciento (90 %). Los responsables académicos correspondientes podrán eximir parcialmente la asistencia por motivos debidamente acreditados.

Índice Ponderado de Permanencia (IPP) / *Global Performance Average* (GPA)

El estudiante deberá obtener un IPP mínimo de 7 sobre 10 en el primer semestre académico y un mínimo de 7 sobre 10 acumulado para poder realizar la defensa del Trabajo Fin de Máster. Excepcionalmente Algunos másteres pueden requerir un IPP menor a 7 pero nunca menor de 6. En caso de no cumplir este requisito, el estudiante no podrá optar al título de Máster.

El IPP es el resultado de la suma aritmética de los créditos en los que se haya matriculado el estudiante, multiplicados cada uno de éstos por el valor de las calificaciones numéricas obtenidas, dividiendo por el número total de créditos.

A efectos de su cálculo, en la siguiente tabla se establecen las equivalencias entre los sistemas de calificación numéricos y alfanuméricos.

Tabla 9 - Equivalencia entre sistemas de calificaciones

Sistema alfanumérico	Sistema numérico	Equivalencia	
A+	10	9,0 - 10	Sobresaliente
A	9,5		
A-	9		
B+	8,5	7,0 - 8,9	Notable
B	8		
B-	7,5		
C+	7		
C	6,5	5,0 - 6,9	Aprobado
C-	6		
D+	5,5		
D	5		

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

D-	4,5	0,0 - 4,9	Suspenso
F	<4,5		

La mención de #Matrícula de Honor# podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola #Matrícula de Honor#.

De la evaluación y las convocatorias.

El plan docente de cada asignatura establecerá el sistema de evaluación aplicable en función de los principios contenidos en esta Memoria.

Los estudiantes tienen derecho a dos convocatorias en cada asignatura; excepcionalmente, el Comité de Coordinación Académica podrá conceder hasta dos convocatorias adicionales en caso de concurrir situaciones extraordinarias debidamente acreditadas.

Los estudiantes no pueden renunciar a las convocatorias, pero cabe obtener la dispensa de aquellas a las que les resulte imposible concurrir por causa debidamente justificada.

Otras disposiciones.

Los estudiantes con necesidades educativas especiales o que cursan estudios a tiempo parcial, que no puedan atenerse a estas disposiciones, deberán plantear cada año su situación antes de formalizar la matrícula, a fin de adaptarla a sus posibilidades de dedicación al estudio.

En el Anexo II se adjunta la Normativa de Admisión y Permanencia, también disponible en la web.

Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional.

3.2 CRITERIOS PARA EL RECONOCIMIENTO Y TRANSFERENCIAS DE CRÉDITOS	
Reconocimiento de Créditos cursados en centros de formación profesional de grado superior	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Convenio	
Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Título Propio	
Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	6
DESCRIPCIÓN	

3.2 Reconocimiento y transferencia de créditos.

La transferencia y reconocimiento de créditos se realizará en concordancia con lo establecido en el artículo 10 del RD 822/2021 y según la normativa de la UIE. Con objeto de hacer efectiva la movilidad de estudiantes, la UIE constituirá una Comisión de Reconocimiento y Transferencia de Créditos que valorará el expediente y los documentos académicos oficiales del estudiante a estos efectos.

Se entiende por reconocimiento la aceptación por la Universidad de los créditos que, habiendo sido obtenidos en unas enseñanzas oficiales, en la misma u otra Universidad, son computados en la titulación de destino a efectos de la obtención de un título oficial, sustituyendo a determinados créditos de dicha titulación. Tal como se indica en el Real Decreto 822/2021, de 28 de septiembre, podrán ser objeto de reconocimiento los créditos cursados en otras enseñanzas superiores oficiales o en enseñanzas universitarias conducentes a la obtención de otros títulos universitarios sin carácter oficial. Se establece igualmente que podrá ser objeto de reconocimiento la experiencia laboral y profesional acreditada en forma de créditos que computarán a efectos de la obtención de un título oficial, siempre que dicha experiencia esté relacionada con las competencias inherentes a dicho título.

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

La transferencia de créditos implica que, en los documentos académicos oficiales acreditativos de las enseñanzas seguidas por cada estudiante, se incluirán la totalidad de los créditos obtenidos en enseñanzas oficiales cursadas con anterioridad, en la misma u otra Universidad, aunque no hayan conducido a la obtención de un título oficial. La UIE transferirá al expediente académico de sus estudiantes, previa petición del interesado, todos los créditos obtenidos en enseñanzas oficiales cursadas en esta Universidad o en otra Universidad del Espacio Europeo de Educación Superior (EEES).

Así, todos los créditos obtenidos por el estudiante en estudios oficiales cursados en cualquier Universidad, tanto los transferidos, como los reconocidos y los cursados para la obtención del correspondiente título, serán incluidos en su expediente académico y reflejados en el Suplemento Europeo al título.

El sistema de reconocimiento de créditos de la UIE está basado en la acreditación de competencias y se podrá reconocer créditos en los estudios oficiales de Máster Universitario teniendo en cuenta la adecuación entre las competencias y conocimientos previstos en el plan de estudios de la titulación y las adquiridas en otras enseñanzas cursadas por el estudiante o en una previa experiencia profesional.

Se podrán reconocer créditos por:

- Estudios universitarios previos de nivel de Máster realizados en otra universidad española o extranjera.
- Estudios en otras enseñanzas superiores oficiales del mismo nivel.
- Experiencia profesional o laboral

El reconocimiento se hará preferentemente con cargo a asignaturas y siempre que la formación recibida garantice que se cubran y alcancen al menos el 75% de los contenidos y competencias de las asignaturas de la titulación de destino. No obstante, podrán ser reconocidos créditos correspondientes a asignaturas cursadas sin necesidad de establecer una correspondencia con asignaturas del plan de destino.

En ningún caso, el Trabajo Fin de Máster podrá ser objeto de reconocimiento de créditos.

El reconocimiento de créditos por estudios universitarios previos o experiencia profesional o laboral no incorporará la calificación de los mismos y no se tendrá en cuenta en el cálculo de la nota media del expediente.

Reconocimiento de créditos por asignaturas de otros Másteres de la UIE.

Los responsables de los Másteres podrán autorizar el reconocimiento de créditos de asignaturas pertenecientes a otros Másteres de la UIE teniendo en cuenta la adecuación entre las competencias y conocimientos adquiridos y los previstos en el plan de estudios.

Los créditos se podrán reconocer con calificación cuando los responsables de los Másteres consideren que las asignaturas reconocidas se integran en el plan de estudios del Máster de destino. En estos casos, las calificaciones computarán a efectos del cálculo de la nota media del expediente académico. Cuando no sea así, se incorporarán al expediente del estudiante como reconocidas y sin calificación, por lo que no computarán en el cálculo de la nota media.

Estudios cursados en titulaciones oficiales en universidades extranjeras.

La Universidad podrá reconocer directamente o mediante convenios, titulaciones extranjeras que den acceso a titulaciones oficiales de la UIE o establecer en esos convenios el reconocimiento parcial de los estudios extranjeros.

En el Anexo III se adjunta la Normativa de Reconocimiento y Transferencia de Créditos, también disponible en la web.

La UIE reconocerá, en los términos establecidos en la normativa de gestión académica de programas de intercambio, los créditos obtenidos en universidades extranjeras cuando el estudiante participe en programas de intercambio, con su correspondiente calificación.

Fuera de los programas de intercambio, para el reconocimiento de créditos obtenidos en titulaciones extranjeras será requisito indispensable que la titulación de origen tenga carácter oficial en el país de la institución que expide el título y que todas las certificaciones académicas sean expedidas por autoridades competentes para expedir títulos de acuerdo con las disposiciones legales, reglamentarias o administrativas del Estado del que procedan. Si la titulación de origen está adaptada al esquema del Espacio Europeo de Educación Superior (EEES) y utiliza el sistema de créditos ECTS, los créditos reconocidos, en su caso, corresponderán a los créditos de las asignaturas de origen. Si la titulación de origen no hace uso del sistema de créditos ECTS, la Comisión de Reconocimiento y Transferencia de Créditos del centro será la encargada de establecer el número de créditos reconocidos a partir de la formación recibida, garantizando que cada crédito reconocido se hace con cargo a unas horas docentes de al menos el 35% del valor del crédito.

Enseñanzas universitarias no oficiales y experiencia laboral.

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

La experiencia laboral y profesional podrá ser reconocida por la asignatura de Prácticas Externas (6 ECTS) siempre que esa experiencia se muestre estrechamente relacionada con las competencias, conocimientos y habilidades (resultados de aprendizaje) inherentes al título y se encuentre debidamente acreditada y explícita en el informe de Vida Laboral y la certificación de la entidad empleadora. La Comisión de Reconocimiento y Transferencia de Créditos será la encargada de evaluar si dicha experiencia es susceptible de reconocimiento. Para el reconocimiento de las prácticas externas sólo se considerarán periodos de actividad profesional no inferiores a 12 meses, asignándose 6 créditos.

3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA

3.3 Movilidad.

Los programas de movilidad de la UIE perseguirán el desarrollo de profesionales abiertos al mundo, con competencias interculturales y motivados a compartir conocimientos y experiencias desde un prisma de respeto a lo diferente. A nivel docente contribuirá a la innovación en la oferta académica y metodologías docentes y al desarrollo de proyectos de investigación. Con este fin la movilidad tendrá carácter transversal y estará dirigida a todos los sectores de la comunidad universitaria UIE. No obstante, en el Máster Universitario en Ciberseguridad, dadas sus características y duración, no se prevén estancias internacionales ni nacionales.

4. PLANIFICACIÓN DE LAS ENSEÑANZAS

4.1 ESTRUCTURA BÁSICA DE LAS ENSEÑANZAS

DESCRIPCIÓN DEL PLAN DE ESTUDIOS

Ver Apartado 4: Anexo 1.

NIVEL 1: Formación de Especialización

4.1.1 Datos Básicos del Nivel 1

ECTS NIVEL1	48

NIVEL 2: Gestión de la Seguridad de la Información

4.1.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	18

DESPLIEGUE TEMPORAL: Semestral

ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
12	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

NIVEL 3: Gobierno de la Seguridad, Análisis de Riesgos y Certificación

4.1.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral

DESPLIEGUE TEMPORAL

ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

NIVEL 3: Ciberinteligencia, Amenazas y Ciberdelitos. Ingeniería Social y Factor Humano

4.1.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral

DESPLIEGUE TEMPORAL

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Marco Regulatorio de la Ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
RPFA-COMP-01 - Evaluar y gestionar riesgos aplicando las metodologías más extendidas. TIPO: Competencias		
RPFA-COMP-02 - Gestionar procesos de auditoría y de certificación. TIPO: Competencias		
RPFA-COMP-03 - Evaluar los distintos tipos de ciberdelitos y su tratamiento legal. TIPO: Competencias		
RPFA-CONO-01 - Integrar y aplicar los principios de gobierno y gestión de la seguridad en una organización. TIPO: Conocimientos o contenidos		
RPFA-CONO-02 - Analizar la complejidad del marco normativo en ciberseguridad. TIPO: Conocimientos o contenidos		
RPFA-CONO-03 - Integrar normativas sectoriales específicas relacionadas con la ciberseguridad. TIPO: Conocimientos o contenidos		
RPFA-CONO-04 - Analizar la regulación aplicable a la Inteligencia Artificial. TIPO: Conocimientos o contenidos		
RPFA-CONO-05 - Interpretar los principios de la ingeniería social TIPO: Conocimientos o contenidos		
RPFA-HABI-01 - Diseñar y aplicar estrategias de cumplimiento para la obtención de certificaciones como la ISO 27001. TIPO: Habilidades o destrezas		
RPFA-HABI-02 - Identificar y analizar amenazas y agentes maliciosos en el ciberespacio TIPO: Habilidades o destrezas		
RPFA-HABI-03 - Ejecutar técnicas de ciberinteligencia OSINT y análisis de información pública. TIPO: Habilidades o destrezas		
RPFA-HABI-04 - Diseñar estrategias para mitigar el riesgo ligado al factor humano. TIPO: Habilidades o destrezas		
RPFA-HABI-05 - Implementar los principios básicos en materia de protección de datos. TIPO: Habilidades o destrezas		
NIVEL 2: Técnicas de Ciberseguridad		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	30	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
18	12	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Criptografía, Autenticación y Biometría		

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Seguridad en las Redes y en los Dispositivos		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Seguridad en el Software y Desarrollo Seguro de Aplicaciones		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
6		
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Técnicas de Análisis, de Defensa y de Respuesta a Incidentes		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Ciberseguridad e Inteligencia Artificial		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Obligatoria	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
RPFA-HABI-09 - Implementar controles de seguridad en diferentes lenguajes de programación y frameworks. TIPO: Habilidades o destrezas		
RPFA-HABI-10 - Analizar código y detectar vulnerabilidades mediante herramientas de análisis estático y dinámico. TIPO: Habilidades o destrezas		
RPFA-HABI-11 - Detectar y analizar vulnerabilidades. TIPO: Habilidades o destrezas		
RPFA-HABI-12 - Utilizar técnicas y herramientas avanzadas de monitorización y análisis forense. TIPO: Habilidades o destrezas		
RPFA-HABI-14 - Analizar el uso de IA en la automatización de respuestas ante incidentes de seguridad. TIPO: Habilidades o destrezas		
RPFA-HABI-13 - Aplicar técnicas de IA y Machine Learning en detección de amenazas y análisis forense digital. TIPO: Habilidades o destrezas		
RPFA-COMP-04 - Comprender y aplicar principios de criptografía para proteger la información. TIPO: Competencias		
RPFA-COMP-05 - Diseñar e implementar medidas de seguridad en redes de ordenadores. TIPO: Competencias		
RPFA-COMP-06 - Identificar y mitigar vulnerabilidades comunes en el código fuente (inyecciones SQL, XSS, CSRF, etc.). TIPO: Competencias		
RPFA-COMP-07 - Ejecutar estrategias efectivas frente a los ciberincidentes. TIPO: Competencias		
RPFA-COMP-08 - Diseñar planes de contención, erradicación y recuperación tras un incidente. TIPO: Competencias		
RPFA-COMP-09 - Identificar vulnerabilidades y riesgos de ciberseguridad en sistemas de IA. TIPO: Competencias		
RPFA-COMP-10 - Evaluar los riesgos éticos y regulatorios de la IA aplicada a la ciberseguridad. TIPO: Competencias		
RPFA-CONO-06 - Analizar el estado actual, las aplicaciones y las limitaciones de las técnicas biométricas. TIPO: Conocimientos o contenidos		
RPFA-CONO-07 - Diagnosticar los problemas de seguridad que afectan a smartphones y dispositivos IoT. TIPO: Conocimientos o contenidos		
RPFA-CONO-08 - Determinar los principios del desarrollo seguro y su importancia en el ciclo de vida del software. TIPO: Conocimientos o contenidos		
RPFA-CONO-09 - Determinar los elementos clave para garantizar la continuidad de negocio. TIPO: Conocimientos o contenidos		
RPFA-CONO-10 - Contrastar el impacto de la IA en el ámbito de la ciberseguridad, tanto en defensa como en ataques. TIPO: Conocimientos o contenidos		
RPFA-HABI-06 - Implementar sistemas seguros de autenticación. TIPO: Habilidades o destrezas		
RPFA-HABI-07 - Configurar las herramientas de protección en dispositivos y equipos de usuarios. TIPO: Habilidades o destrezas		
RPFA-HABI-08 - Aplicar metodologías de desarrollo seguro (DevSecOps, OWASP, SDL de Microsoft) en proyectos reales. TIPO: Habilidades o destrezas		
NIVEL 1: Prácticas Académicas Externas		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	6	
NIVEL 2: Prácticas Académicas Externas		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
ECTS NIVEL 2	6	

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Prácticas Externas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Prácticas Externas	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
RPFA-HABI-15 - Aplicar la normativa laboral del entorno donde se desarrolla la práctica, utilizar las competencias adquiridas y seleccionar los conceptos y herramientas adecuadas para resolver problemas propios del ejercicio profesional. TIPO: Habilidades o destrezas		
RPFA-COMP-11 - Desarrollar un trabajo profesional en un entorno laboral con responsabilidad, ética y eficiencia. TIPO: Competencias		
RPFA-CONO-11 - Analizar la estructura, el funcionamiento y las normas de un entorno laboral real. TIPO: Conocimientos o contenidos		
NIVEL 1: Trabajo Fin de Máster		
4.1.1 Datos Básicos del Nivel 1		
ECTS NIVEL1	6	
NIVEL 2: Trabajo Fin de Máster		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Semestral		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**
	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**
NIVEL 3: Trabo Fin de Máster		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Trabajo Fin de Grado / Máster	6	Semestral
DESPLIEGUE TEMPORAL		
ECTS Semestral 1	**ECTS Semestral 2**	**ECTS Semestral 3**

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

	6	
ECTS Semestral 4	**ECTS Semestral 5**	**ECTS Semestral 6**
ECTS Semestral 7	**ECTS Semestral 8**	**ECTS Semestral 9**
ECTS Semestral 10	**ECTS Semestral 11**	**ECTS Semestral 12**

4.1.1.2 RESULTADOS DE APRENDIZAJE

RPFA-COMP-12 - Elaborar, redactar y defender un proyecto con rigor académico y científico, que resuelva un problema dentro del ámbito del conocimiento de la titulación y con una complejidad y alcance. TIPO: Competencias

RPFA-CONO-12 - Sintetizar y desarrollar las competencias de la titulación para desarrollar un proyecto dentro del ámbito de la profesión. TIPO: Conocimientos o contenidos

RPFA-HABI-16 - Utilizar con autonomía los recursos bibliográficos, documentales, la capacidad de análisis y seleccionar los conceptos, métodos y herramientas apropiadas para resolver un problema complejo. TIPO: Habilidades o destrezas

4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES

ACTIVIDADES FORMATIVAS

4.2 Actividades y metodologías docentes.

La clasificación de las modalidades organizativas de las actividades de enseñanza- aprendizaje en la UIE se realiza, por una parte, atendiendo al carácter de la modalidad y por otra según su tipo.

Las modalidades formativas se clasifican en: introductoria, teórica, guiada, personalizada, autónoma, ApS y seguimiento.

Tabla 16 - Modalidades organizativas de las actividades E-A

Actividades Formativas			
Código	**Nombre**	**Modalidad**	**Tipo**
AF01	Introductoria	PR	Motivacional / Informativa
AF02	Expositiva y Participativa	PR	Teórica
AF03	Guiada	PR	Teórica / Práctica
AF04	Personalizada (Individual / Grupal)	PR	Teórica / Práctica
AF05	Autónoma	NP	Teórica / Práctica
AF06	Aprendizaje Servicio	PR	Aprendizaje Servicio
AF07	Autoevaluación continua	NP	Evaluación de la Calidad
PR: Presencial **NP**: No presencial			

En todas las asignaturas son obligatorias las modalidades AF01 Introductoria y AF07 Autoevaluación continua.

METODOLOGÍAS DOCENTES

Tabla 17 - Actividades de enseñanza-aprendizaje de la UIE

Código	Actividad	Tipo	Modalidad E-A	Modo
MD01	Primer Contacto y Motivación	**I**	Introductoria	PR
MD02	Presentación, Plan de Trabajo y Compromiso	**I**		
MD03	Clase Magistral	**T**	Expositiva y Participativa	PR
MD04	Charlas Invitadas de Expertos	**T**		
MD05	Metodología UIE	**T/P**	Guiada / Autónoma	PR / NP
MD06	Resolución de Problemas y Ejercicios	**P**		
MD07	Aula Virtual UIE	**T/P**		
MD08	Estudio de Contenidos	**T**	Autónoma	NP
MD09	Elaboración de Proyectos y Trabajos	**T/P**		
MD10	Estudio de Casos	**P**	Guiada	PR
MD11	Seminarios	**T/P**		
MD12	Debates y Discusiones	**P**		
MD13	Exposiciones	**T/P**		
MD14	Juegos, Concursos y Competencias	**P**		
MD15	Recreación de un Entorno Laboral	**T/P**		

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

MD16	Uso de Herramientas de Software	**P**		
MD17	Prácticas de Laboratorio	**P**		
MD18	Prácticas Externas	**P**		
MD19	Aprendizaje Servicio (ApS)	**T/P**	Aprendizaje Servicio	PR
MD20	Tutorías	**T/P**	Personalizada (Individual / Grupal)	PR
MD21	Contrato de Enseñanza-Aprendizaje	**I/T/P**		
MD22	Portafolio (Porfolio Assessment)	**T/P**	Autónoma	NP
MD23	Foros de Discusión	**T/P**		
MD24	Análisis y Síntesis de Material Documental	**T**		
MD25	Seguimiento y Finalización	**C**	Autoevaluación continua	NP
I: Informativa **T**: Teórica **P**: Práctica **C**: Complementaria				
PR: Presencial **NP**: No presencial				

Las actividades de enseñanza-aprendizaje MD05 Metodología UIE, MD19 ApS y MD25 Seguimiento y Finalización, son propias del modelo académico de la UIE.

El Máster Universitario en Ciberseguridad incorpora un conjunto de metodologías docentes activas orientadas al desarrollo de las competencias técnicas y profesionales en entornos realistas. Estas metodologías se articulan en torno a los siguientes ejes:

1. Laboratorios técnicos especializados

Se desarrollarán actividades prácticas en entornos controlados que permitan al estudiante:

- Configurar y securizar sistemas operativos, redes y aplicaciones.
- Analizar vulnerabilidades utilizando herramientas profesionales (escáneres de vulnerabilidades, herramientas de pentesting).
- Implementar mecanismos de protección (cortafuegos, sistemas de detección de intrusiones, cifrado, control de accesos).

Los laboratorios se ejecutarán en infraestructuras virtualizadas (fundamentalmente herramientas disponibles en el sistema operativo Linux Kali instalado en máquinas virtuales) y en entornos securizados.

2. Simulaciones de incidentes de ciberseguridad

Se plantean escenarios realistas de ataque que requieren:

- La detección de incidentes mediante sistemas de monitorización.
- El análisis técnico de evidencias (logs, tráfico de red, artefactos digitales).
- La toma de decisiones en tiempo limitado.
- La aplicación de procedimientos de respuesta y recuperación.

Estas simulaciones reproducen dinámicas organizativas reales, incluyendo la coordinación entre distintos roles (equipo técnico, dirección, comunicación).

3. Entornos controlados de ciberseguridad

Los estudiantes trabajarán en plataformas específicas que replicarán infraestructuras empresariales completas, donde podrá:

- Ejecutar ataques controlados para comprender su funcionamiento.
- Evaluar el impacto de diferentes vulnerabilidades.
- Implementar y validar contramedidas en tiempo real.

Estos entornos facilitarán el aprendizaje basado en la experimentación sin riesgos para sistemas reales.

4. Desarrollo de ejercicios tipo #Capture The Flag# (CTF)

Se desarrollarán competiciones prácticas en las que los estudiantes debe resolver retos de ciberseguridad relacionados con:

- Explotación de vulnerabilidades.
- Análisis forense.
- Seguridad en aplicaciones web.

5. Proyecto práctico integrado

A lo largo del programa los estudiantes podrán desarrollar un proyecto práctico integrado en los que debe:

- Diseñar e implementar soluciones completas de ciberseguridad.
- Analizar riesgos y proponer medidas de mitigación.
- Integrar aspectos técnicos, organizativos y legales.

Este proyecto podrá simular un encargo profesional real y podrá estar vinculado a casos de empresas o instituciones.

6. Uso de herramientas profesionales

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Las actividades prácticas incorporarán el uso de herramientas y tecnologías ampliamente utilizadas en el ámbito profesional, tales como:

- Plataformas de análisis de seguridad.
- Sistemas SIEM.
- Herramientas de análisis forense.
- Entornos de desarrollo seguro.

Para asegurar la realización de todas estas actividades formativas, se cuenta con los mecanismos de coordinación docente que están descritos en el Manual de la Calidad del Sistema de Garantía Interno de Calidad (SGIC). Es decir, en coherencia con la política de calidad, con los principios de su aseguramiento y con el propio SGIC, en la estructura organizativa de la UIE se contemplan las funciones y responsabilidades relacionadas de manera específica con la calidad garantizando los principios de transparencia, coordinación y cooperación.

En la UIE existen órganos cuyas funciones permiten garantizar la planificación, implantación, seguimiento, análisis y mejora de los procesos relacionados con la docencia y con la gestión académica entre Campus; estos procesos permiten a la institución estar en disposición de garantizar el cumplimiento de los compromisos adquiridos con los diferentes grupos de interés. Entre ellos, cabe destacar tanto al Comité de Coordinación Académica como a la Coordinación General Académica, la Coordinación de Desarrollo Académico, los Decanos y Coordinación de Titulación.

En consecuencia, la coordinación horizontal y vertical de la titulación queda garantizada por la labor específica de la Coordinación de la Titulación, bajo la supervisión directa del Decanato y el resto de los órganos que velan por el desarrollo académico de la UIE. En cuanto a tareas específicas desagregadas de las responsabilidades anteriormente señaladas:

Coordinación horizontal

- Analizar las fichas docentes para la elaboración de los Contratos de Enseñanza-Aprendizaje para las asignaturas de cada semestre de cada curso.
- Analizar los Contratos de Enseñanza-Aprendizaje para las asignaturas de cada semestre de cada curso y su actualización.
- Analizar las Guías Docentes y su interrelación con los distintos Contratos de Enseñanza-Aprendizaje para las asignaturas de cada semestre de cada curso y su actualización.
- Revisar la programación temporal de actividades formativas realizadas para cada semestre de cada curso.
- Tratar de adecuar la carga de trabajo real del estudiante a lo previsto en el plan de estudios.
- Contrastar que el sistema de evaluación continua se desarrolle adecuadamente en cada asignatura de acuerdo a los resultados de aprendizaje que se persiguen en cada una de ellas.
- Atender a los resultados de las encuestas de calidad de los estudiantes (cuatro tomas por cada asignatura).

Coordinación vertical

- Optimizar la actividad de los profesores encargados de la docencia de las diferentes asignaturas.
- Contrastar que la secuenciación de la interrelación entre módulo-materia-asignatura del plan de estudios.
- Analizar los resultados de aprendizaje de las asignaturas del plan de estudios para evitar solapamientos y/o ausencias en cuanto a conocimientos, habilidades y competencias.
- Supervisar el Campus Virtual como medio de comunicación directa entre estudiantes y profesores.
- Promover la consulta y la participación de los docentes en el área del Campus Virtual #Sala de Profesores# que incluye materiales formativos, foros y grabaciones de reuniones generales y específicas realizadas con el equipo docente.
- Intercambiar experiencias metodológicas y de innovación docente.

4.3 SISTEMAS DE EVALUACIÓN

4.3 Sistemas de evaluación.

El sistema de evaluación de la UIE es de carácter continuo, compartido y progresivo, permitiendo un seguimiento del aprendizaje a lo largo de cada semestre, haciendo de ello un proceso natural.

En el sistema de evaluación continua se realiza la calificación en escala numérica de 0 a 10, según lo establece el Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en todo el territorio nacional. El sistema dispone de una variedad de alternativas de evaluación como se muestra en la Tabla 17. Todas las actividades de evaluación están habilitadas en las asignaturas y dependiendo del resultado de aprendizaje se les otorga un rango de ponderación.

Tabla 18 - Sistema de Evaluación Continua

Sistema de Evaluación Continua				
Código	**Metodología**	**Ponderación Mínima**	**Ponderación Máxima**	**Modo**
AE01	Pruebas Parciales	15	60	O/E
AE02	Prueba Parcial Final	0	20	O/E
AE03	Proyectos	10	30	O/E
AE04	Exposición	0	20	O
AE05	Actividad en el Campus Virtual	5	15	O/E

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

AE06	Participación, Actividades Diarias y Voluntariado	5	20	O/E
AE07	Memoria y Defensa (TFG/TFM/PE)	70	90	O/E
AE08	Aprendizaje Servicio	0	30	O/E
AE09	Portafolio Digital	0	20	CD
AE10	Recuperar	0	30	O/E
O: Oral **E**: Escrito **CD**: Carpeta Digital				

La actividad AE10 Recuperar forma parte del sistema de evaluación continua y puede ser utilizada en todas sus asignaturas, con la excepción de Prácticas Externas y Trabajo Fin de Máster.

Esta actividad posibilita mejorar la calificación o llegar al nivel mínimo exigido en la misma oportunidad de convocatoria; en todos los casos, dentro de una primera convocatoria de las dos que se garantizan por matrícula. También permite recuperar una cantidad de pruebas sobre las previstas para la totalidad de los parciales de la asignatura, hasta un máximo del 30% de la nota final. El resto de las actividades, al tratarse de evaluación continua, no podrán ser objeto de recuperación.

Las calificaciones obtenidas en AE10 reemplazan las iniciales en las pruebas objeto de recuperación, independientemente de que éstas sean superiores o inferiores.

4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

PERSONAL ACADÉMICO
Ver Apartado 5: Anexo 1.
OTROS RECURSOS HUMANOS
Ver Apartado 5: Anexo 2.

6. RECURSOS MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver Apartado 6: Anexo 1.

7. CALENDARIO DE IMPLANTACIÓN

7.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2026
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	
No procede.	
7.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	**ESTUDIO - CENTRO**

8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD Y ANEXOS

8.1 SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD	
ENLACE	https://uie.edu/calidad/
8.2 INFORMACIÓN PÚBLICA	

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

8. Sistema Interno de Garantía de la Calidad.

El compromiso de la UIE con el aseguramiento de la calidad afecta a todos sus procesos y con ello se garantiza:

- La definición de una política de aseguramiento de la calidad que forme parte de su gestión estratégica.
- La existencia de procesos para el diseño y aprobación de los programas de estudio.
- La enseñanza, aprendizaje y evaluación centrados en el estudiante.
- El establecimiento de procedimientos de admisión, reconocimiento y certificación de los estudiantes.
- El aseguramiento de la competencia y actualización continua del profesorado.
- La disponibilidad de recursos para el aprendizaje y apoyo a los estudiantes.
- La gestión de la información pertinente para la coordinación eficaz de programas y actividades.
- La publicidad de la información garantizando la claridad, precisión, objetividad y fácil accesibilidad.
- El seguimiento continuo y la evaluación periódica de sus programas con el fin de garantizar el logro de los objetivos y la respuesta a las necesidades de los estudiantes y de la sociedad, así como su orientación a la mejora.

El soporte documental del Sistema de Garantía Interno de Calidad (SGIC) incluye el manual de la calidad, la política y objetivos de calidad, el mapa de procesos, los resultados e indicadores y los planes de mejora, entre otros. Todo ello, acompañado de la correspondiente definición de funciones y de asignación de responsabilidades con el fin de asegurar la adecuada planificación, operación, verificación y actuación de los procesos de acuerdo con el ciclo de mejora continua.

La UIE cuenta con el Dictamen Favorable de la Axencia para a Calidade do Sistema Universitario de Galicia -ACSUG- a su SGIC con fecha 23 de abril de 2025.

8.3 ANEXOS

Ver Apartado 8: Anexo 1.

PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Coordinadora General Académica	BEATRIZ	CHECCHIA	COTTI
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Rúa Nova 33	15705	A Coruña	Santiago de Compostela
EMAIL	**FAX**		
bettina.checchia@uie.edu			

REPRESENTANTE LEGAL			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Rector	MIGUEL ÁNGEL	ESCOTET	ÁLVAREZ
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Rúa Nova 33	15705	A Coruña	Santiago de Compostela
EMAIL	**FAX**		
notificaciones@uie.edu			

SOLICITANTE			
El responsable del título no es el solicitante			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Rector	MIGUEL ÁNGEL	ESCOTET	ÁLVAREZ
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Rúa Nova 33	15705	A Coruña	Santiago de Compostela
EMAIL	**FAX**		
notificaciones@uie.edu			

INFORME PREVIO DE LA COMUNIDAD AUTÓNOMA

Informe previo de la Comunidad Autónoma: Ver Apartado Informe previo de la Comunidad Autónoma: Anexo 1.

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 1: Anexo 6

Nombre : Apartado 1 Descripción, objetivos formativos y justificación.pdf

HASH SHA1 :8147878FFC5FB86320CB38C3A2867FC3C4D9F302

Código CSV :99799511771066383793627 5

Ver Fichero: Apartado 1 Descripción, objetivos formativos y justificación.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 4: Anexo 1

Nombre :APARTADO 4 Y FICHAS DE ASIGNATURAS.pdf

HASH SHA1 :8D6A193F07A0BD11B30C4B31CD7A9CDDB760B07C

Código CSV :99799539145246275351966 6

Ver Fichero: APARTADO 4 Y FICHAS DE ASIGNATURAS.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 1

Nombre :APARTADO 5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA_17.4.2026.pdf

HASH SHA1 :23E18706B8B52973E8580448FC72B2DB08638E49

Código CSV :981004343438566999794472

Ver Fichero: APARTADO 5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA_17.4.2026.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 2

Nombre :APARTADO 5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA.OTROS RECURSOS HUMANOS.pdf

HASH SHA1 :F24927F8009AE82BC084B8555F54320C8B31579C

Código CSV :91892844746545038698157

Ver Fichero: APARTADO 5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA.OTROS RECURSOS HUMANOS.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 6: Anexo 1

Nombre :APARTADO 6. APARTADO 6. RECURSOS PARA EL APRENDIZAJE_17.4.2026.pdf

HASH SHA1 :BBEDF48A096EE18A7EF57E9D077B461F186C6F1E

Código CSV :981005523001585204743035

Ver Fichero: APARTADO 6. APARTADO 6. RECURSOS PARA EL APRENDIZAJE_17.4.2026.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 7: Anexo 1

Nombre :APARTADO 7. CALENDARIO DE IMPLANTACIÓN.pdf

HASH SHA1 :BA5FFED27DC2278EF559AFF2ECCCBF54402F4252

Código CSV :918936543504127843721866

Ver Fichero: APARTADO 7. CALENDARIO DE IMPLANTACIÓN.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 8: Anexo 1

Nombre :APARTADO 8.3. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD-ANEXOS.pdf

HASH SHA1 :175B9DE62D8E3A3C635834E29047687EB27648C4

Código CSV :918938529819199574169913

Ver Fichero: APARTADO 8.3. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD-ANEXOS.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado Informe previo de la Comunidad Autónoma: Anexo 1

Nombre :APARTADO 10. INFORME PREVIO COMUNIDAD AUTÓNOMA_MÁSTER CIBERSEGURIDAD.pdf

HASH SHA1 :E6D561CDB3F5DFEFB25C6806C647990C1192F7A0

Código CSV :920347534621747689040944

Ver Fichero: APARTADO 10. INFORME PREVIO COMUNIDAD AUTÓNOMA_MÁSTER CIBERSEGURIDAD.pdf

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CSV: 103518648995405070614863 3 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es