21-22

TITULACION

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

CÓDIGO 310901

UNED

21-22

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

CÓDIGO 310901

ÍNDICE

PRESENTACIÓN

Uno de los objetivos estratégicos de la UNED es abrirse a todos los sectores de la sociedad con propuestas plurales e interdisciplinares. También lo es captar estudiantes que tienen interés en profundizar en materias específicas, como puede ser la Ciberseguridad, y que ya tengan una base científica y cultural importante en otras áreas del conocimiento.
El objetivo principal del Máster es llevar a cabo la formación de estudiantes en el ámbito de la Ciberseguridad. El programa propuesto intentará cubrir los principales aspectos de la Ciberseguridad, haciendo hincapié en aspectos técnicos y de legislación, y desde diferentes puntos de vista dentro del área. Para lograr este fin, los estudiantes aprenderán sobre mecanismos de defensa y prevención mediante la auditoría, la monitorización, el hacking ético y la criptografía, así como de reacción ante un incidente mediante la gestión de incidentes informáticos y su análisis forense, teniendo en cuenta en todo momento el marco legal vigente.

OBJETIVOS Y COMPETENCIAS

OBJETIVOS

El objetivo principal del Máster es llevar a cabo la formación de estudiantes en el ámbito de la Ciberseguridad, tanto para fines de investigación como fines profesionalizantes. El programa propuesto intentará cubrir los principales aspectos de la Ciberseguridad, haciendo hincapié en aspectos técnicos y de legislación, y desde diferentes puntos de vista dentro del área.
El objetivo principal del plan de estudios puede desglosarse en diferentes objetivos específicos:

- Utilizar mecanismos criptográficos avanzados para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.
- Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.
- Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.
- Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.
- Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.
- Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.
- Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.
- Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.

•Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.
•Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

COMPETENCIAS

Según el Real Decreto 1027/2011, de 15 de julio, por el que se establece el Marco Español de Cualificaciones para la Educación Superior (MECES):

"Artículo 7. Nivel de Máster.

1. El nivel de Máster se constituye en el nivel 3 del MECES, en el que se incluyen aquellas cualificaciones que tienen como finalidad la adquisición por el estudiante de una formación avanzada, de carácter especializado o multidisciplinar, orientada a la especialización académica o profesional, o bien a promover la iniciación en tareas investigadoras.

2. Las características de las cualificaciones ubicadas en este nivel vienen definidas por los siguientes descriptores presentados en términos de resultados del aprendizaje:

a) haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altamente especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en uno o más campos de estudio;

b) saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigadores como profesionales altamente especializados;

c) saber evaluar y seleccionar la teoría científica adecuada y la metodología precisa de sus campos de estudio para formular juicios a partir de información incompleta o limitada incluyendo, cuando sea preciso y pertinente, una reflexión sobre la responsabilidad social o ética ligada a la solución que se proponga en cada caso;

d) ser capaces de predecir y controlar la evolución de situaciones complejas mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional concreto, en general multidisciplinar, en el que se desarrolle su actividad;

e) saber transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan;

f) haber desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia del conocimiento;

g) ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio.

3. Las cualificaciones incluidas en este nivel se indican en el apartado correspondiente del cuadro que figura en el anexo a esta norma.
4. Los títulos de Grado que por exigencias de normativa de la Unión Europea sean de al menos 300 créditos ECTS, siempre que comprendan un mínimo de 60 créditos ECTS que participen de las características propias de los descriptores del apartado 2 de este precepto, podrán obtener la adscripción al Nivel 3 (Máster) regulado en este real decreto. La normativa sobre ordenación de las enseñanzas universitarias oficiales establecerá el procedimiento a seguir para obtener esa adscripción."

Con el fin de cumplir con las normativas mencionadas anteriormente se establecen las siguientes competencias del Master Universitario en Ciberseguridad:

Competencias Básicas (CB)

- CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
- CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
- CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
- CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades
- CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias Generales (CG)

- CG1 - Analizar métodos y técnicas de ciberataques.
- CG2 - Diseñar, poner en marcha y mantener un sistema de ciberseguridad.
- CG3 - Conocer la normativa y la legislación en materia de ciberseguridad, sus implicaciones en el diseño y puesta en marcha de sistemas informáticos.
- CG4 - Identificar, gestionar y desarrollar medidas y protocolos de seguridad en la operación y gestión de sistemas informáticos.

Competencias Transversales (CT)

- CT1 - Ser capaz de abordar y desarrollar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

•CT2 - Ser capar de tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

Competencias Específicas (CE)

•CE1 - Utilizar mecanismos criptográficos avanzados de para garantizar los requisitos de seguridad en un sistema, así como el acceso y seguridad en las comunicaciones.

•CE2 - Diseñar mecanismos de prevención de amenazas a la seguridad, así como de reconocer y resolver incidentes de seguridad en los sistemas críticos.

•CE3 - Utilizar herramientas para monitorizar el tráfico de red y generar, explorar y manipular el tráfico en los sistemas de comunicación.

•CE4 - Analizar e identificar vulnerabilidades ante posibles ataques en los sistemas de comunicaciones y los servicios asociados.

•CE5 - Analizar e identificar técnicas de ocultación de ataques a sistemas de comunicaciones y aplicaciones.

•CE6 - Conocer las tendencias actuales en técnicas de ciberataque, los mecanismos de defensa mediante aprendizaje automático y especialmente dirigido a casos reales.

•CE7 - Analizar sistemas para encontrar evidencias de ataques en los mismos y adoptar las medidas precisas para mantener la cadena de custodia de dichas evidencias.

•CE8 - Conocer las técnicas y herramientas para la realización de un análisis forense con la preservación de pruebas digitales.

•CE9 - Comprender la importancia del Derecho como sistema regulador de las relaciones sociales.

•CE10 - Conseguir la percepción del carácter unitario del ordenamiento jurídico y de la necesaria visión interdisciplinaria de los problemas jurídicos.

Para asegurar la adquisición de las competencias anteriormente descritas, todas las asignaturas cuentan con actividades prácticas para fomentar dicha orientación profesional. Estas asignaturas tienen una fuerte componente de actividades prácticas que utilizarán tecnologías procedentes o cercanas al mundo de la empresa. Además, el Máster cuenta con profesores con experiencia en el entorno empresarial, que aportan tanto a los estudiantes como a la planificación docente una valiosa experiencia profesional.

La información completa sobre las asignaturas y las competencias que cubren se encuentra en la memoria verificada, aunque se incluye a continuación la tabla representativa de las competencias específicas y las asignaturas que las cubren :

ID	**Materia**	*CG 1*	*CG 2*	*CG 3*	*CG 4*	*CT1*	*CT2*	*CE 1*	*CE 2*	*CE 3*	*CE 4*	*CE 5*	*CE 6*	*CE 7*	*CE 8*	*CE 9*	*CE 10*

311090 10	*Criptografía Aplicada*	X	X		X	X	X	X								
311090 25	*Auditoría y Monitorización de la Seguridad*	X	X		X	X	X		X	X			X			
311090 3-	*Análisis Forense*	X		X		X	X					X		X	X	
311090 44	*Hacking Ético*	X		X		X	X		X		X		X			
311090 59	*Ciberilícitos*			X	X	X	X								X	X

31109115	*Seguridad en Infraestructuras Críticas*	X	X		X	X	X			X	X					
31109078	*Análisis de Malware*	X			X	X	X					X				
31109082	*Gestión de Incidentes de Ciberseguridad*	X		X		X	X		X				X			

31109097	*Introducción al Aprendizaje Automático para Ciberseguridad*	X	X			X	X						X				
3110910-	*Marco jurídico de la Defensa Nacional en el Ciberespacio*			X	X	X	X									X	X

311090 63	*Trabajo Fin de Máster (TFM)*	X	X	X	X	X	X										

SALIDAS PROFESIONALES, ACADÉMICAS Y DE INVESTIGACIÓN

La Ciberseguridad es uno de los campos de investigación más activos, tanto a nivel nacional como internacional, y uno en los que más innovaciones se producen. En el Máster participarán profesores con una amplia experiencia científica, lo que influye positivamente en capacitar al estudiante para el desempeño de actividades de investigación necesarias en las empresas, siempre relacionadas con el campo de la Ciberseguridad. Asimismo, el Máster procura, dentro de sus posibilidades, que el estudiante pueda configurarse un diseño curricular acorde a sus propios intereses formativos o de investigación.

Desde el punto de vista académico, el objetivo principal del Máster es llevar a cabo la formación de estudiantes en el ámbito de la Ciberseguridad. El programa propuesto intentará cubrir los principales aspectos de la Ciberseguridad, haciendo hincapié en aspectos técnicos y de legislación, y desde diferentes puntos de vista dentro del área. Para lograr este fin, se aplicará la metodología de educación a distancia propia de la UNED, con la inclusión de una gran variedad recursos multimedia educativos, tanto para los contenidos como las prácticas de evaluación. Se utilizarán los medios de los que dispone la institución para tal fin.

Desde el punto de vista profesional, los Ingenieros en Informática especializados en la Ciberseguridad juegan un papel fundamental en el desarrollo de la sociedad. Este Máster aporta a los profesionales de la Ingeniería Informática (o titulaciones afines) una formación de 60 créditos ECTS, dotándole con capacidades dentro del campo de la Ciberseguridad. En este sentido, el Trabajo Fin de Máster (TFM) potencia las habilidades personales, en diversos aspectos, que van desde la integración de tecnologías, a la adecuada presentación de resultados y conclusiones.

REQUISITOS ACCESO

El Máster Universitario en Ciberseguridad está dirigido a estudiantes que deseen recibir una formación avanzada en el ámbito de la Ciberseguridad y desarrollar una carrera profesional en este sector. Se dirige especialmente a estudiantes egresados de un título de Grado en Ingeniería Informática o grados con otras denominaciones, vinculados al ejercicio de la profesión de ingeniero en informática.

En base a lo anterior, y teniendo en cuenta lo establecido en el Real Decreto 1393/2007, será requisito mínimo para matricularse en el Máster Universitario en Ciberseguridad por la

Universidad Nacional de Educación a Distancia que el estudiante esté en posesión del **Título de Licenciado, Ingeniero y/o Graduado en Informática.**
La Comisión de Coordinación del Máster (CCM) es el órgano encargado de la admisión de estudiantes. La Comisión de Coordinación del Máster podría considerar también la admisión a titulados universitarios de carreras afines, como Telecomunicaciones, Física, Matemáticas, o Química, y a Ingenieros Técnicos en Informática. Se valorarán también los conocimientos de informática adquiridos fuera de la carrera y en la práctica profesional.
Se recomienda que los estudiantes de nuestro máster tengan el nivel B1 (del Marco Común Europeo de Referencia para las Lenguas). De esa manera, los estudiantes deben ser capaces de leer textos en inglés. No se requiere ningún conocimiento de las otras habilidades lingüísticas (hablar, escribir y escuchar) en los mencionados idiomas.

CRITERIOS DE ADMISIÓN

Los criterios para la selección de estudiantes son:

1. **Titulación de acceso** (*hasta 4 puntos*). Adecuación de la Titulación por la que se accede al máster en el área de Ingeniería.
2. **Expediente académico** (*hasta 4 puntos*).
3. **Currículum Vitae** (*hasta 2 puntos*).

•*Experiencia profesional*. Se valorará positivamente con una puntuación de hasta un punto a aquellos estudiantes que presenten un currículum vitae de experiencias profesionales que avalen su capacidad para poder seguir el programa con aprovechamiento, siempre y cuando dispongan de acceso a la universidad según la normativa vigente *(hasta 1 punto*).

•*Formación complementaria.* Otros títulos de posgrado no universitarios en materia de Informática (*hasta 0,5 puntos)*.

•*Conocimiento de idiomas.* Se valorará preferentemente a aquellas personas que tengan un conocimiento intermedio y/o avanzado del inglés (*hasta 0,5 puntos*). El conocimiento en idiomas podrá ser demostrado a través de la presentación de un título y/o a través de otros procesos de evaluación establecidos por la comisión de Máster.

En cada una de las fases de reparto de las plazas únicamente se considerarán las solicitudes de aquellos estudiantes que cumplan y hayan demostrado documentalmente los requisitos planteados y los méritos aludidos.

NO. DE ESTUDIANTES DE NUEVO INGRESO

Son un máximo de 75 plazas ofertadas.

PLAN DE ESTUDIOS

Para alcanzar estos objetivos del Máster se propone el siguiente plan de estudios distribuido en dos cuatrimestres y con un diseño equilibrado de créditos por semestres. Para alcanzar los objetivos anteriores se propone una estructura de Máster Universitario con 60 créditos impartidos en un solo curso académico. En la Tabla 1 se presenta la distribución de créditos según el carácter de las asignaturas que lo componen.

Tipo de materia/asignatura	Créditos
Obligatorias	36
Optativas	12
Trabajo Fin de Máster	12
TOTAL	60

Tabla 1: Distribución de créditos por tipo de asignatura

En la Tabla 2 se muestra para cada asignatura se indica el número de créditos y si es obligatoria u optativa. Se debe destacar que se pretende con la oferta de optatividad en cada materia (excepto el Trabajo Fin de Máster) que el estudiante pueda focalizar su interés profesional en temas específicos de Ciberseguridad, tales y como aspectos legales, profundización en la automatización de tareas, etc.

Materia/asignatura	Créditos ECTS	Tipo	Semestre
Criptografía Aplicada	6	Obligatoria	1
Auditoría y Monitorización de la Seguridad	6	Obligatoria	1
Análisis Forense	6	Obligatoria	1
Hacking Ético	6	Obligatoria	1
Ciberilícitos	6	Obligatoria	1
Seguridad en Infraestructuras Críticas	6	Obligatoria	2
Análisis de Malware	6	Optativa	2
Gestión de Incidentes de Ciberseguridad	6	Optativa	2

Introducción al Aprendizaje Automático para Ciberseguridad	6	Optativa	2
Marco jurídico de la Defensa Nacional en el Ciberespacio	6	Optativa	2
Trabajo Fin de Máster (TFM)	12	Obligatoria	2

Tabla 2: Asignaturas, créditos, su carácter obligatorio/optativo y semestre de impartición

En esta titulación todas las asignaturas tienen un carácter semestral. El plan de estudios del título está organizado en dos semestres. La planificación intenta garantizar una distribución uniforme de créditos por semestre, de forma que el estudiante deberá cursar 30 créditos en el primer semestre y otros 30 créditos en el segundo. Cada crédito supondrá un volumen total de trabajo del estudiante de 25 horas. La Tabla 3 recoge los semestres en los que se planifican las asignaturas del plan de estudios, de carácter anual.

Primer semestre	**Segundo semestre**
Criptografía Aplicada	Seguridad en Infraestructuras Críticas
Auditoría y Monitorización de la Seguridad	Optativa 1
Análisis Forense	Optativa 2
Hacking Ético	Trabajo Fin de Máster
Ciberilícitos	

Tabla 3: Planificación temporal del curso académico

NORMATIVA

En el siguiente enlace se encuentran disponibles los documentos (formato PDF) con la normativa aplicable a la realización de los estudios de Máster: http://portal.uned.es/portal/page?_pageid=93,36824502&_dad=portal&_schema=PORTAL

Queremos destacar, en cualquier caso, la siguiente normativa:

- RD 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales
- RD 861/2010, de 2 de julio, por el que se modifica el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales

- RD 43/2015, de 2 de febrero, por el que se modifica el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, y el Real Decreto 99/2011, de 28 de enero, por el que se regulan las enseñanzas oficiales de doctorado.
- Actualización de los procedimientos de organización y gestión académica de los Másteres Universitarios oficiales y Doctorado de la UNED, para su adaptación en lo dispuesto en el RD. 1393/2007.
- Normas y criterios generales de reconocimiento y transferencia de créditos para los másteres.
- Normas de permanencia en estudios conducentes a títulos oficiales de la Universidad Nacional de Educación A Distancia.
- Regulación de los trabajos de fin de master en las enseñanzas conducente al título oficial de master de la UNED.

PRÁCTICAS

Dado el carácter práctico del título, en las asignaturas en las que hay un contenido importante de prácticas, se detalla qué laboratorios (presenciales o virtuales) tendrá el estudiante a su disposición, así como las aplicaciones necesarias.
En general, el software necesario para la realización de las prácticas es software libre que se puede ejecutar en diversas plataformas. Algunos ejemplos son máquinas virtuales o contenedores ligeros para simular distintos sistemas operativos, entornos de desarrollo para lenguajes como Python o Java, simuladores, herramientas colaborativas, clasificadores, aplicaciones de análisis de redes, etc. En los casos en que se necesite ordenador, si el estudiante no dispone de él, puede acudir a su Centro Asociado.
En cualquier caso, la Escuela de Ingeniería Informática de la UNED cuenta con diversos servidores que permiten la realización específica de prácticas que requieran un soporte particular. Concretamente, cuenta con una sala fría con 47 servidores físicos, 43 servidores virtuales, 9 racks, 2 cabinas de almacenamiento, 2 máquinas de climatización, 8 SAIS y una librería de copias de seguridad. La Escuela cuenta también con 4 laboratorios, con equipamiento informático y experimental.

DOCUMENTACIÓN OFICIAL DEL TÍTULO

De acuerdo con la legislación vigente, todas las Universidades han de someter sus títulos oficiales a un proceso de verificación, seguimiento y acreditación.
En el caso de la UNED, el Consejo de Universidades recibe la memoria del título y la remite a la ANECA para su evaluación y emisión del Informe de verificación. Si el informe es favorable, el Consejo de Universidades dicta la Resolución de verificación, y el Ministerio de Educación eleva al Gobierno la propuesta de carácter oficial del título, ordena su inclusión en el Registro de Universidades, Centros y Títulos (RUCT) y su posterior publicación en el Boletín Oficial del Estado.

Los títulos oficiales de Máster han de renovar su acreditación antes de los cuatro años desde su verificación o bien desde la fecha de su última acreditación, con el objetivo de comprobar si los resultados obtenidos son adecuados para garantizar la continuidad de su impartición. Si son adecuados, el Consejo de Universidades emite una Resolución de la acreditación del título.
Estas resoluciones e informes quedan recogidos en el Registro de Universidades, Centros y Títulos (RUCT).

VERIFICACIÓN / MODIFICACIÓN

•Memoria del título

•Informe de verificación de la ANECA

•Resolución de verificación del CU

•Inscripción del título en el Registro de Universidades, Centros y Títulos

•Publicación del Plan de Estudios en el BOE.

SEGUIMIENTO

•Informe de Seguimiento del Título.

ACREDITACIÓN

SISTEMA DE GARANTÍA INTERNA DE CALIDAD DEL TÍTULO

La UNED dispone de un Sistema de Garantía Interna de Calidad (SGIC-U) que alcanza a todos sus títulos oficiales de grado, máster y doctorado, así como a los servicios que ofrece, cuyo diseño fue certificado por la ANECA.
El SGIC-U contempla todos los procesos necesarios para asegurar la calidad de su profesorado, de los recursos y de los servicios destinados a los estudiantes: el acceso, la admisión y la acogida, las prácticas externas, los programas de movilidad, la orientación académica e inserción laboral, el seguimiento y evaluación de los resultados de la formación, la atención de las sugerencias y reclamaciones y la adecuación del personal de apoyo, entre otros.
Los responsables del SGIC son:

•La Comisión Coordinadora del Título

•La Comisión de Garantía de Calidad del Centro

•El Equipo Decanal o de Dirección

•La Comisión de Garantía de Calidad de la UNED

A través del Portal estadístico, la UNED aporta información a toda la comunidad universitaria tanto de los resultados de la formación como de los resultados de satisfacción de los distintos colectivos implicados.
Documentos del SGIC del título:

•Principales resultados de rendimiento

•Resultados de satisfacción de los diferentes colectivos

•Objetivos de Calidad del Centro

El Sistema de Garantía Interna de Calidad de la UNED ha sido verificado por la ANECA en la primera convocatoria del Programa AUDIT (2009), recibiendo la certificación total a este Sistema. Esta certificación indica que el SGIC es aplicable a todos los títulos de Máster que se imparten en la UNED. La Comisión de Coordinación del Máster (CCM) es el órgano responsable del SGIC de programa. Asimismo, esta comisión es la responsable de garantizar la existencia de mecanismos para obtener la información relativa al desarrollo del programa.

Los **mecanismos de coordinación docente** con los que cuenta el título están recogidos en el documento: "Actualización de los procedimientos de organización y gestión académica de los Másteres Universitarios oficiales y Doctorado de la UNED, para su adaptación en lo dispuesto en el RD. 1393/2007", aprobado por acuerdo del Consejo de Gobierno de fecha 16 de diciembre de 2008. En dicho documento se dice que para facilitar la coordinación académica interna de cada Título, y con los órganos de decisión académica del Centro, se constituirá una Comisión de Coordinación de Título de Máster de Centro, responsable de la organización y control de resultados.

La Comisión de Coordinación del Título de Máster de Centro está formada por:

•Director de la ETS de Ingeniería Informática: Dr. D. Rafael Martínez Tomás.

•Responsable de calidad del centro: Dra. Dña. Margarita Bachiller Mayoral.

•Coordinador del Máster: Dr. D. Roberto Hernandez Berlinches.

•Secretario del Máster: Dra. Dña. Maria de los Llanos Tobarra Abad.

•Representante del Personal de Administración y Servicios: Dña. Carmen Lidia Segovia Orellana.

•Representante de alumnos: D. Juan Carlos Ruiz González.

•Representantes de los Departamentos/Facultades/Escuela:

•Departamento Inteligencia Artificial (IA): Dr. D. José Ramon Álvarez Sánchez.

•Departamento Lenguajes de Sistemas Informáticos (LSI): Dr. D. Miguel Rodriguez Artacho.

•Departamento de Sistemas de Comunicación y Control (SCC): Dr. D. Rafael Pastor Vargas.

•ETSI Industriales: Dr. D. Gabriel Díaz Orueta.

•Facultad de Derecho: Dra. Dña. Alicia Gil Gil.

ATRIBUCIONES PROFESIONALES

La Ingeniería Informática, y por ende este Máster, no tiene aún atribuciones profesionales oficialmente reconocidas.

ESTUDIANTES CON DISCAPACIDAD

UNIDIS (Centro de Atención a Universitarios con Discapacidad) es un servicio dependiente del Vicerrectorado de Estudiantes y Emprendimiento de la UNED, cuyo objetivo principal es

que los estudiantes con discapacidad que deseen cursar estudios en esta Universidad, puedan gozar de las mismas oportunidades que el resto de estudiantes de la UNED. Puedes obtener más información en el siguiente enlace.

BUZÓN DE SUGERENCIAS, RECLAMACIONES Y FELICITACIONES

La UNED pone a disposición de toda la comunidad universitaria a través del Centro de Atención al Estudiante (CAE), un del Buzón de Quejas, Sugerencias y Felicitaciones. Para más información visita este enlace.

CONTACTAR PARA MÁS INFORMACIÓN

¡Preinscríbete o/y pregúntanos tu caso concreto!!

INFORMACIÓN EN: http://www.ii.uned.es/

Si tienes alguna duda de naturaleza administrativa escribe un correo a: informatica.posgradosoficiales@adm.uned.es

---

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.