Este anexo describe de forma detallada los resultados de aprendizaje de cada una de las materias del título

Materia 1.1 Matemática	
Número de créditos ECTS	24
Tipología	*Básico*
Organización temporal	*Semestres nº 1, 2 y 3*
Modalidad	*Presencial*
Resultados del proceso de formación y aprendizaje	Conocer el concepto de convergencia de una serie numérica y saber sumar algunos tipos básicos de series numéricas. Saber utilizar las propiedades de las funciones elementales y el vector gradiente para resolver problemas relacionados con las ingenierías y en particular problemas de optimización. Saber utilizar las técnicas básicas del cálculo de primitivas y sus propiedades para calcular integrales en una y varias variables usando el teorema de Fubini y cambios de variable. Conocer y aplicar técnicas básicas de teoría de números y aritmética modular a problemas relacionados con las ciencias de la computación y la criptografía. Conocer los fundamentos de la teoría de grafos y saber aplicar sus técnicas y algoritmos básicos. Saber trabajar con matrices para resolver problemas del álgebra lineal y sus aplicaciones a las ciencias de la computación. Conocer los fundamentos de la teoría intuitiva de conjuntos, funciones y relaciones. Saber utilizar la lógica clásica como sistema de representación de conocimiento y usar algoritmos de demostración automática. Conocer las posibilidades y limitaciones de la lógica clásica y trabajar con algunas extensiones que salven estas limitaciones. Saber utilizar las herramientas de estadística descriptiva uni- y bi-dimensional y saber modelar estadísticamente conjuntos de datos usando técnicas de regresión lineal simple y múltiple. Saber utilizar las técnicas y modelos básicos de series temporales para resolver problemas de predicción, usando las herramientas de descomposición de series, de suavizado exponencial y los modelos ARIMA. Saber emplear los resultados principales de probabilidad y regla de Bayes, conocer las principales distribuciones de probabilidad y saber utilizarlas para realizar inferencia estadística.
Asignaturas	*- Matemáticas I (Mathematics I), (1º semestre, 6 créditos, español/ inglés)* *- Matemáticas II (Mathematics II), (2º semestre,6 créditos, español)* *- Probabilidad y Estadística (Probability and Statistics) , (3º semestre, 6 créditos, español)* *- Representación del Conocimiento y Razonamiento Knowledge Representation and Reasoning) ,(1º semestre, 6 créditos, español)*

Materia 1.2 Fundamentos de Informática	
Número de créditos ECTS	36
Tipología	*Básico*
Organización temporal	*Semestres nº 1 y 2*
Modalidad	*Presencial*
Resultados del proceso de formación y aprendizaje	Conocer y entender la organización, los elementos y el funcionamiento de Internet y otras redes telemáticas para la comunicación entre ordenadores. Conocer y entender las aplicaciones y servicios en Internet y otras redes telemáticas. Diseñar soluciones algorítmicas, con rigurosidad y teniendo muy en cuenta la calidad de las mismas, a problemas concretos mediante el uso del paradigma de la programación imperativa, de la programación estructurada y la abstracción procedimental, usando tipos de datos simples y estructurados, punteros, buffers de memoria, gestión dinámica de memoria, ficheros y estructuras de selección e iteración. Utilizar entornos y herramientas de desarrollo con los que implementar los algoritmos diseñados en un determinado lenguaje de programación, que puedan ayudar a medir la calidad de las soluciones planteadas.

	Diseñar soluciones algorítmicas, con rigurosidad y teniendo muy en cuenta la calidad de las mismas, a problemas concretos mediante el uso del paradigma de la programación orientada a objetos. Identificar, localizar y corregir los errores que puedan aparecer en las soluciones obtenidas para los problemas planteados, haciendo hincapié en el uso de pruebas unitarias adecuadas. Evaluar las principales amenazas de seguridad y su impacto en redes y sistemas de información. Distinguir los diferentes protocolos y servicios de seguridad aplicables a la protección frente a las amenazas más comunes. Distinguir los diferentes mecanismos para autenticación y control de acceso usados en los sistemas modernos, y en particular los de aplicación a la web. Poner en práctica diferentes protocolos y mecanismos de privacidad y anonimato. Entender la virtualización de un sistema completo y basado en contenedores, Explicar las tecnologías de una infraestructura como servicio. Discutir mecanismos de automatización, control, gestión y monitorización de infraestructuras virtualizadas.
Asignaturas	*- Programación I (Programming I) , (1º semestre,6 créditos, español)* *- Programación II (Programming II) , (2º semestre, 6 créditos, español)* *- Fundamentos de Redes Telemáticas (Foundations of Telematic Services) , (1º semestre. 6 créditos, español)* *- Arquitectura de Computadores (Computer Architecture) (2º semestre,6 créditos,español)* *- Identidad Digital y Privacidad (Digital Identity and Privacy) (2º semestre,6 créditos,español)* *- Fundamentos de Ciberseguridad (Foundations of Cybersecurity) (1º semestre,6 créditos,español)*

Materia 2. 1 Ingeniería del Software y Procesamiento de la Información	
Número ECTS	30
Tipología	Obligatoria
Organización temporal	semestres nº 3, 4 y 6
Modalidad	Presencial
Resultados del proceso de formación y aprendizaje	Crear y consultar un esquema de base de datos relacional usando el lenguaje SQL, Identificar las diferencias entre modelos de Bases de Datos, Gestionar la Seguridad en bases de datos, creando usuarios, privilegios y configurando la auditoría Evaluar la calidad de los datos para realizar las acciones necesarias en las fases previas al procesamiento de los datos, Determinar la idoneidad de las diferentes técnicas disponibles para el procesamiento de los datos (estadísticas y de aprendizaje automático) atendiendo al problema y objetivos establecidos, Evaluar los resultados alcanzados e integrar los modelos generados para usarlos en sistemas que puedan ayudar a la toma de decisiones Conocer los distintos tipos de vulnerabilidades y excepciones que pueden ocurrir fruto de la programación. Aplicar prácticas y herramientas de validación automática de las propiedades de seguridad. Aplicar prácticas seguras de programación. Conocer los conceptos, el papel en el proceso de desarrollo, y las herramientas de la Ingeniería del Software Seguro, Entender la seguridad de un sistema desde una perspectiva holística y ser capaz de desarrollar un análisis de seguridad basado en riesgos, amenazas y propiedades de seguridad. Ser capaz de seleccionar y aplicar las técnicas y herramientas adecuadas para el desarrollo de sistemas seguros, desde los requisitos a la implementación y evolución. Explicar los estándares utilizados para el desarrollo Web tanto en el cliente como el servidor . Enumerar las distintas amenazas de seguridad a la que son susceptibles las aplicaciones Web. Saber utilizar técnicas para el desarrollo seguro de aplicaciones y la protección de infraestructura de ejecución.

Asignaturas	- Bases de Datos (Databases), (4º semestre, 6 créditos, español) - Minería de Datos (*Data Mining*), (6º semestre, 6 créditos, español) - Programación Segura (*Secure Programming*), (3º semestre, 6 créditos, español) - Ingeniería de Software Seguro (Secure Software Engineering),(4º semestre, 6 créditos, español) - Seguridad de Aplicaciones Web (Security in Web Applications),(4º semestre, 6 créditos, español)

Materia 2. 2 Inteligencia Computacional	
Número ECTS	12
Tipología	Obligatoria
Organización temporal	semestres nº 2 y 4
Modalidad	Presencial
Resultados del proceso de formación y aprendizaje	Describir los principales paradigmas de la IA (simbólico y conexionista) y sus aplicaciones, métodos y algoritmos básicos. Formular y resolver problemas básicos de satisfacción de restricciones, planificación, búsqueda y juegos. Calcular la complejidad de algoritmos sencillos y demostrar la calculabilidad de problemas. Describir los principales métodos de búsqueda y optimización computacional empleados en Inteligencia Artificial. Formular y resolver problemas de búsqueda y optimización. Programar soluciones e integrar soluciones ya existentes para la resolución de problemas de búsqueda y optimización
Asignaturas	- Fundamentos de Inteligencia Artificial (Foundations of Artificial Intelligence), (2º semestre, 6 créditos, español) - Algoritmos de Búsqueda y Optimización Computacional (Computacional Search Algorithms and Computational Optimization), (4º semestre, 6 créditos, español)

Materia 2. 3 Tecnologías Informáticas y de Sistemas	
Número ECTS	12
Tipología	Obligatoria
Organización temporal	semestres nº 3 y 5
Modalidad	Presencial
Resultados del proceso de formación y aprendizaje	Enunciar los subsistemas que forman un sistema operativo y sus funciones, Explicar los mecanismos de planificación y comunicación entre procesos, de gestión de la memoria y de organización del sistema de ficheros, Identificar las técnicas básicas para la administración de un sistema operativo Entender la virtualización de un sistema completo y basado en contenedores, Explicar las tecnologías de una infraestructura como servicio, Discutir mecanismos de automatización, control, gestión y monitorización de infraestructuras virtualizadas
Asignaturas	-Arquitectura de Sistemas Virtualizados (Virtualized Systems Architecture),(5º semestre, 6 créditos, español) - Sistemas Operativos (Operating Systems), (3º semestre, 6 créditos, español)

Materia 3.1 Ciberseguridad	
Número ECTS	24
Tipología	Obligatoria
Organización temporal	semestres nº 3,5, 6 y 7
Modalidad	Presencial
Resultados del proceso de formación y aprendizaje	Identificar las diferencias y características entre las diferentes generaciones de redes móviles. Desarrollar aplicaciones seguras para plataformas móviles y evaluar su seguridad.

	Aplicar mecanismos y herramientas de seguridad básicos, fundamentales para configurar de manera segura dispositivos en red., Evaluar la efectividad de los mecanismos y las herramientas de seguridad establecidos a nivel de red y host. Descubrir las vulnerabilidades de sistemas interconectados a través de técnicas de pentesting, Aplicar técnicas de hacking para la explotación de sistemas interconectados, Describir los principios básicos relacionados con la ciberdelincuencia, la cibervictimización y la persecución y prevención de este tipo de delitos, Identificar los conceptos fundamentales dentro de las diferentes disciplinas y escenarios de la informática forense, Aplicar los principios de la informática forense para la extracción y análisis de evidencias digitales
Asignaturas	- Seguridad en Servicios y Protocolos de Internet (Security in Services and Internet Protocols), (3º semestre, 6 créditos, español) - Pentesting y Hacking Ético (Pentesting and Ethical Hacking) NOTA: Penetration Testing parece más formal. , (5º semestre, 6 créditos, español) - Informática Forense y Ciberdelincuencia (Computer Science Forensics and Cybercrime) , (6º semestre, 6 créditos, español) - Seguridad en entornos Móviles (Security in Mobile Environments),(7º semestre, 6 créditos, español)

Materia 4. 1 Inteligencia Artificial	
Número ECTS	24
Tipología	Obligatoria
Organización temporal	semestres nº 3, 4,5, y 6
Modalidad	Presencial
Resultados del proceso de formación y aprendizaje	Describir los principales métodos del aprendizaje no supervisado y por refuerzo. Formular y resolver problemas de agrupamiento y aprendizaje por refuerzo. Programar soluciones e integrar soluciones ya existentes para la resolución de problemas de aprendizaje no supervisado y por refuerzo. Describir métodos avanzados del aprendizaje profundo. Formular y resolver problemas de visión y procesamiento del lenguaje. Programar soluciones e integrar soluciones ya existentes para la resolución de problemas de aprendizaje profundo. Describir los principales métodos del aprendizaje supervisado. Formular y resolver problemas de clasificación y regresión. Programar soluciones e integrar soluciones ya existentes para la resolución de problemas de aprendizaje supervisado. Identificar el estado del arte de la Robótica Inteligente. Identificar las herramientas de IA más importantes involucradas en la Robótica Móvil Inteligente. Programar métodos de IA para Robótica Móvil Inteligente.
Asignaturas	- Aprendizaje Computacional I (Computational Learning I) , (3º semestre, 6 créditos, español) - Aprendizaje Computacional II (Computational Learning II) , (4º semestre, 6 créditos, español) - Aprendizaje Profundo (Deep Learning) , (5º semestre, 6 créditos, español) - Robótica Inteligente (Intelligent Robotics) , (6º semestre, 6 créditos, español)

Materia 5.1 Integración de Ciberseguridad e Inteligencia Artificial	
Número ECTS	30
Tipología	Obligatoria
Organización temporal	semestres nº 5, 6 y 7
Modalidad	Presencial
Resultados del proceso de formación y aprendizaje	Identificar las distintas propiedades básicas de una muestra malware a nivel estático y dinámico que le permita reconocer técnicas empleadas en los ciberataques.

	Analizar estática y dinámicamente la funcionalidad básica de una muestra malware para concluir su riesgo potencial. Aplicar técnicas básicas de machine learning sobre las propiedades y comportamiento del malware para su identificación y clasificación. Interpretar las amenazas que afectan a los sistemas de Inteligencia Artificial. Identificar las amenazas más relevantes para un sistema de Inteligencia Artificial concreto. Describir mecanismos de prevención ante amenazas en IA Seleccionar técnicas para mejorar la seguridad de sistemas de Inteligencia Artificial. Aplicar mecanismos de privacidad de los datos en sistemas IA Validar la robustez del sistema IA ante posibles amenazas Aplicar tecnologías para la detección, respuesta y recuperación frente a ciberincidentes y anomalías. Valorar la relevancia de la compartición de los datos de acuerdo a formatos y estándares existentes para la consciencia situacional. Explicar e interpretar los procesos de autenticación biométrica Elegir y configurar las técnicas de autenticación biométrica más relevantes para una situación concreta. Aplicar software de autenticación biométrica
Asignaturas	- Inteligencia Malware (Malware Intelligence) , (5º semestre, 6 créditos, español) - Ciberseguridad en Sistemas de Inteligencia Artificial (Cyber Threats in Artificial Intelligence Systems) , (6º semestre, 6 créditos, español) - Gestión Inteligente de Anomalías y Ciberincidentes (Intelligent Management of Anomalies and Cyber Incidents) , (7º semestre, 6 créditos, español) - Sistemas de Inteligencia Artificial Ciberseguros (Cyber secure AI Systems) ,(7º semestre, 6 créditos, español) - Sistemas Biométricos (Biometric Systems) ,(7º semestre, 6 créditos, español)