CIBERSEGURIDAD (2019-20)

Código:	Fecha de aprobación:	Precio:
D104	16/02/2019	39,27 Créditos en 1ª matrícula
Créditos:	**Título:**	
60	Máster Universitario Oficial	

RAMA
Ingeniería y Arquitectura

PLAN
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

TIPO DE ENSEÑANZA
Mixto: presencial y no presencial

CENTROS DONDE SE IMPARTE
Escuela Politécnica Superior

ESTUDIO IMPARTIDO CONJUNTAMENTE CON
Solo se imparte en esta universidad

FECHAS DE EXAMEN
Acceda al listado de fechas de examen para esta titulación.

PLAN DE ESTUDIOS OFERTADO EN EL CURSO 2019-20

Leyenda: No ofertada | Sin docencia

MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

OBLIGATORIAS — 48 créditos

Curso	Título	Créditos	Asignatura
1	OBLIGATORIA	6	49500 - SISTEMAS DE GESTIÓN DE LA SEGURIDAD
1	OBLIGATORIA	6	49501 - PROTECCIÓN DE LA INFORMACIÓN
1	OBLIGATORIA	6	49502 - SEGURIDAD EN LOS SISTEMAS OPERATIVOS
1	OBLIGATORIA	6	49503 - SEGURIDAD EN LAS COMUNICACIONES
1	OBLIGATORIA	6	49504 - SEGURIDAD EN APLICACIONES Y BASES DE DATOS
1	OBLIGATORIA	6	49505 - DESARROLLO DE APLICACIONES SEGURAS
1	OBLIGATORIA	6	49506 - HACKING ÉTICO Y CONTRAMEDIDAS
1	OBLIGATORIA	6	49507 - ANÁLISIS FORENSE

TFM — 12 créditos

Curso	Título	Créditos	Asignatura
1	TRABAJO FIN DE MÁSTER	12	49508 - TRABAJO FIN DE MÁSTER

Superado este bloque se obtiene
MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD

OBJETIVOS

El Máster Universitario en Ciberseguridad ofrecerá una formación especializada de alto nivel, con el objetivo de mejorar las competencias específicas en el ámbito profesional de la seguridad informática. Los estudiantes adquirirán los conocimientos y habilidades necesarios para diseñar y ejecutar proyectos de seguridad informática tanto en organismos públicos como privados.

La demanda social del Máster Universitario en Ciberseguridad se puede considerar muy alta si se tienen en cuenta aspectos como:

- El aumento de la importancia tanto económica como estratégica del sector TIC en la sociedad.
- La demanda laboral creciente, incluso escasez, de profesiones cualificados y especializados en ciberseguridad.
- El aumento de la preocupación por la seguridad informática en todos los ámbitos de la sociedad: ciudadanos, empresas e instituciones públicas.

COMPETENCIAS

COMPETENCIAS GENERALES

- CG1:Saber aplicar los conocimientos adquiridos a problemas reales relacionados con la ciberseguridad.
- CG2:Ser capaz de trabajar y aprender de forma autodirigida o autónoma.
- CG3:Adaptarse a nuevas situaciones, en entornos nuevos o poco conocidos, fomentando la creatividad, la capacidad crítica y el espíritu emprendedor.
- CG4:Desenvolverse en contextos multidisciplinares y/o internacionales aportando soluciones desde el punto de vista de la ciberseguridad.
- CG5:Conocer y aplicar en cada situación las responsabilidades sociales, éticas y legales vinculadas a la aplicación de los conocimientos.
- CG6:Gestionar la información y los recursos disponibles.
- CG7:Ser capaz de trabajar en equipo con iniciativa y espíritu colaborador.
- CG8:Ser capaz de adaptarse al ambiente cambiante propio de la disciplina y de comprender y aplicar los nuevos avances técnicocientíficos relacionados con la ciberseguridad.
- CG9:Saber proyectar, diseñar, desarrollar, implantar y mantener productos, aplicaciones y servicios relacionados con la ciberseguridad, teniendo en cuenta aspectos técnicos, económicos y de eficiencia.
- CG10:Saber dirigir proyectos relacionados con la ciberseguridad, cumpliendo la normativa vigente y asegurando la calidad del servicio.

COMPETENCIAS BÁSICAS

- 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 ESPECÍFICAS

- CE1:Ser capaz de combinar tecnologías de seguridad activa y pasiva para diseñar soluciones integrales.
- CE2:Ser capaz de fortalecer los sistemas operativos implantando medidas de seguridad.
- CE3:Ser capaz de administrar y configurar de manera segura los servicios de Internet.
- CE4:Ser capaz de diseñar arquitecturas de seguridad de sistemas de comunicaciones.
- CE5:Ser capaz de identificar, analizar y evaluar las vulnerabilidades y riesgos de seguridad de las redes, los sistemas informáticos y las aplicaciones.
- CE6:Ser capaz de diseñar y planificar estrategias de protección y defensa de entornos informáticos corporativos, basándose en las tecnologías y herramientas de seguridad informática existentes.
- CE7:Ser capaz de utilizar las herramientas y técnicas de manipulación de dispositivos electrónicos e informáticos para extraer de ellos cualquier evidencia digital, de adoptar las medidas adecuadas para su preservación como prueba legal.
- CE8:Ser capaz de aplicar el método científico en el desarrollo del caso forense digital, conocer los procedimientos y las herramientas de análisis de las pruebas digitales y ser capaz de documentar adecuadamente los hallazgos de la investigación en un informe forense con validez judicial.
- CE9:Ser capaz de integrar distintas primitivas criptográficas para diseñar protocolos de seguridad.
- CE10:Ser capaz de seleccionar y utilizar las diferentes técnicas criptográficas de protección de la información más adecuadas.
- CE11:Ser capaz diseñar y desarrollar aplicaciones que garanticen la privacidad y la seguridad de la información.

- CE12:Ser capaz de diseñar y desarrollar aplicaciones seguras atendiendo a criterios de usabilidad, robustez y eficiencia.
- CE13:Ser capaz de conocer y aplicar los diferentes enfoques y metodologías del desarrollo y auditoría de software seguro.
- CE14:Ser capaz de diseñar el plan de continuidad de negocio y el plan de concienciación y formación en seguridad informática de una organización.
- CE15:Ser capaz de construir un sistema de clasificación de la información de una organización.
- CE16:Ser capaz de diseñar un plan de seguridad de la información.
- CE17:Ser capaz de diseñar, desarrollar, presentar y defender, individualmente ante un tribunal universitario, un trabajo integral de ciberseguridad en el que se sinteticen los conocimientos adquiridos en las enseñanzas.

COMPETENCIAS TRANSVERSALES

- CT1:Desarrollar competencias en un idioma extranjero a nivel técnico en el ámbito de la ciberseguridad
- CT2:Mostrar competencias informáticas e informacionales en el ámbito de la ciberseguridad.
- CT3:Reunir competencias en comunicación oral y escrita.

- Estructura del Máster por créditos y materia
- Distribución de asignaturas por curso / semestres
- Planificación general del plan de estudios

ESTRUCTURA DEL MÁSTER POR CRÉDITOS Y MATERIA

Tipo de materia	Créditos
Obligatorias (OB)	48
Trabajo Fin de Máster (OB)	12
TOTAL CRÉDITOS	**60**

DISTRIBUCIÓN DE ASIGNATURAS POR CURSO / SEMESTRES

CURSO 1º					
PRIMER SEMESTRE (30 ECTS)			SEGUNDO SEMESTRE (30 ECTS)		
ASIGNATURA	**TIPO**	**ECTS**	**ASIGNATURA**	**TIPO**	**ECTS**
SISTEMAS DE GESTIÓN DE LA SEGURIDAD	OB	6	DESARROLLO DE APLICACIONES SEGURAS	OB	6
PROTECCIÓN DE LA INFORMACIÓN	OB	6	HACKING ÉTICO Y CONTRAMEDIDAS	OB	6
SEGURIDAD EN LOS SISTEMAS OPERATIVOS	OB	6	ANÁLISIS FORENSE	OB	6
SEGURIDAD EN LAS COMUNICACIONES	OB	6	TRABAJO FIN DE MÁSTER	OB	12
SEGURIDAD EN APLICACIONES Y BASES DE DATOS	OB	6			

PLANIFICACIÓN GENERAL DEL PLAN DE ESTUDIOS

El Máster Universitario en Ciberseguridad de la Universidad de Alicante se compone de 8 materias obligatorias, que suman un total de 48 créditos ECTS, y de un Trabajo Fin de Máster de 12 créditos ECTS. Estas materias ofrecen una visión amplia de los diferentes aspectos relacionados con la ciberseguridad o seguridad informática, y no se ofrece ningún contenido optativo.

Todas las materias se imparten siguiendo una metodología enseñanza-aprendizaje de carácter semipresencial, en la que se definen las siguientes actividades: clases teóricas online, prácticas con ordenador, trabajo fin de máster tutorizado y trabajo autónomo del alumno. En particular:

1. En las actividades teóricas online se desarrolla un aprendizaje experimental y creativo con material multimedia para la formación a distancia. Esta actividad se desarrollará mediante la metodología docente clase invertida (flipped classroom), que

surge en el marco de la docencia semipresencial como un sistema de aprendizaje en el que los estudiantes adquieren los nuevos conocimientos a través de materiales y recursos interactivos en casa (online), para posteriormente realizar las actividades, problemas y debates en el aula con el soporte del profesor. El término sugiere la inversión de las clases tradicionales en las que en el aula los estudiantes recibían las lecciones y los ejercicios los realizaban en casa. El estudiante dispondrá de materiales y recursos de apoyo disponibles en línea para una consulta continuada en cualquier momento y de canales para comunicarse con sus compañeros y con el profesorado. Entre los materiales disponibles cabe destacar los videos educativos online, tutoriales, píldoras formativas, clases grabadas y blogs. La Universidad de Alicante dispone de la plataforma tecnológica necesaria para la elaboración y aprovisionamiento del material multimedia mencionado.

2. Las clases prácticas con ordenador se realizarán presencialmente en la Universidad de Alicante. Se plantearán para el desarrollo de trabajos prácticos de aplicación inmediata de las ideas vistas en las clases de teoría, o en el desarrollo de proyectos de naturaleza colaborativa. Dentro de las prácticas de todas las asignaturas, aparte de plantear una serie de problemas y ejercicios de desarrollo, se realizará un proyecto de integración común en el que se irán introduciendo nuevas características conforme se vayan estudiando en teoría. Se contará también con profesores invitados provenientes de diferentes empresas para profundizar en algunos casos prácticos de la vida real relacionados con los contenidos de las materias del máster. Este proyecto se construirá de forma incremental a lo largo de todo el máster, y será independiente del Trabajo Fin de Máster, que se realizará en el segundo cuatrimestre y deberá ser personal y original.

3. El trabajo fin de máster tutorizado tiene por objeto guiar, ayudar y aconsejar al alumno en todo el proceso de elección, diseño, desarrollo y defensa pública del trabajo fin de máster. La tutorización se realizará de manera grupal.

4. Una parte del trabajo que el estudiante debe realizar, se propondrá mediante un aprendizaje autónomo no presencial, como son el trabajo fin de máster y los trabajos que se encarguen para la evaluación de determinadas asignaturas. Por ello, todas las asignaturas utilizan tanto el UACloud de la Universidad de Alicante, como la plataforma de e-learning Moodle, que además de permitir a los profesores la realización de una estructuración del conocimiento que debe adquirir el estudiante, permite la introducción de hitos para la solicitud de cada una de las entregas que han de realizar a lo largo del curso. Esto ayuda al alumnado a gestionar y a organizar sus esfuerzos fuera de las aulas.

Todos los sistemas de evaluación de las asignaturas se realizarán de forma presencial en la Universidad de Alicante y así quedará garantizado el control de la identidad de los estudiantes. La evaluación tendrá como objetivo fundamental cuantificar el grado de cumplimiento de los objetivos formativos. Además, en todas las materias, la evaluación a realizar tendrá en cuenta los siguientes supuestos:

- Existen normas predefinidas y conocidas de antemano por el alumnado.
- Es coherente con los objetivos fijados de antemano.
- Abarca todos los niveles de conocimiento y actividades del alumnado en relación a cada materia.
- Habrá diferentes modalidades de evaluación como pruebas y exámenes, evaluación de prácticas realizadas de forma individual o en grupo, etc.

- Requisitos de Acceso
- Admisión y Criterios de Valoración
- Preinscripción y Matrícula
- Oferta de Plazas

REQUISITOS DE ACCESO

Según la Normativa de la Universidad de Alicante, para acceder a las enseñanzas oficiales de Máster Universitario será necesario:

1. Estar en posesión de un TÍTULO UNIVERSITARIO OFICIAL ESPAÑOL u otro expedido por una institución de educación superior del EEES (Espacio Europeo de Educación Superior) que facultan en el país expedidor del título para el acceso a enseñanzas de Máster.
2. Estar en posesión de un TÍTULO DE EDUCACIÓN SUPERIOR EXTRANJERO que haya sido HOMOLOGADO al título que permite acceder a los estudios solicitados.
3. Estar en posesión de un TÍTULO UNIVERSITARIO obtenido en una Universidad o Centro de Enseñanza Superior de PAÍSES AJENOS AL EEES, sin necesidad de la homologación previa de sus estudios. En este supuesto hay que tener en cuenta:
    - El Título no homologado requiere un informe técnico de equivalencia expedido por la Universidad de Alicante (ContinUA - Centro de Formación Continua), por el que se deberá abonar la tasa correspondiente.
    - El acceso por esta vía no implicará, en ningún caso, la homologación del título previo de que esté en posesión el/la interesado/a, ni su reconocimiento a otros efectos que el de cursar las enseñanzas de máster universitario.

ADMISIÓN Y CRITERIOS DE VALORACIÓN

Según el artículo 20 de la Normativa sobre títulos oficiales de Máster Universitario de la Universidad de Alicante (BOUA 20/12/2012), el órgano encargado de llevar a cabo la selección del alumnado a efectos de su admisión será la Comisión Académica del Máster que estará compuesta al menos por:

- El Coordinador o Coordinadora del máster universitario, que la preside.
- Un mínimo de tres miembros representantes del profesorado que imparte docencia en el máster universitario, elegidos entre y por el profesorado del máster universitario, procurando que estén representados los departamentos que intervienen en el plan de estudios.
- 1 representante del centro proponente.
- 1 representante del alumnado, que será elegido cada año entre y por el alumnado del máster universitario.
- 1 representante de las empresas y/o instituciones cuando se contemplen prácticas externas. Será propuesto por el Coordinador o Coordinadora del máster universitario, oídas las empresas y/o instituciones.
- 1 miembro del PAS para cuestiones relacionadas con la gestión administrativa del máster universitario.

La admisión será directa en los siguientes casos:

- Quienes estén en posesión del título de Grado en Ingeniería Informática.
- Quienes estén en posesión del título de Grado en Ingeniería Multimedia.
- Quienes estén en posesión de un título de Ingeniero/Licenciado o Ingeniero Técnico en Informática correspondiente a anteriores ordenaciones de las enseñanzas universitarias.

- Quienes estén en posesión del título de Ingeniero o Graduado en tecnologías de las Telecomunicaciones.

En caso de existir un número mayor de solicitudes que de plazas, se utilizará el expediente académico para establecer un orden en las solicitudes.

PREINSCRIPCIÓN Y MATRÍCULA

PREINSCRIPCIÓN +info

El alumno interesado en cursar un Máster Oficial en la UA, deberá realizar una preinscripción en los plazos y condiciones que se establezcan anualmente.

MATRÍCULA +info

Tras la publicación de las listas definitivas de admitidos se enviará por correo electrónico a los alumnos admitidos una contraseña que servirá de identificación de usuario para poder matricularse a través de **Campus Virtual** en los plazos y condiciones que se establezcan anualmente.

En el procedimiento de matrícula, los **documentos expedidos en el extranjero** deberán ser oficiales y estar debidamente legalizados y traducidos, más información:

- http://sga.ua.es/es/normativa-academica/legalizacion/legalizacion-de-documentos.html

OFERTA DE PLAZAS

CURSO	OFERTA DE PLAZAS
2018-19	20

CALENDARIO DE IMPLANTACIÓN

Cronograma de implantación del Título

Curso académico	Implantación del máster
2018-2019	1º curso

- Memoria Verificada
- Resolución Consejo de Universidades (CU): Verificación positiva
- Autorización de la Generalitat Valenciana

Sistema de Garantía Interna de Calidad (SGIC) del Título

- Estructura del Centro para la Calidad
  - Comisión de Garantía Interna de Calidad
  - Otras Comisiones
- Manual SGIC
- Procedimientos
  - Estratégicos (PE)
  - Clave (PC)
  - Apoyo (PA)
  - Medida (PM)
- Gestión del SGIC (Acceso a ASTUA)

Seguimiento del Título

- Autoinformes UA
- Informes externos AVAP
- Otros informes
- Planes de mejora
- Progreso y resultados del aprendizaje

Información del Centro	Información general para el alumno
• **Escuela Politécnica Superior** Campus de San Vicente del Raspeig Ctra. de Alicante s/n 03690 San Vicente del Raspeig (Alicante) Teléfono:+ 34 96 590 3648 Fax:+ 34 96 590 3644 eps@ua.es http://www.eps.ua.es/ • **Centro de Formación Continua (ContinUA)** **Solo para el proceso de preinscripción** Edificio Germán Bernácer, planta baja Teléfono: + 34 96 590 9422 Fax: + 34 96 590 9442 continua@ua.es http://web.ua.es/es/continua	• Becas y ayudas • Alojamiento • Comedores y cafeterías • Transporte • Atención médica de urgencia • Seguros • Atención estudiantes con necesidades especiales • Representación y participación estudiantil • Tarjeta de identificación universitaria (TIU) • Preguntas frecuentes
Normativa general de la UA	**+ Información titulación**
• Normativa y procedimientos académicos de la Universidad de Alicante	• Publicación del plan de estudios (BOE 16/02/19) • Web propia • Folleto informativo • Datos del título en el RUCT