

## 5. PLANIFICACION DE LAS ENSEÑANZAS

A lo largo de este apartado se presenta, en detalle el conjunto de módulos y asignaturas que componen el Máster. La carga docente del Máster es de 60 créditos ECTS, de los cuales:

- El alumno tendrá que cursar obligatoriamente 45 créditos ECTS.
- El alumno podrá seleccionar 6 créditos ECTS en asignaturas optativas correspondientes a los módulos de Seguridad en entornos Web, Auditoría de seguridad o Peritaje informático. Así mismo, el alumno en lugar de realizar estos créditos optativos podrá realizar Prácticas de empresa con una duración de 150 horas (6 créditos ECTS) en algunas de las empresas que firmen convenios de colaboración con el Máster (se adjuntan cartas de intenciones de algunas de ellas).
- Los 9 créditos restantes corresponden al Trabajo Fin de Título obligatorio en este tipo de titulaciones.

### 5.1. Estructura de la enseñanza y descripción del plan de estudios

TIPO DE MATERIA		Nº créditos ECTS
Ob	Obligatorias	45
Op	Optativas	6
PE	Prácticas externas (si son obligatorias)	(6)
TFM	Trabajo Fin de Título (obligatorio en Máster)	9
CRÉDITOS TOTALES		60

#### Relación de módulos, materias y asignaturas del plan de estudios:

Módulos	ECTS	Materias / asignaturas	ECTS	Tipo	Semestre
Módulo A: Seguridad en Internet	3	A1.- Seguridad en Internet	3	Ob	S1
Módulo B: Seguridad de Sistemas	9	B1.- Introducción a la seguridad de sistemas	3	Ob	S1
		B2.- Aseguramiento de servidores, backups y monitorización	3	Ob	S1
		B3.- Seguridad en redes	3	Ob	S1
Módulo C: Desarrollo de aplicaciones seguras	9	C1.- Programación Segura, vulnerabilidades	3	Ob	S1
		C2.- Desarrollo de Exploits con Metasploit	3	Ob	S1
		C3.- Ingeniería Inversa, Cracking, Tipos de protecciones y debilidades	3	Ob	S1
Módulo D: Aspectos legales	6	D1.- Derecho y seguridad informática	3	Ob	S2
		D2.- Régimen jurídico en Internet	3	Ob	S2
Módulo E: Seguridad en entornos Web	9	E1.- Programación web segura	3	Ob	S2
		E2.- Problemas de seguridad Web, Tipos de ataques	6	Op	S2
Módulo F: Auditoría de seguridad	9	F1.- Introducción a la auditoría de seguridad	3	Ob	S1
		F2.- Metodologías	3	Op	S1
		F3.- Certificaciones	3	Op	S1
Módulo G: Metodologías para llevar a cabo peritaje informáticos	9	G1.- El perito informático forense	3	Ob	S2
		G2.- La evidencia telemática, técnicas y herramientas	3	Op	S2
		G3.- El informe pericial	3	Op	S2

### Líneas de optativas ofertadas (y relación, en su caso, con especializaciones):

El Máster no tiene especialidades, los estudios conducen a la adquisición de los conocimientos para actuar como Experto en Seguridad en Internet.

No obstante, en el programa académico del Máster se contemplan la existencia de 6 créditos ECTS que el estudiante podrá elegir entre las asignaturas de los Módulos E, F y G; o la realización de un máximo de 150 prácticas (correspondientes a 6 créditos ECTS) de empresa en una entidad externa.

### Contribución de las materias al logro de las competencias del título:

	CB1	CB2	CB3	CB4	CB5	CG1	CE1	CE2	CE3	CE4	CE5	CE6	CE7	CE8	CE9	CE10
A 1	*	*	*	*	*	*					*	*				
B 1	*	*	*	*	*	*	*				*	*			*	
B 2	*	*	*	*	*	*	*				*	*		*	*	
B 3	*	*	*	*	*	*	*				*	*			*	
C 1	*	*	*	*	*	*	*	*	*			*				
C 2	*	*	*	*	*	*	*	*	*			*				
C 3	*	*	*	*	*	*	*	*	*			*				
D 1	*	*	*	*	*	*					*				*	*
D 2	*	*	*	*	*	*					*				*	*
E 1	*	*	*	*	*	*	*	*	*	*	*					
E 2	*	*	*	*	*	*					*	*			*	*
F 1	*	*	*	*	*	*					*	*		*	*	
F 2	*	*	*	*	*	*	*				*	*		*	*	
F 3	*	*	*	*	*	*	*				*	*		*	*	
G 1	*	*	*	*	*	*	*							*	*	*
G 2	*	*	*	*	*	*	*				*	*		*	*	*
G 3	*	*	*	*	*	*	*				*	*		*	*	*

**Organización temporal de asignaturas:**

Semestre	Asignatura	ECTS	Tipo
S1	A1.- Seguridad en Internet	3	Ob
S1	B1.- Introducción a la seguridad de sistemas	3	Ob
S1	B2.- Aseguramiento de servidores, backups y monitorización	3	Ob
S1	B3.- Seguridad en redes	3	Ob
S1	C1.- Programación Segura, vulnerabilidades	3	Ob
S1	C2.- Desarrollo de Exploits con Metasploit	3	Ob
S1	C3.- Ingeniería Inversa, Cracking, Tipos de protecciones y debilidades	3	Ob
S2	E1.- Programación web segura	3	Ob
S2	E2.- Problemas de seguridad web, Tipos de ataques	6	Op
S1	F1.- Introducción a la auditoría de seguridad	3	Ob
S1	F2.- Metodologías	3	Op
S1	F3.- Certificaciones	3	Op
S2	G1.- El perito informático forense	3	Ob
S2	G2.- La evidencia telemática, Técnicas y herramientas	3	Op
S2	G3.- El informe pericial	3	Op
S2	D1.- Derecho y seguridad informática	3	Op
S2	D2.- Régimen jurídico en Internet	3	Op

El periodo docente comenzará en las primeras semanas del mes de octubre y terminarán entre marzo y abril. A continuación los alumno podrán realizar el Trabajo Fin de Título y

**Mecanismos de coordinación docente entre asignaturas (en la organización horaria y de desarrollo y en la coherencia de objetivos) del plan de estudios:**

El órgano de gobierno más importante en el marco de este título propio del Máster, será la Comisión Académica, cuya composición será la siguiente:

- El director el Máster.
- Dos profesores PDI-USAL, uno de ellos actuará como secretario.
- Un profesor externo asociado al entorno académico.
- Dos profesionales externos de reconocido prestigio y asociados al mundo empresarial.
- Dos alumnos del Título Propio, en cualquier caso la representación de los estudiantes deberá ser al menos del 25%.

La coordinación general del Máster estará delegada por la comisión académica en el director del título propio Dr. D. Juan M. Corchado Rodríguez, Catedrático asociado al Departamento de Informática y Automática. No obstante, el director académico podrá convocar reuniones extraordinarias de la Comisión Académica en el caso de que sea

necesario, con el objeto de resolver problemas que se puedan dar en el desarrollo de la docencia del título propio, tal y como indica el Sistema de Garantía de Calidad (interno).

Dado la elevada carga docente del Título Propio de Máster que se propone, 60ECTS, el director académico requiere de ayuda por parte del personal docente en las labores de coordinación. Por ello será necesario definir una jerarquía entre profesores, coordinadores y director académico. En este sentido, se contemplan las siguientes figuras:

- **Coordinador Académico**, que será el director del Máster. el director del Máster podrá delegar estas funciones en un profesor del Máster, siempre y cuando éste sea PDI-USAL. El coordinador Académica tendrá la obligación de establecer reuniones periódicas de coordinación con los diferentes Coordinadores de Módulo.

Su labor principal será la de realizar la coordinación general del Título Propio de Máster, es decir, realizar la coordinación entre los módulos y asignaturas que lo componen.

- Deberá realizar reuniones de seguimiento periódicas para cada módulo y asegurarse de que la coordinación interna de cada módulo se está llevando a cabo correctamente y en los plazos adecuados.
- Definir, revisar o actualizar las competencias específicas y transversales de los módulos/asignaturas/materias, en colaboración con los coordinadores de módulo, asegurando que no existe solapamiento entre ellas.
- Informar a la Comisión Académica de la coordinación y actividades que se están llevando a cabo en el título propio.
- Ejecutar sistemáticamente los mecanismos definidos en el Sistema de Garantía de Calidad para asegurar que se están cumpliendo los objetivos docentes propuestos, y la máxima calidad en la formación.
- Tomar las medidas adecuadas en el caso de que se detecten desviaciones o incidencias en el desarrollo de la formación del Máster, entre las que puede estar la de convocar reuniones extraordinarias de la Comisión Académica para solucionar conflictos.
- Reservar de espacios (aulas de pupitres, aulas de informática y plataforma de tele formación) para la ejecución de la formación. Coordinar la disponibilidad de recursos con los responsables del centro académico, en este caso, la Facultad de Ciencias.
- Intercambiar experiencias metodológicas entre los diferentes profesores de las asignaturas.
- Atender a los estudiantes, así como resolver cualquier tipo de duda que estos tengan sobre el desarrollo general del Máster.
- Atender las sugerencias y propuestas de mejora realizadas por los estudiantes.
- Coordinar la inclusión de todas las actividades realizadas en el Informe Interno de Seguimiento del Máster.
- Definir, revisar o actualizar las competencias específicas y transversales de cada módulo, y determinar los objetivos específicos a lograr.
- Asegurarse que no existe repetición o carencia en los planes docentes causadas por la carencia de coordinación entre módulos.

- Coordinador de Módulo, su labor será la de coordinar la docencia entre las diferentes asignaturas/materias que componen un módulo. Será designado por el coordinador académico entre todos los entre todos los profesores que imparten docencia en las asignaturas/materias del módulo, siguiendo criterios de experiencia y méritos acreditados. Para realizar la coordinación convocará reuniones periódicas de seguimiento con los coordinadores de cada asignatura.
- Sus tareas principales serán las siguientes:
  - Evitar el solapamiento de competencias/objetivos docentes entre las asignaturas del módulo
  - Revisar y validar la propuesta de plan de cada bloque, velando para estas contribuyan de la forma prevista a los objetivos generales del producto formativo.
  - Realizar un seguimiento sistemático de la ejecución del Plan Docente de cada asignatura. Con cuyo objeto, se planificará cada curso la realización de las reuniones necesarias con el equipo docente del módulo, considerando imprescindibles la reunión inicial de curso, la de seguimiento y la de fin. No siendo necesariamente estas reuniones presenciales, sino que también pueden ser online a través de videoconferencia.
  - Informar al Coordinador Académico formativo de las desviaciones, incidencias o no conformidades en la impartición de las asignaturas y proponer soluciones.
  - Elaborar los informes de seguimiento del bloque durante su prestación y al acabamiento del curso, proponiendo las mejoras oportunas.
  - Organizar y liderar la comunidad de aprendizaje, facilitando el intercambio y la socialización del conocimiento.
  - Revisar, validar y actualizar los materiales didácticos que se utilicen (en cualquier formato).
  - Participar en la redacción del Informe Interno de Seguimiento del Máster, según lo requiera el coordinador académico.
- Profesores, son los docentes de las asignaturas. Su labor será la de impartir docencia, coordinando la misma en función de las directrices propuestas por el Coordinador de Módulo.

Sus funciones principales serán las de:

- Impartir docencia en cada una de las asignaturas en la que es profesor, velando por el cumplimiento de los objetivos docentes marcados previamente.
  - Realizar un seguimiento sistemático de la evaluación de los alumnos siguiendo unos criterios objetivos y las directrices marcadas previamente al inicio del curso.
  - Informar al Coordinador de Módulo de las desviaciones, incidencias o no conformidad que puedan ocasionarse en el desarrollo de cada asignatura.
  - Revisar y actualizar los material didácticos que se utilicen en coordinación con el Coordinador de Módulo.
- Tutores, son docentes que asistirán a los profesores en las tareas de tutorización, principalmente online. El objetivo es que el alumno tenga un

seguimiento individualizado y el tiempo de respuesta sea lo más corto posible.

- Realizar un seguimiento individualizado de los alumnos, siguiendo criterios objetivos, y las directrices del o los profesores de la asignatura.
- Informar a los profesores de cualquier incidencia que pueda surgir en el proceso de tutorización.

Dentro de esta jerarquía se completa el puesto de coordinador de asignatura, en casos muy excepcionales también donde la complejidad técnica o de coordinación de la asignatura sea alta. No obstante, generalmente, esta figura no es necesaria, ya que con módulos de 3 asignaturas como máximo, como es este caso, un nivel de coordinación adicional no se considera necesario y puede llegar a ser contraproducente.

Finalmente, en caso de existir la necesidad, y de forma puntual también se fija la figura de Técnico en Teleformación, cuya labor será la de dar asistencia técnica a los profesores y tutores en su interacción la plataforma de teleformación.

### Prácticas externas (justificación y organización):

Las prácticas externas se realizarán en las empresas del sector que muestren su interés para acoger alumnos para el desarrollo de las mismas, así como las empresas que muestren su interés en el futuro. El programa de prácticas de Externas estará regulado por el Servicio de Inserción Profesional y Empleo (SIPPE) dependiente del Vicerrectorado de Estudiantes e Inserción Profesional. Las prácticas se oficializarán a través de un convenio específico renovable anualmente con cada una de las empresas interesadas. La Comisión Académica del Master elaborará la normativa en la que se garantice que las actividades desarrolladas por el alumno permitan que el mismo alcance las competencias deseadas.

En cada curso académico, el Director de Máster, asistido por la Comisión Académica, revisará la lista de empresas que con las que se han establecido convenios de colaboración y realizará una ronda de consultas, acerca del número de alumnos y el tipo de prácticas que pueden ofrecerse en el año en curso. Posteriormente, con estos datos, se realizará la asignación entre alumnos y empresas, teniendo en cuenta la preferencias de perfiles de alumnos por parte de las empresas, así como las preferencias de los propios estudiantes.

Por cada alumno, la empresa deberá asignar un responsable que tutorice las prácticas de empresa, guíe al alumno y finalmente lo evalúe, emitiendo un informe a tal efecto. Por su parte, del mismo modo, el título propio deberá asignar un tutor a cada alumno, que será el coordine la participación del alumno en la empresa, a través del seguimiento de reuniones y tutorías (online y presenciales). Este tutor, será el evalúe la asignatura a través de los siguientes baremos:

- Informe del tutor externo.
- Entrevistas personales del alumno.
- Informe del alumno
- Grado de completitud del trabajo propuesto.

La duración de las práctica será de 9 créditos ECTS (225 horas) que se realizarán en un horario y fechas que se establecerán de mutuo acuerdo entre la empresa, el alumno y el tutor responsable por parte del Título Propio, respetando siempre la normativa en vigor establecida por la Universidad de Salamanca para tal efecto. El detalle de las prácticas de las prácticas (contenidos, tipo de jornada, fecha de inicio, fin, etc.) se oficializarán como anexo al convenio de colaboración entre la Universidad y la

empresa.

**Idiomas (justificación y organización):**

La docencia se impartirá en español salvo en algunos seminarios que se pueden impartir en inglés. Este idioma se utilizará en parte de la bibliografía y en documentación técnica y material audiovisual.

**Tipo de enseñanza (presencial, semipresencial, a distancia) (justificación y organización):**

La docencia será online. La metodología formativa, y el modelo de evaluación se exponen en detalle en los siguientes apartados (Actividades formativas y Sistemas de Evaluación).

**Actividades formativas (justificación y organización):**

La metodología de formación que se sigue en el marco de esta titulación permitirá a los alumnos aprender practicando, colaborando y cooperando entre ellos y con los profesores. La formación se impartirá teniendo en cuenta que los estudiantes son profesionales que deben llegar a cabo una jornada laboral y la deben compatibilizar con el estudio.

La metodología docente debe ser un trabajo que refleje de forma razonada el qué, el cuánto, el cuándo, el cómo y el dónde enseñar. Estos cinco aspectos permiten concretar no sólo lo qué se va a enseñar, con cuánta profundidad y cuándo se van a ir introduciendo los temas, sino también el cómo se va a enseñar, es decir, la metodología docente que se va a emplear. Se propone un modelo constructivista, basado en objetivos, que permita al alumno aprender practicando y descubriendo. En este contexto formativo, la utilización de las nuevas tecnologías de la información y la comunicación (TIC) son fundamentales. Internet se ha convertido en un elemento dinamizador del conocimiento, en el que se puede y debe apoyar la docencia, especialmente en un área como ésta, dado el perfil tecnológicamente avanzado que se le presupone a los alumnos.

Los tres primeros aspectos (qué, cuánto y cuándo) quedan claramente reflejados en la estructura académicamente propuesta, susceptible de ser modificado, ampliada y mejorada en función de la incesante evolución de la tecnología. Respecto al dónde, los alumnos utilizarán la plataforma BISITE - Campus On Line, además de los espacios físicos disponibles en la Facultad de Ciencias Además se incorporará acceso a un potente sistema de videoconferencia múltiple que permite la conexión a través de Internet de los estudiantes y tutores.

El cómo que es el aspecto que permite alcanzar el qué y el cuánto se determina a través de la metodología docente. En este sentido se propone un paradigma híbrido entre el constructivista y el descubrimiento activo. Tradicionalmente se le ha prestado más atención e importancia al qué enseñar que al cómo enseñar, lo que llevó a planificar la enseñanza prestando atención sólo a la materia y olvidando a los sujetos que debían aprender. Se propone este modelo híbrido, que concibe la enseñanza como una actividad crítica y al alumno como un profesional autónomo que investiga reflexionando sobre la práctica. En este enfoque, la enseñanza no es una simple transmisión de conocimiento, es un conjunto de métodos de apoyo que permite a los

alumnos construir su propio saber, centrando la educación no en contenidos, sino en objetivos que se pretenden alcanzar. Los objetivos plantean “lo que se pretende que el alumnado llegue a saber” como consecuencia del proceso de aprendizaje, y obligan por tanto a planificar la docencia orientándola al logro de tales objetivos marcados previamente. Por otro lado los objetivos también proporcionan un medio de evaluación del éxito de la docencia, pues se podrá observar el grado de cumplimiento de los mismos después del proceso docente. Hay que destacar asimismo que la enseñanza centrada en objetivos, plantea por primera vez que una enseñanza de calidad debe perseguir no sólo que el alumnado adquiera no sólo ciertos “conocimientos teóricos” como en la enseñanza tradicional, sino que también resalta la importancia de la adquisición de destrezas o “conocimientos prácticos” y de actitudes/comportamientos.

A continuación se detallan las diferentes acciones formativas que se llevarán a cabo en el contexto del Título Propio de Máster. Para la elaboración de este listado de acciones formativas se ha seguido las Directrices para la elaboración de las fichas de planificación docente de asignaturas y guías académicas de titulación de Grado y Máster, aprobado en el consejo de Docencia de 16 de enero de 2012.

- Actividades introductorias (dirigidas por el profesor).
  - Actividades introductorias. Este tipo de actividades serán realizadas al inicio de los módulos, para poner a los alumnos en el contexto de la formación que se va a impartir en el módulo.
    - *Formación a distancia*: Esta información estará disponible en la plataforma online al inicio del módulo y de cada asignatura, junto con los primeros contenidos docentes.
- Actividades teóricas (dirigidas por el profesor).
  - Sesión magistral. Presentación sintética, secuencial, motivadora y precisa sobre los aspectos clave de los contenidos de la asignatura.
    - *Formación a distancia*: Las clases magistrales se grabarán y colgarán a través de la plataforma, así mismo, también se emitirán en directo a través de video streaming.

En cualquier caso, los alumnos dispondrán de abundante documentación textual y audiovisual en formato digital a través de la plataforma, el seguimiento de estos contenidos será guiado por el profesor y los recursos técnicos disponibles en la propia plataforma.

- Actividades prácticas guiadas (dirigidas por el profesor).
  - Prácticas en aula de informática. Una vez que se realice las sesiones formativas magistrales e introductorias y magistrales, se realizarán las actividades guiadas. En estas actividades prácticas se intercalará teoría y práctica para que el alumno pueda construir adecuada su propio mapa mental sobre la material.
    - *Formación a distancia*. Las prácticas guiadas, se sustituirán en la formación mediante recursos y guiones sobre las prácticas, unidos a videos explicativos.

Así mismo, al igual que en las sesiones magistrales, las prácticas se emitirán en directo y se grabarán para que los alumnos online las puedan seguir.

- Atención personalizada (dirigidas por el profesor).
  - Tutorías. Se utilizará para comprender y ayudar al estudiante, así como guiarlo en su trabajo individual. Tratando de que la formación sea personalizada.
    - *Formación a distancia*. Seguimiento realizado a través de videoconferencia, audioconferencia, mensajería (síncrona o asíncrona) y email.



- Actividades de seguimientos on-line. A través del campus se realizarán diferentes actividades de interacción y seguimiento, que permitan facilitar el trabajo de los alumnos.
- **Actividades prácticas autónomas (Sin el profesor)**
  - Preparación de trabajos. Permite al alumno aprender en profundidad sobre un tema determinado. Esta estrechamente ligado a la siguiente forma de evaluación, ya que la preparación constituye el paso previo a la realización de trabajos.
  - Trabajos. El alumno tendrá que realizar informes o reportes sobre una tema concreto, así como prácticas individuales sobre algunos de los temas que componen las asignaturas. Estos trabajos podrán realizarse de forma individual y en grupo.
  - Resolución de problemas. Es un proceso mental que permite la identificación y análisis de un problema, y la propuesta de solución. En el marco del máster, los problemas serán eminentemente prácticos.
  - Foros de discusión. Los foros se utilizarán de forma online con dos objetivos primarios. En primer lugar, la dinamización de la formación, a través del planteamiento de preguntas en los foros que los alumnos tendrán que contestar, y los profesores podrán evaluar. En segundo lugar, la generación de debates públicos sobre cuestiones que tengan los alumnos, y que puedan ser objeto de interés por parte del resto de alumnos.

#### Sistemas de evaluación (justificación y organización):

A continuación se detallan las diferentes acciones de evaluación que se llevarán a cabo en el contexto del Título Propio de Máster. Para la elaborar este listado de acciones formativas se ha seguido las Directrices para la elaboración de las fichas de planificación docente de asignaturas y guías académicas de titulación de Grado y Máster, aprobado en el consejo de Docencia de 16 de enero de 2012.

- **Pruebas objetivas de tipo test.** Cuestionarios de evaluación que estarán disponibles a través de la plataforma online. Existirán dos tipos de test en el contexto de la formación del título propio.
  - *Test de autoevaluación*, que constará de una serie de preguntas orientadas a autoevaluar y a afianzar los conocimientos del alumno. La realización de este tipo de test será valorable en la evaluación continua de cada módulo. Los test de repaso tendrán entre 7 y 15 preguntas aleatorias, no existirá un tiempo para realizarlos y el número de intentos será ilimitado.
  - *Test de evaluación*, en cada asignatura, existirán un conjunto de test evaluación, en función de las necesidades docentes. que el alumno tendrá que aprobar para superar correctamente el módulo.
- **Pruebas prácticas.** Estas pruebas se corresponden con la evaluación de un conjunto de las actividades dónde el alumno deberá realizar trabajos individuales y en grupo. Los trabajos serán supervisados por un profesor/tutor y evaluados conjuntamente con otro profesor. La entrega de estas pruebas prácticas, será a través de la plataforma de formación y su realización será puramente online. No obstante, los alumnos podrán realizarlas en el horario de prácticas libres de las aulas de informática reservadas para este Título Propio.

A continuación se detallarán las directrices de evaluación de los alumnos por cada uno de los módulos que componen el Máster, es importante señalar, que los porcentajes exactos de evaluación se fijarán por la comisión académica y los coordinadores de módulos al inicio del curso académico:

- Evaluación alumnos matriculados en la modalidad online:
  - *Bloque A. Evaluación continua.* Participación en foros, videoconferencias, audioconferencias, participación activa en las clases online sincrónicas, test de autoevaluación, interacción en el campus de formación y acceso a recursos en la plataforma. Los criterios serán especificados por el coordinador de módulo.
  - *Bloque B. Realización de Test objetivos de evaluación.* Este tipo de test tendrán entorno a 20 preguntas aleatorias, los alumnos dispondrán de 40 minutos para completarlo y será necesario superar el 70% de las preguntas de forma que cada pregunta correcta otorga un punto y cada pregunta errónea penaliza 1 punto. Se concederán tres intentos para superar el test, teniendo en cuenta que las preguntas serán aleatorias en cada uno de ellos. Tras la realización del test, y en función de la evaluación continua el profesor de la asignatura determinará si es necesaria una prueba oral (realizada por videoconferencia) para validar los resultados del test y garantizar su autenticidad.
  - *Bloque C. Realización de Prácticas.* Se valorará su calidad técnica, la memoria realizada para presentar el trabajo realizado, la originalidad y el cumplimiento de las especificaciones indicadas en la definición del trabajo. Los trabajos serán propuestos por los profesores de cada asignatura y serán de tipo práctico. Si los evaluadores del trabajo consideran que no se ha realizado adecuadamente, sugerirán al alumno los cambios necesarios para superarlo y le proporcionarán un tiempo extra para que lo mejore. Tras la entrega de las prácticas, y en función de la evaluación continua el profesor de la asignatura determinará si es necesaria una prueba oral (realizada por videoconferencia) para analizar conjuntamente el trabajo realizado y garantizar su autenticidad.

La calificación de cada asignatura estará compuesta por la aritmética entre los tres bloques anteriores de evaluación. Así mismo, la calificación del módulo se corresponderá con la media ponderada de la calificación de cada asignatura, entre los créditos ECTS de la asignatura.

En el caso de la evaluación de las prácticas externas, el tutor interno responsable será el encargado de calificar al alumno atendiendo a los siguientes criterios:

- Informe del tutor externo.
- Entrevistas personales del alumno.
- Informe del alumno
- Grado de completitud del trabajo propuesto.

La calificación de las prácticas estará en función de la naturaleza de éstas, y será obligación del tutor o tutores de la prácticas establecerlas y comunicárselas alumno antes de comenzarlas.

La forma de calificación del Trabajo Fin de Título vendrá establecido por las directrices que conforman el apartado 3 del Reglamento de Trabajo o Proyecto de fin de Máster de la Universidad de Salamanca, aprobado por el Consejo de Gobierno de la Universidad en su sesión de 27 de Julio de 2010.

#### Sistema de calificaciones:

El sistema de calificaciones dentro de este Título Propio se ajustará al sistema de calificaciones vigente (RD 1125/2003), artículo 5º.

Los resultados obtenidos por el alumno en cada una de las materias del plan de estudios se calificarán en función de la siguiente escala numérica de 0 a 10, con expresión de un decimal, a la que podrá añadirse su correspondiente calificación cualitativa:

- 0-4,9: Suspenso (SS);
- 5,0-6,9: Aprobado (AP);
- 7,0-8,9: Notable (NT);
- 9,0-10: Sobresaliente (SB).
- La mención de Matrícula de Honor (MT) podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del 5% de los alumnos matriculados en una asignatura 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.

Así mismo, se seguirá la Normativa sobre el sistema de calificaciones y cálculo de la nota media y de la calificación global de los expedientes académicos de los estudiantes de la USAL (Consejo Gobierno 23/junio/2011) que actualiza el sistema de calificaciones y el cálculo de la nota media en la USAL [http://campus.usal.es/~gesacad/coordinacion/normativaproce/notas\\_23\\_06\\_2011.pdf](http://campus.usal.es/~gesacad/coordinacion/normativaproce/notas_23_06_2011.pdf)

Se tendrá en cuenta el Reglamento de Evaluación de la Universidad de Salamanca (aprobado en Consejo de Gobierno de Diciembre de 2008 y modificado en el Consejo de Gobierno de 30 de octubre de 2009) [http://campus.usal.es/~gesacad/coordinacion/normativaproce/regla\\_eval.pdf](http://campus.usal.es/~gesacad/coordinacion/normativaproce/regla_eval.pdf)

## 5.2. Descripción detallada de las asignaturas (FICHAS de planificación)

A lo largo de este apartado, se presentarán las fichas de las asignaturas que componen el Máster.

<p><b>MATERIA: A1.- Seguridad en Internet</b>  Módulo al que pertenece: A. Seguridad en Internet  Tipo: Obligatoria  ECTS: 3  Semestre: S1  Lenguas en las que se imparte: Español  Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE5 y CE6</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"> <li>• Adquirir las competencias básicas, generales y específicas detalladas anteriormente.</li> <li>• Adquisición de los principios generales sobre seguridad informática, y en especial, sobre seguridad en Internet, las redes de ordenadores y los nodos informáticos que la forman.</li> <li>• Distinguir entre los diferentes modelos criptográficos y aplicarlos correctamente en función del contexto.</li> </ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"> <li>• Introducción, definición y objetivos de la seguridad en Internet.</li> <li>• La seguridad en cifras.</li> <li>• Aspectos relevantes de la seguridad.</li> <li>• Aspectos desde los que se tiene que estudiar la seguridad (Sistemas, Información, Programación etc.).</li> <li>• Criptografía (Privacidad, Integridad, Autenticidad, No repudio).</li> <li>• Criptografía simétrica (AES).</li> <li>• Funciones Hash.</li> <li>• Criptografía Asimétricas (Fundamentos teóricos, cifrado, firma digital, aspectos importantes, algoritmos asimétricos, etc.).</li> <li>• Otras herramientas criptográficas (criptografía visual, dinero electrónico, certificado digital, infraestructura de claves públicas).</li> <li>• Comercio electrónico (Protocolos de seguridad, SSL, TSL, Protocolo IPsec).</li> </ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Esta asignatura tiene como objetivo introducir los principios generales sobre seguridad, y en especial, sobre seguridad en Internet. Los conceptos desarrollados en esta asignatura permiten al alumno conocer y formar el mapa mental acerca de la relación existente entre el resto de asignaturas y módulos que componen el Máster.</p> <p>No se contemplan requisitos previos que el alumno deba conocer, puesto que esta asignatura es de introducción.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: Seguridad en Internet</b>  Carácter: Obligatoria  ECTS: 3  Unidad temporal: S1  Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				8		0%
Sesión magistral				8		0%
Prácticas en el aula de informática				2		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				23		0%
Trabajos				18		0%
Resolución de problemas				11		0%
Foros de discusión				3		0%
Total Horas	75	Total Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: B1.- Introducción a la seguridad de sistemas</b> Módulo al que pertenece: B.- Seguridad de sistemas Tipo: Obligatoria ECTS:3 Semestre: S1 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE5, CE6 y CE9</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquirir de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Distinguir los diferentes problemas de seguridad, así como poseer la capacidad de identificarlos en un contexto real.</li><li>• Conocer y saber utilizar las herramientas que permiten asegurar un sistema informático.</li><li>• Comprender que la seguridad física es el primer problema de seguridad en cualquier infraestructura tecnológica</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Introducción y objetivos de la seguridad de sistemas, ámbito de aplicación.</li><li>• Protección del equipo (copias de seguridad, seguridad de la información, consejos de protección)</li><li>• La seguridad físicas (acceso físico, desastres naturales, desastres del entorno, protección de datos, listado de comprobaciones).</li><li>• Otras herramientas (Antivirus, cortafuegos, utilidades).</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Se conoce como Seguridad de sistemas, al aseguramiento de los nodos de redes que se encuentran en una red de ordenadores, esto es, servidores informáticos. El alumno deberá conocer como aplicar técnicas de seguridad para proteger estos equipos frente a posibles ataques.</p> <p>No se contemplan requisitos previos que el alumno sepa conocer, puesto que esta asignatura es de introducción.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: B1.- Introducción a la seguridad de sistemas</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S1 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS							
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad	
Actividades introductorias				2		0%	
Sesión magistral				8		0%	
Prácticas en el aula de informática				5		0%	
Tutorías							
Actividades de seguimiento online				5		0%	
Preparación de trabajos				16		0%	
Trabajos				17		0%	
Resolución de problemas				20		0%	
Foros de discusión				2		0%	
Total Horas	75	Total Presenciales	horas 0	Total Horas Trabajo Autónomo	75	0%	
SISTEMAS DE EVALUACION							
Prueba de evaluación				Ponderación máxima		Ponderación mínima	
Evaluación continua, Participación online y/o presencial				50%		40%	
Pruebas objetivas de tipo test				50%		40%	
Pruebas prácticas				50%		20%	

**MATERIA: B2.- Aseguramiento de servidores, backups y monitorización**

Módulo al que pertenece: B.- Seguridad de sistemas

Tipo: Obligatoria

ECTS:3

Semestre: S1

Lenguas en las que se imparte: Español

Modalidad de enseñanza: Online

**COMPETENCIAS:****Básicas / Generales / Transversales:** CB1, CB2, CB3, CB4, CB5 y CG1**Específicas:** CE1, CE5, CE6, CE8 y CE9**RESULTADOS DE APRENDIZAJE PREVISTOS:**

- Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.
- Aplicar técnicas y saber utilizar herramientas para monitorizar el estado de los servidores informáticos.
- Conocer los posibles modelos de realización de copias de seguridad, con el objetivo de aplicar el más adecuado en cada caso concreto en función del entorno tecnológico existente.
- Aplicar técnicas para proteger un servidor informático frente a posibles ataques externos.

**BREVE DESCRIPCIÓN DE CONTENIDOS:**

- Configuración y uso seguro (Acceso a la máquina, seguridad local, cuentas de usuario y grupos, auditoría, propietarios, permisos efectos).
- Teoría sobre copias de seguridad
- Herramientas existentes para realizar copias de seguridad.
- Monitorización de propósito general (Tweedo, Nagios, Watchdog).
- Monitorización especializada (IDS, clasificación IDS, tipos de análisis, respuesta, herramientas y complementos).
- Productos IDS (Snort, Microsoft ISA / Forefront, OSSEC, OSSIM).
- IDS de aplicación (PHPIDS, Mod\_security, IDS para Windows).

**OBSERVACIONES (Requisitos previos, coordinación. Otras)**

Los contenidos de esta asignatura son eminentemente prácticos y permitirán al alumno conocer tanto las técnicas y herramientas para instalar un servidor informático orientado a la explotación, asegurando que se cumplen directivas de seguridad y están preparado para resistir ataques de seguridad.

Esta asignatura requiere de los conceptos previos estudiados en la asignatura B1.- Introducción a la seguridad de Sistemas.

**ASIGNATURAS QUE COMPONEN LA MATERIA:****Asignatura 1: B2.- Aseguramiento de servidores, backups y monitorización**

Carácter: Obligatoria

ECTS:3

Unidad temporal: S1

Lenguas en las que se imparte: Español



ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				2		0%
Sesión magistral				8		0%
Prácticas en el aula de informática				15		0%
Tutorías						
Actividades de seguimiento online				5		0%
Preparación de trabajos				16		0%
Trabajos				17		0%
Resolución de problemas				10		0%
Foros de discusión				2		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: B3.- Seguridad en redes</b>  Módulo al que pertenece: B.- Seguridad de Sistemas  Tipo: Obligatoria  ECTS: 3  Semestre: S1  Lenguas en las que se imparte: Español  Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE5, CE6 y CE9</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"> <li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li> <li>• Conocer y evaluar los problemas de seguridad existentes en una red, así como los posibles puntos de vulnerabilidad.</li> <li>• Saber aplicar diferentes técnicas de seguridad función de la tipología, topología y protocolo de red.</li> <li>• Ser capaz de recuperar información acerca de una red de ordenadores (equipos vivos, elementos, paquetes de red, etc.).</li> </ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"> <li>• Introducción y ámbito de aplicación.</li> <li>• Acopio de información en Internet (portal web, buscadores, registros, información de red, DNS, contramedidas, etc.).</li> <li>• Descubrimiento de equipos vivos (Escaneado de puertos).</li> <li>• Sniffing y detección de sniffers).</li> <li>• Spoofing (nivel de enlace y nivel de red).</li> <li>• Firewals (Soluciones hardware y software y definición de políticas de filtrado)</li> <li>• Wifi (ocultación y cifrado).</li> </ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>En cualquier sistema informático, los diferentes equipos informáticos están conectados entre si a través de un red. Este medio de comunicación es un punto de vulnerabilidad ya que es por ella por donde viaja toda la información (encriptada o no). Por ello, en esta asignatura el alumno podrá conocer las principales técnicas y herramientas disponibles en el mercado para asegurar la seguridad en este punto de vulnerabilidad</p> <p>Esta asignatura requiere de los conceptos previos estudiados en la asignatura B1.- Introducción a la seguridad de Sistemas, se desarrollarán en paralelo a la asignatura B2.- Aseguramiento de servidores, backups y monitorización</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: B3.- Seguridad en redes</b>  Carácter: Obligatoria  ECTS: 3  Unidad temporal: S1  Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias						0%
Sesión magistral				4		0%
Prácticas en el aula de informática				8		0%
Tutorías						
Actividades de seguimiento online				5		0%
Preparación de trabajos				16		0%
Trabajos				20		0%
Resolución de problemas				20		0%
Foros de discusión				2		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

**MATERIA: C1.- Programación segura, vulnerabilidades**

Módulo al que pertenece: C. Desarrollo de aplicaciones seguras

Tipo: Obligatoria

ECTS: 3

Semestre: S1

Lenguas en las que se imparte: Español

Modalidad de enseñanza: online

**COMPETENCIAS:**

**Básicas / Generales / Transversales:** CB1, CB2, CB3, CB4, CB5 y CG1

**Específicas:** CE1, CE2, CE3 y CE6

**RESULTADOS DE APRENDIZAJE PREVISTOS:**

- Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.
- Aplicar un modelo de programación segura en el desarrollo de software de aplicación.
- Conocer las vulnerabilidades en el desarrollo de software, desde el punto de vista del programa software, así como de las debilidades de las arquitecturas computacionales.
- Capacitar para evaluar y emitir un juicio sobre el mismo las vulnerabilidades de un producto software previamente desarrollado.

**BREVE DESCRIPCIÓN DE CONTENIDOS:**

- Desbordamiento de buffer (estructura de memoria, pila de procesadores, desbordamiento de pila, creación de Shellcodes).
- Herramientas (Pax, Stackguard, ProPolice, ASLR).
- Otras tecnologías de protección (DEP, SEHOP).
- EMET
- Analizadores de código (Desbordamiento de memoria, variables, pila, herramientas existentes, etc.).
- Condiciones de carrera (Condiciones en secuencias no atómicas, Bloqueo de ficheros).

**OBSERVACIONES (Requisitos previos, coordinación. Otras)**

Esta asignatura permite ofrecer al alumno una visión general acerca de los problemas de seguridad que se puedan dar durante el desarrollo del software, de forma que sepa capaz de distinguir y eliminar vulnerabilidades software.

Es recomendable, aunque no indispensable, tener conocimientos básicos de programación.

**ASIGNATURAS QUE COMPONEN LA MATERIA:**

**Asignatura 1: C1.- Programación segura, vulnerabilidades**

Carácter: Obligatoria

ECTS: 3

Unidad temporal: S1

Lenguas en las que se imparte: Español

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				6		0%
Prácticas en el aula de informática				4		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				23		0%
Trabajos				20		0%
Resolución de problemas				12		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: C2.- Desarrollo de Exploits con metasploits</b> Módulo al que pertenece: C. Desarrollo de aplicaciones seguras Tipo: Obligatoria ECTS: 3 Semestre: S1 Lenguas en las que se imparte: Español Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE2, CE3 y CE6</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer la metodología para buscar vulnerabilidades ya conocidas en el software y saber aprovecharlas para realizar ataques contra la seguridad de sistemas, así como para evitar estos ataques.</li><li>• Saber desarrollar exploits de software existente en un entorno de formación.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Introducción, definiciones y ámbito de aplicación.</li><li>• El framework de desarrollo (metasploit)</li><li>• Ciclo de desarrollo (Fuzzing, Debugging, Stack/Heap Overflow, Craeción de exploits, Payloads, NOPS, Opcodes, Shellcodes, etc.).</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>El objetivo de esta asignatura es dar a conocer el framework metasploit, así como las directrices para la explotación de vulnerabilidades del software teniendo en cuenta la información disponible.</p> <p>Los conocimientos de esta asignatura son la continuación de la temática desarrollada en la asignatura previa del módulo C1.- Programación segura, vulnerabilidades</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: C2.- Desarrollo de Exploits con metasploit</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S1 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				2		0%
Sesión magistral				4		0%
Prácticas en el aula de informática				7		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				25		0%
Trabajos				20		0%
Resolución de problemas				12		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: C3.- Ingeniería Inversa, Cracking, tipos de protecciones y debilidades</b> Módulo al que pertenece: C. Desarrollo de aplicaciones seguras Tipo: Obligatoria ECTS: 3 Semestre: S1 Lenguas en las que se imparte: Español Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE2, CE3 y CE6</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Comprender las técnicas existentes para asegurar la protección de software comercial</li><li>• Aplicar metodologías sistemáticas para descubrir debilidades en las técnicas de protección, y en base a este conocimiento asegurar la protección del software desarrollado por el alumno.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Fundamentos y herramientas para realizar ingeniería inversa.</li><li>• Metodologías aplicables.</li><li>• Tipos de protección y debilidades (protección mediante cifrado, duración limitada, número limitado de ejecuciones, restricciones numéricas, protección con número de serie, ficheros clave, programas limitados, presencia del CD, protecciones comerciales, codificadores y compresores PE).</li><li>• Protecciones hardware (Método pregunta-respuesta, ejecución de componentes en el hardware, Rockey Smart de Feitan).</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>El alumno a lo largo de esta asignatura conocerá las técnicas para realizar ingeniería inversa sobre aplicaciones compiladas, de forma que pueda descubrir las metodologías existentes en la protección de software comercial.</p> <p>Se recomienda cursar previamente las asignaturas del módulo C1.- Programación segura, vulnerabilidades y C2.- Desarrollo de Exploits con metasploit</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: C3.- Ingeniería inversa, Cracking, tipos de protecciones y debilidades</b> Carácter: Obligatoria ECTS:3 Unidad temporal: S1 Lenguas en las que se imparte: Español</p>



ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				2		0%
Sesión magistral				4		0%
Prácticas en el aula de informática				7		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				25		0%
Trabajos				20		0%
Resolución de problemas				12		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: D1.- Derecho y seguridad informática</b> Módulo al que pertenece: D.- Aspectos legales Tipo: Obligatoria ECTS: 3 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE5, CE9 y CE10</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer el marco jurídico aplicable a Internet y a la informática en general.</li><li>• Saber evaluar si un sistema informático cumple con la legislación vigente.</li><li>• Saber evaluar si las acciones que se llevan a cabo pueden constituir un delito informático.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Delitos informáticos, caracteres y consecuencias.</li><li>• El acceso ilegal a datos reservados y sistemas de información. Hacking, intimidad y espionaje industrial</li><li>• La alteración, destrucción o inutilización de datos. Virus, crackings, ataques DdS.</li><li>• La posición jurídica de los responsables y encargados de los tratamientos de ficheros de datos.</li><li>• Las estafas y fraudes informáticos. Phising y spoofing.</li><li>• Acceso no autorizado a determinados servicios informáticos.</li><li>• La elusión de las medidas tecnológicas que protegen la propiedad intelectual.</li><li>• La responsabilidad de los proveedores de servicios de la sociedad la información.</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Esta asignatura tiene por objetivo darle al alumno una visión general sobre el marco jurídico existe y las posibles implicaciones en diferentes contextos tecnológicos.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: D1.- Derecho y seguridad informática</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				6		0%
Sesión magistral				14		0%
Prácticas en el aula de informática						0%
Tutorías						
Actividades de seguimiento online				5		0%
Preparación de trabajos				25		0%
Trabajos				20		0%
Resolución de problemas						0%
Foros de discusión				5		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: D2.- Régimen jurídico en Internet</b> Módulo al que pertenece: D.- Aspectos legales Tipo: Obligatoria ECTS: 3 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE5, CE9 y CE10</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer las diferentes leyes orgánicas del marco jurídico nacional aplicables en el contexto tecnológico.</li><li>• Conocer las implicaciones legales que conlleva diferentes actividades en el marco de Internet, como por ejemplo la compraventa, o las transferencias electrónicas de fondos o datos.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Derecho, copia privada y tecnología anticopia</li><li>• La responsabilidad de los PSSI por las actividades terceros en Internet.</li><li>• Regulación jurídica de la compraventa realizada en Internet</li><li>• Régimen jurídico de las transferencias electrónicas de fondos</li><li>• Régimen jurídico de las transferencias electrónicas de datos.</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>A partir de los conocimientos previos desarrollados en la asignatura previa del módulo (D1.- Derecho y seguridad informática), en este módulo se desarrollarán en profundidad las diferentes leyes existentes, siendo el principal objetivo su comprensión a la hora de la aplicación en casos prácticos.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: D2.- Regimen jurídico en Internet</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				6		0%
Sesión magistral				14		0%
Prácticas en el aula de informática						0%
Tutorías						
Actividades de seguimiento online				5		0%
Preparación de trabajos				25		0%
Trabajos				20		0%
Resolución de problemas						0%
Foros de discusión				5		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: E1.- Programación web segura</b> Módulo al que pertenece: E.- Seguridad en entornos Web Tipo: Obligatoria ECTS: 3 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE2, CE3, CE4, CE5</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer y aplicar los fundamentos de seguridad web a la hora de realizar aplicaciones para este entorno de despliegue cuyas características son tan particulares y a la vez está tan extendido.</li><li>• Conocer y aplicar las herramientas y técnicas de seguridad web.</li><li>• Conocer y aplicar las técnicas de técnicas de seguridad en aplicaciones web orientadas a plataformas móviles.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Introducción y ámbito de aplicación</li><li>• Vulnerabilidades (Inyección, XSS, Errores en autenticación, Referencias inseguras a objetos, CSRF (Cross Site Request Forgery), Configuración insegura, Almacenamiento inseguro, Errores de control de acceso, Protección en la capa de transporte y Redirecciones y envíos no válidos).</li><li>• Evaluación de la seguridad</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>El objetivo es conocer los problemas de seguridad existentes y los tipos de ataques en la seguridad de aplicaciones web.</p> <p>Sería recomendable, aunque no indispensable, que los que los estudiantes tuvieran nociones básicas sobre la programación en aplicaciones Web. Se proporcionará material de apoyo para los alumnos que no tengan este conocimiento.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: E1.- Programación web segura</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				2		0%
Sesión magistral				4		0%
Prácticas en el aula de informática				7		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				25		0%
Trabajos				20		0%
Resolución de problemas				12		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: E2.- Problemas de seguridad web, tipos de ataques</b> Módulo al que pertenece: E.- Seguridad en entornos Web Tipo: Optativa ECTS: 6 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE5, CE6, CE9 y CE10</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer los problemas de seguridad habituales en el entorno web, y en base a este conocimiento, desarrollar software para este entorno seguro.</li><li>• Evaluar y descubrir las vulnerabilidades de portales web públicos, con el objetivo de maximizar la seguridad de los mismos.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Problemas de seguridad (Entradas no validadas, Desbordamiento de buffer, manejo incorrecto de errores y denegación de servicios).</li><li>• Aplicación de las técnicas de seguridad en el entorno Web (Eliminación de directorios, CGI o ejemplo, deshabilitar el listado de directorio, usuario que ejecuta el servicio, perfilado de aplicaciones web).</li><li>• Metodología de ataques.</li><li>• Tipos de ataques (Hidden manipulation, Cookie Poisoning, Inyección SQL).</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Esta asignatura complementa a la anterior, y se recomienda cursar una vez se ha cursado la asignatura previa del módulo (E1.- Programación Web segura).</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: E2.- Problemas de seguridad web, tipos de ataques</b> Carácter: Optativa ECTS: 6 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>



ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				8		0%
Prácticas en el aula de informática				14		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				50		0%
Trabajos				40		0%
Resolución de problemas				30		0%
Foros de discusión				2		0%
Total Horas	150	Total horas Presenciales	0	Total Horas Trabajo Autónomo	150	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: F1.- Introducción a la auditoría de seguridad</b> Módulo al que pertenece: F.- Auditorías de seguridad Tipo: Obligatoria ECTS: 3 Semestre: S1 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE5, CE6, CE8 y CE9</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer los principios básicos de una auditoría informática en el contexto de un entorno tecnológico.</li><li>• Conocer la diferencia entre una auditoría informática y una auditoría de seguridad; y la diferencia de ambas con la consultoría.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• El concepto de auditoría, aspectos relevantes.</li><li>• Auditoría contra consultoría</li><li>• Auditoría informática</li><li>• Auditoría de seguridad</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Módulo introductorio sobre las Auditoría informática en general, y Auditoría en seguridad en particular. No se requiere ningún conocimiento previo.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: F1.- Introducción a la auditoría de seguridad</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S1 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				16		0%
Prácticas en el aula de informática						
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				30		0%
Trabajos				20		0%
Resolución de problemas						0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: F2.- Metodologías</b> Módulo al que pertenece: F.- Auditorías de seguridad Tipo: Optativa ECTS: 3 Semestre: S1 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE5, CE6, CE8 y CE9</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer y saber aplicar las metodologías existentes para poder realizar auditorías de seguridad de forma sistemática.</li><li>• Desarrollar auditorías de seguridad en entornos específicos a partir las directrices marcadas por una metodología.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Introducción, metodologías existentes</li><li>• Tipos de amenazas (vulnerabilidades, riesgo, exposición o impacto).</li><li>• Actuaciones (Evitarlos, Transferirlos, Reducirlos, Asumirlos)</li><li>• Tipos de metodologías (Cuantitativas, Cualitativas).</li><li>• Metodologías existentes</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Para cursar esta asignatura, se recomienda haber cursado previamente la asignatura F1.- Introducción a las auditorías de seguridad.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: F2.- Metodologías</b> Carácter: Optativa ECTS: 3 Unidad temporal: S1 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				16		0%
Prácticas en el aula de informática						
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				30		0%
Trabajos				20		0%
Resolución de problemas						0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: F3.- Certificaciones</b>  Módulo al que pertenece: F.- Auditorías de seguridad  Tipo: Optativa  ECTS: 3  Semestre: S1  Lenguas en las que se imparte: Español  Modalidad de enseñanza: Online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE5, CE6, CE8 y CE9</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"> <li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li> <li>• Conocer la certificación ISO 270001 y su marco de aplicación</li> <li>• Conocer la certificación OSSTMM y su marco de aplicación</li> <li>• Saber discernir que metodología aplicar en función del contexto en el que se realice la auditoría.</li> </ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"> <li>• Certificación ISO 27001. <ul style="list-style-type: none"> <li>○ Términos y definiciones (Seguridad de la información, Evaluación del Riesgo, Gestión del riesgo).</li> <li>○ Dominios de control (Política de seguridad, Aspectos organizativos, clasificación y control de activos, Seguridad ligada al personal, Seguridad física y del entorno, Gestión de comunicaciones y operaciones, Control de accesos, Desarrollo y mantenimiento de sistemas, Respuesta a incidentes, Gestión de la continuidad del negocio, Conformidad con la legislación).</li> <li>○ Objetivos de control (Política de seguridad, Aspectos organizativos, clasificación y control de activos, Seguridad ligada al personal, Seguridad física y del entorno, Gestión de comunicaciones y operaciones, Control de accesos, Desarrollo y mantenimiento de sistemas, Respuesta a incidentes, Gestión de la continuidad del negocio, Conformidad con la legislación)</li> <li>○ Esquema ISO 27001 (Política de seguridad, Aspectos organizativos, clasificación y control de activos, Seguridad ligada al personal, Seguridad física y del entorno, Gestión de comunicaciones y operaciones, Control de accesos, Desarrollo y mantenimiento de sistemas, Respuesta a incidentes, Gestión de la continuidad del negocio, Conformidad con la legislación)</li> </ul> </li> <li>• Certificación OSSTMM <ul style="list-style-type: none"> <li>○ Introducción, Mapa de seguridad, Seguridad Controles, Limitaciones y Test</li> <li>○ Formulas (Porosidad, Controles, Limitación y Seguridad actual).</li> </ul> </li> </ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Para cursar esta asignatura, se recomienda haber cursado previamente la asignatura F1.- Introducción a las auditorías de seguridad, así como la asignatura F2.- Metodologías.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: F3.- Certificaciones</b>  Carácter: Optativa  ECTS: 3  Unidad temporal: S1  Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				16		0%
Prácticas en el aula de informática						
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				30		0%
Trabajos				20		0%
Resolución de problemas						0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: G1.- El perito informático forense</b> Módulo al que pertenece: G.- Fundamentos para llevar a cabo peritajes informáticos Tipo: Obligatoria ECTS: 3 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE8, CE9 y CE10</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer las responsabilidades de la figura del perito informático y los escenarios de actuación de este tipo de profesionales.</li><li>• Conocer y aplicar una metodología sistemática a la hora de realizar un peritaje informático en un escenario real.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Introducción, objetivos, aspectos relevantes y ámbitos relevantes</li><li>• La figura del perito informático, funciones y atribuciones</li><li>• Perito informático de gestión y mediación tecnológica</li><li>• Metodologías de actuación.</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>Este módulo es complementario al resto de módulos de la certificación, nace con el objetivo de cubrir un sector, el del peritaje informático, que hoy en día está falto de profesionales. A lo largo del módulo, que comienza en esta asignatura, el alumno conocerá como aplicar las técnicas y conocimientos aprendidos en otros módulos para aplicarlos en este módulo de peritaje.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: G1.- El perito informático forense</b> Carácter: Obligatoria ECTS: 3 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>



ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				6		0%
Prácticas en el aula de informática				5		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				20		0%
Trabajos				20		0%
Resolución de problemas				15		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: G2.- La evidencia telemática, técnicas y herramientas</b> Módulo al que pertenece: G.- Fundamentos para llevar a cabo peritajes informáticos Tipo: Optativa ECTS: 3 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b> Básicas / Generales / Transversales: CB1, CB2, CB3, CB4, CB5 y CG1  Específicas: CE1, CE8, CE9 y CE10</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer las principales herramientas de un perito informático, así como el entorno de trabajo, es decir el Laboratorio Informático Forense.</li><li>• Utilizar las técnicas periciales adecuadamente para la extracción de evidencias que puedan ser pruebas utilizables en un contexto judicial.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• La evidencia telemática</li><li>• Preservación de la evidencia digital</li><li>• Como recuperar datos perdidos</li><li>• Pen-test, herramientas y programas forenses</li><li>• Cibercrimen, ciberataques, ciberamas, ciberdefensas</li><li>• Tecno vigilancia y las fuerzas de seguridad</li><li>• Laboratorio informático forense.</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b> El objetivo de esta asignatura es que al alumno aprenda a utilizar técnicas y herramientas para la extracción de evidencias y pruebas utilizables en un contexto judicial</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b> Asignatura 1: G2.- La evidencia telemática, técnicas y herramientas Carácter: Optativa ECTS: 3 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				2		0%
Sesión magistral				2		0%
Prácticas en el aula de informática				8		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				20		0%
Trabajos				18		0%
Resolución de problemas				20		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: G3.- El informe pericial</b> Módulo al que pertenece: G.- Fundamentos para llevar a cabo peritajes informáticos Tipo: Optativa ECTS: 3 Semestre: S2 Lenguas en las que se imparte: Español Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b></p> <p><b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1</p> <p><b>Específicas:</b> CE1, CE8, CE9 y CE10</p>
<p><b>RESULTADOS DE APRENDIZAJE PREVISTOS:</b></p> <ul style="list-style-type: none"><li>• Adquisición de las competencias básicas, generales y específicas detalladas anteriormente.</li><li>• Conocer los tipos de informes periciales, su estructura y el tipo de redacción jurídica requerida.</li><li>• Saber realizar un informe pericial a partir de un conjunto de evidencias.</li></ul>
<p><b>BREVE DESCRIPCIÓN DE CONTENIDOS:</b></p> <ul style="list-style-type: none"><li>• Redacción de un informe pericial</li><li>• Tipos de informe.</li><li>• El informe pericial (secciones, diligencia de identificación y análisis, conclusiones finales, diligencia de entrega).</li><li>• El protocolo de actuación.</li><li>• Código deontológico</li><li>• Referencia legislativa.</li></ul>
<p><b>OBSERVACIONES (Requisitos previos, coordinación. Otras)</b></p> <p>El objetivo de este módulo es que el alumno conozca las peculiaridades de un informe pericial en el campo de la informática, el código deontológico y las referencias legislativas.</p> <p>Para cursar esta asignatura es recomendable cursar también la asignatura G2.- La evidencia telemática, técnicas y herramientas.</p>
<p><b>ASIGNATURAS QUE COMPONEN LA MATERIA:</b></p> <p><b>Asignatura 1: G3.- El informe pericial</b> Carácter: Optativa ECTS: 3 Unidad temporal: S2 Lenguas en las que se imparte: Español</p>

ACTIVIDADES FORMATIVAS						
Actividad Formativa		Horas de dedicación presencial del estudiante		Horas de trabajo personal del estudiante.		Porcentaje de presencialidad
Actividades introductorias				4		0%
Sesión magistral				10		0%
Prácticas en el aula de informática				3		0%
Tutorías						
Actividades de seguimiento online				2		0%
Preparación de trabajos				32		0%
Trabajos				21		0%
Resolución de problemas				0		0%
Foros de discusión				3		0%
Total Horas	75	Total horas Presenciales	0	Total Horas Trabajo Autónomo	75	0%
SISTEMAS DE EVALUACION						
Prueba de evaluación				Ponderación máxima		Ponderación mínima
Evaluación continua, Participación online y/o presencial				50%		40%
Pruebas objetivas de tipo test				50%		40%
Pruebas prácticas				50%		20%

<p><b>MATERIA: TFM.- Trabajo fin de titulación</b>  Módulo al que pertenece: TFM  Tipo: TFM  ECTS: 9  Semestre: S2  Lenguas en las que se imparte: Español  Modalidad de enseñanza: online</p>
<p><b>COMPETENCIAS:</b>  <b>Básicas / Generales / Transversales:</b> CB1, CB2, CB3, CB4, CB5 y CG1  <b>Específica :</b> Capacidad para la creación y elaboración de proyectos de originales y pertinentes, con metodología apropiada y establecimiento de conclusiones relevantes en el ámbito de conocimiento de la Animación Digital</p>
<p><b>ACTIVADES FORMATIVAS:</b></p> <ul style="list-style-type: none"> <li>• Asegurar la tutela efectiva de los TFM.</li> <li>• Asegurar que los TFM se realicen en el tiempo establecido en la memoria de verificación de los títulos.</li> <li>• Reconocer la actividad docente de los profesores que los dirijan.</li> <li>• Potenciar la realización de TFM en instituciones externas y empresas.</li> <li>• Disponer de los medios necesarios para la realización de los TFM.</li> </ul>
<p><b>TAREAS DENTRO DEL TFM:</b></p> <ul style="list-style-type: none"> <li>• Elección del tema selección de tutor/a</li> <li>• Elaboración del proyecto para el tutor/a y aprobación</li> <li>• Acuerdo con el tutor para decidir la metodología aplicable</li> <li>• Búsqueda, lectura y selección de información</li> <li>• Consulta, recopilación y selección de datos, fuentes y documentos</li> <li>• Tutorías con el profesor/tutor</li> <li>• Desarrollo metodológico</li> <li>• Establecimiento de las conclusiones</li> <li>• Elaboración del trabajo</li> <li>• Creación de un discurso y soporte para la defensa.</li> </ul>
<p><b>EVALUACIÓN</b>  El trabajo fin de Máster podrá presentarse ante un tribunal para su defensa siempre que su tutor/a haya aprobado y calificado el trabajo /las especificaciones del trabajo en cuanto a formato le serán especificadas al alumno a través de la plataforma en el la que se desarrolla la formación. No podrá presentarse ante el tribunal o comisión juzgadora del TFM ningún trabajo que no haya alcanzado una calificación de 5 puntos.  La calificación final de cada TFM será la ponderada entre la nota del tutor/a y la del tribunal.</p> <ul style="list-style-type: none"> <li>• Calificación numérica (5-10) del tutor/a del trabajo: 60%. Es importante entender que el peso del TFM del alumno/a recae fundamentalmente sobre el tutor/a y, por ello, es quien mejor conoce la dedicación del alumno/a, la dificultad, el esfuerzo y el rendimiento. Por eso, su informe será de todo punto necesario.</li> <li>• Calificación numérica (5-10) del tribunal: 40%. En esta calificación se tendrá en cuenta la calidad del TFM a juicio de la comisión y su defensa oral.</li> </ul>
<p><b>PRESENTACIÓN Y DEFENSA DE LOS TFM</b>  La presentación del TFM consistirá en la exposición oral (10 minutos) donde el alumno presentará los objetivos, fuentes, metodología y conclusiones más destacables del trabajo realizado. El tribunal realizará cuantas cuestiones considere pertinentes. Por último, el alumno deberá responder a cada miembro del tribunal las preguntas u observaciones formuladas.</p> <p>Se valorará en la presentación de la memoria, la calidad y organización del trabajo, su originalidad y resultados, la capacidad comunicativa y la exposición del trabajo y su defensa.</p>
<p><b>CONSTITUCIÓN DE LOS TRIBUNALES DEL MÁSTER:</b>  El Tribunal calificador o Comisión juzgadora del TFM estará integrado por tres miembros que serán o bien profesores del Máster o bien profesionales expertos en la materia. Podrán constituirse varios Tribunales para la calificación de los TFM. En tal caso, la distribución de los estudiantes entre los distintos Tribunales será realizada por la Comisión Coordinadora del Máster.</p>

**MATERIA: PE.- Prácticas de empresa**

Módulo al que pertenece: PE Prácticas de empresa

Tipo: PE

ECTS: 6

Semestre: S2

Lenguas en las que se imparte: Español

Modalidad de enseñanza: online

**COMPETENCIAS:**

**Básicas / Generales / Transversales:** CB1, CB2, CB3, CB4, CB5 y CG1

**Específica :**

- Integrar conocimientos y enfrentarse a la complejidad de las responsabilidades sociales vinculadas al trabajo en una empresa.
- Aplicar un campo de estudio y el dominio de las habilidades relacionados con dicho campo.
- Comunicarse con sus colegas de trabajo y aprender a trabajar en grupo dentro de un entorno laboral.

**RESULTADOS DE APRENDIZAJE PREVISTOS:**

- Aplicar los conocimientos adquiridos en la universidad
- Adquirir nuevas competencias relacionadas con la profesión
- Enfrentarme a situaciones y problemas multidisciplinares
- Conocer los condicionantes del trabajo actual
- Ajustar las actitudes y comportamientos al mundo laboral.

**OBSERVACIONES (Requisitos previos, coordinación. Otras)**

Las prácticas pueden cubrir créditos de optativos necesarios para la obtención de la titulación.

La Empresa u Organismo en el que se desarrolle el módulo de prácticas de empresa designará un Tutor de Prácticas (tutor externo), que deberá ser un profesional de la plantilla de dicha Entidad. Este asignará las funciones a realizar por los alumnos durante el desarrollo de las prácticas, asistiéndoles en lo que fuere preciso y evaluando su aprovechamiento.

La comisión del título propio designará un Tutor de Prácticas interno que supervisará que las líneas de trabajo a desarrollar por los estudiantes queden enmarcadas dentro de la oferta incluida en el plan de estudios de la titulación y les atenderá en su formación

La asignación de las plazas de prácticas se realizará en un función de las preferencias del alumno y las necesidades de la empresa que lo acoge, valoración que realizará el Director del Título. El expediente académico del alumnos dentro de la titulación servirá como varemos en caso de conflicto en la asignación de una plaza.

## 6. PERSONAL ACADÉMICO

El profesorado encargado de impartir la docencia del Título Propio de Máster en Seguridad está vinculado tanto al ámbito académico como al investigador y empresarial.

Este Título Propio incorpora profesores de los siguientes departamentos de la USAL:

- Departamento de Informática y Automática
- Departamento de Derecho Privado

Así mismo, dentro del mundo académico también se cuenta con docentes de la Oficina de Transferencia de Resultados de Investigación (OTRI) de la Universidad de Salamanca y del Depto. de Informática de la Universidad de Valladolid. A nivel internacional se cuenta con el centro de investigación CNRS (<http://www.cnrs.fr/>) de Francia.

En todo caso se trata de profesores con dilatada experiencia y de investigadores con experiencia práctica y actualizada en las materias que imparten. El listado de miembros del cuerpo docente pertenecientes a estos departamentos se detalla en la Tabla 6.1.

También se cuenta con profesorado no vinculado directamente a la USAL, ligado a empresas con unidades de negocio centradas en la seguridad informática:

- INDRA (<http://www.indracompany.com/>)
- Oesía (<http://www.oesia.com/>)
- Banco Popular (<http://www.bancopopular.es/>)
- Flag Solutions (<http://www.flagsolutions.net/>)

### Otros recursos humanos disponibles:

El desarrollo de un curso de este tipo requiere la implicación de personal técnico y administrativo cualificado. En este sentido se dispone de la infraestructura del grupo de Investigación de Bioinformática, Sistemas Inteligentes y Tecnología Educativa de la Universidad de Salamanca.

Este Grupo, que está compuesto por unos 40 investigadores pone a disposición de este título propio su infraestructura administrativa (2 técnicos) un equipo de 3 técnicos de laboratorio para la preparación de prácticas, un técnico para la gestión del campus virtual y los sistemas de formación y el resto de su personal de mantenimiento de sistemas informáticos, formado por 4 ingenieros.

También se cuenta con la colaboración del Personal de la Biblioteca de área de Ciencias Abraham Zanut, del profesionales destinados en las Conserjerías de la Facultad de Ciencias para que asistan y asesoren a estudiantes y profesores en el marco de las competencias que tienen asignadas.

El número de créditos totales contando las asignaturas obligatorias y optativas del Máster es 54 créditos. El reparto de la dedicación docente se realiza de la siguiente forma entre profesorado asociado y no asociado a la Universidad de Salamanca:

- Personal Docente e Investigador de la USAL : 24 créditos
- Profesorado no perteneciente al PDI de la USAL : 30 créditos

En este reparto de créditos no se incluyen los créditos del Trabajo Fin de Máster, ni tampoco, de las Prácticas de Empresa, ya que la carga docente de estos módulos depende del número de estudiantes matriculados. La tutorización de estas asignaturas se realizará por el Personal Docente e Investigador de la USAL, que se profesores del presente Máster.