

Escuela de Doctorado y Estudios de Posgrado

Máster Universitario en Ciberseguridad e Inteligencia de Datos

GUÍA DOCENTE DE LA ASIGNATURA (ESCENARIO 1):

Trabajo Fin de Máster (2021 - 2022)

1. Datos descriptivos de la asignatura

Asignatura: Trabajo Fin de Máster	Código: 835871206
- Centro: Escuela de Doctorado y Estudios de Postgrado - Lugar de impartición: - - Titulación: Máster Universitario en Ciberseguridad e Inteligencia de Datos - Plan de Estudios: 2018 (Publicado en 2018-09-19) - Rama de conocimiento: Ingeniería y Arquitectura - Itinerario / Intensificación: - Departamento/s: Ingeniería Informática y de Sistemas Matemáticas, Estadística e Investigación Operativa Física Ingeniería Industrial - Área/s de conocimiento: Arquitectura y Tecnología de Computadores Ciencia de la Computación e Inteligencia Artificial Estadística e Investigación Operativa Física Aplicada Ingeniería Telemática Lenguajes y Sistemas Informáticos - Curso: 1 - Carácter: - Duración: Segundo cuatrimestre - Créditos ECTS: 6,0 - Modalidad de impartición: Semipresencial - Horario: Enlace al horario - Dirección web de la asignatura: http://www.campusvirtual.ull.es - Idioma: Castellano e Inglés (0,30 ECTS en Inglés)	

2. Requisitos para cursar la asignatura

Contacto

- Teléfono 1: **922 31 8176**
- Teléfono 2:
- Correo electrónico: **pcaballe@ull.es**
- Correo alternativo:
- Web: **<http://www.campusvirtual.ull.es>**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	09:00	12:00	Edificio de Física y Matemáticas - AN.2B	85
Todo el cuatrimestre		Miércoles	11:30	14:30	Edificio de Física y Matemáticas - AN.2B	85

Observaciones: Este horario es orientativo. Prevalecerá el que se ponga en las aulas virtuales de las asignaturas.

Tutorías segundo cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	09:00	12:00	Edificio de Física y Matemáticas - AN.2B	85
Todo el cuatrimestre		M				

- CG1** - Ser capaces de aplicar los conocimientos adquiridos para resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con seguridad informática o inteligencia de datos
- CG2** - Integrar conocimientos para formular juicios a partir de información concreta, y a la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de esos conocimientos y juicios en materia de asesoramiento en seguridad informática
- CG3** - Mantener una actitud de permanente actualización, que les permita estudiar de manera autónoma mediante formación continua en su futuro desempeño profesional como expertos en seguridad informática e inteligencia de datos
- CG4** - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática, e implementarlos y desarrollarlos mediante los métodos y procesos adecuados
- CG5** - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática e inteligencia de datos, en el seno de entidades de TIC
- CG6** - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la continua revisión del proceso que conlleva la seguridad informática y la inteligencia de datos
- CG7** - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes
- CG8** - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente
- CG9** - Manejar adecuadamente información relativa al sector de la seguridad informática atendiendo a la legislación vigente, estándares, certificaciones, documentos internos, etc.
- CG10** - Diseñar, evaluar y monitorizar un proyecto de inteligencia de datos

Básicas

- CE6** - Capacidad de detección y evaluación de vulnerabilidades que afectan a los sistemas informáticos y de aplicación de técnicas y herramientas de análisis forense
- CE7** - Conocer las diferentes técnicas de análisis y explotación de datos y valorar su correcta aplicación en la extracción de información relevante
- CE8** - Saber elaborar documentación y manuales de formación para usuarios sobre las Políticas de Seguridad de la Información establecidas en la compañía
- CE9** - Ser capaz de obtener, procesar y almacenar datos de diferentes fuentes y en diversos formatos
- CE10** - Ser capaz de visualizar los datos y las relaciones relevantes existentes entre ellos
- CE11** - Ser capaz de comunicar efectivamente las conclusiones alcanzadas tras analizar un conjunto de datos
- CE12** - Conocer los métodos y procedimientos par la preparación de conjuntos de datos para aplicar técnicas de análisis de forma adecuada

6. Contenidos de la asignatura

Contenidos teóricos y prácticos de la asignatura

El Trabajo Fin de Máster (TFM) supone la realización, presentación y defensa, de un ejercicio original realizado individualmente ante un tribunal, consistente en un proyecto integral de Ciberseguridad e Inteligencia de Datos, en el que se sinteticen las competencias adquiridas en las enseñanzas del máster.

El TFM será realizado bajo la supervisión de uno/a o dos tutores/as, de los/as que al menos uno/a pertenecerá a la plantilla docente de la Universidad de La Laguna que imparta docencia en el título correspondiente y que actuará como tutor/a principal si el/la segundo/a tutor/a es personal externo a la Universidad de La Laguna.

La comisión académica del máster aprobará un listado con

La metodología docente en el trabajo fin de máster contempla, por una parte, las tutorías de trabajo fin de máster, que son horas presenciales a desarrollar entre el alumnado y el/la tutor/a académico/a para realizar el seguimiento de las tareas que conforman el trabajo fin de máster; y por otra parte, el desarrollo del trabajo fin de máster, que será una actividad consistente en la concepción, planificación, gestión y desarrollo del trabajo fin de máster por el alumnado.

Actividades formativas en créditos ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante

Actividades formativas	Horas presenciales	Horas de trabajo autónomo	Total horas	Relación con competencias
Realización de exámenes	1,00	0,00	1,0	[CB9], [CG10], [CG9], [CG8], [CG5]
Asistencia a tutorías	29,50	0,00	29,5	[CB8], [CG10], [CG9]
Informes, trabajos y proyectos	29,50	0,00	29,5	[CB7], [CG10], [CG9], [CG7], [CG6], [CG4], [CG1]
Desarrollo del Trabajo Fin de Máster	0,00	90,00	90,0	[CE12], [CE11], [CE10], [CE9], [CE8], [CE7], [CE6], [CE5], [CE4], [CE3], [CE2], [CE1], [CB10], [CB6], [CG10], [CG9], [CG6], [CG3], [CG2]
Total horas	60,00	90,00	150,00	

El resto de recursos se centralizan de forma electrónica en el Aula Virtual de la asignatura, alojada en el Campus Virtual Institucional de la ULL

9. Sistema de evaluación y calificación

Descripción

El TFM concluirá obligatoriamente con la presentación y defensa del mismo ante un tribunal, que será necesariamente pública.

La evaluación del Trabajo Fin de Máster se basará en la memoria y seguimiento del trabajo realizado (70%) y en la presentación y defensa del mismo ante un tribunal (30%).

La memoria del TFM deberá seguir las pautas de formato y estructura especificadas por la Comisión Académica del Máster, y será presentada en formato digital a través de la sede electrónica de la ULL, quedando accesible de forma pública.

En la evaluación del seguimiento del TFM se contemplarán como hitos, parte de las prácticas de diferentes asignaturas.

La Comisión Académica del máster propondrá el tribunal o tribunales que habrán de evaluar los TFM, y hará público el calendario completo de defensas al menos con diez días naturales de antelación respecto de la fecha señalada para la correspondiente convocatoria, donde se indique para cada alumno/a el lugar, día y hora fijados para la defensa de su trabajo. Los tribunales estarán formados por profesorado que imparta docencia en esa titulación, designando en cada uno a un/a presidente/a y un/a secretario/a.

Presentación y defensa	[CE12], [CE11], [CE10], [CE9], [CE8], [CE7], [CE6], [CE5], [CE4], [CE3], [CE2], [CE1], [CB10], [CB9], [CB8], [CB7], [CB6], [CG10], [CG9], [CG8], [CG7], [CG6], [CG5], [CG4], [CG3], [CG2], [CG1]	- Calidad del trabajo realizado. - Defensa oral del Trabajo de Fin de Máster.	30,00 %
------------------------	---	--	---------

10. Resultados de Aprendizaje

El alumnado será capaz de desarrollar un trabajo original consistente en un proyecto integral de Ciberseguridad e Inteligencia de Datos en el que se sintetizarán las competencias adquiridas en el máster.

11. Cronograma / calendario de la asignatura

Descripción

Esta asignatura se cursará en el segundo cuatrimestre, dentro del cuarto bimestre.
La asignación de TFM se realizará en el primer bimestre con objeto de que en su evaluación se contemplen como hitos, parte de las prácticas de diferentes asignaturas.

Segundo cuatrimestre					
Semana	Temas	Actividades de enseñanza aprendizaje	Horas de trabajo presencial</		

Semana 12:	-	Desarrollo del TFM. Preparación de informes u otros trabajos. Asistencia a reuniones de seguimiento del TFM.	7.00	11.00	18.00
Semana 13:	-	Desarrollo del TFM. Preparación de informes u otros trabajos. Asistencia a reuniones de seguimiento del TFM.	7.00	11.00	18.00
Semana 14:	-	Desarrollo del TFM. Preparación de informes u otros trabajos. Asistencia a reuniones de seguimiento del TFM.	7.00	11.00	18.00
Semana 15:	-	Desarrollo del TFM. Preparación de informes u otros trabajos. Asistencia a reuniones de seguimiento del TFM. Preparación y realización de la defensa presencial del TFM.	7.00	11.00	18.00
Semana 16 a 18:	-	Preparación y realización de la defensa presencial del TFM.	7.00	7.00	14.00
Total			60.00	90.00	150.00