Escuela de Doctorado
y Estudios de Posgrado
Universidad de La Laguna

Escuela de Doctorado y Estudios de Posgrado

Máster Universitario en Ciberseguridad e Inteligencia de Datos

GUÍA DOCENTE DE LA ASIGNATURA (ESCENARIO 0):

Programación de Código Seguro
(2021 - 2022)

1. Datos descriptivos de la asignatura

Asignatura: Programación de Código Seguro	Código: 835871202

- 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
- Área/s de conocimiento:
  Ciencia de la Computación e Inteligencia Artificial
  Lenguajes y Sistemas Informáticos
- Curso: **1**
- Carácter:
- Duración: **Segundo cuatrimestre**
- Créditos ECTS: **3,0**
- Modalidad de impartición: **Semipresencial**
- Horario: **Enlace al horario**
- Dirección web de la asignatura: **http://www.campusvirtual.ull.es**
- Idioma: **Castellano e Inglés (0,15 ECTS en Inglés**

2. Requisitos para cursar la asignatura

3. Profesorado que imparte la asignatura

Profesor/a Coordinador/a: LUZ MARINA MORENO DE ANTONIO

- Grupo:

General
- Nombre: **LUZ MARINA**
- Apellido: **MORENO DE ANTONIO**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Lenguajes y Sistemas Informáticos**

Contacto
- Teléfono 1: **922319908**
- Teléfono 2:
- Correo electrónico: **lmmoreno@ull.edu.es**
- Correo alternativo:
- Web: **http://www.campusvirtual.ull.es**

Tutorías primer cuatrimestre:						
Desde	**Hasta**	**Día**	**Hora inicial**	**Hora final**	**Localización**	**Despacho**
27-09-2021	21-01-2022	Martes	10:30	13:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031
27-12-2021	21-01-2022	Miércoles	16:30	19:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031
24-01-2022	09-02-2022	Martes	10:30	13:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031
24-01-2022	09-02-2022	Miércoles	10:30	13:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031
Observaciones: El horario y lugar de tutorías es orientativo y prevalecerá la información que aparezca en el aula virtual de la asignatura. Se establecerá un sistema de cita previa para las tutorías. La reserva de una cita deberá realizarse al menos una hora antes del inicio de la tutoría.						
Tutorías segundo cuatrimestre:						
Desde	**Hasta**	**Día**	**Hora inicial**	**Hora final**	**Localización**	**Despacho**
10-02-2022	27-05-2022	Lunes	16:30	19:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031

10-02-2022	27-05-2022	Miércoles	16:30	19:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031
30-05-2022	23-09-2022	Martes	10:30	13:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031
30-05-2022	23-09-2022	Miércoles	10:30	13:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.031

Observaciones: El horario y lugar de tutorías es orientativo y prevalecerá la información que aparezca en el aula virtual de la asignatura. Se establecerá un sistema de cita previa para las tutorías. La reserva de una cita deberá realizarse al menos una hora antes del inicio de la tutoría.

Profesor/a: **CRISTOFER JUAN EXPOSITO IZQUIERDO**

- Grupo:

General
- Nombre: **CRISTOFER JUAN**
- Apellido: **EXPOSITO IZQUIERDO**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto
- Teléfono 1: **Extensión 9191**
- Teléfono 2:
- Correo electrónico: **cexposit@ull.es**
- Correo alternativo: **cexposit@ull.edu.es**
- Web: **http://www.campusvirtual.ull.es**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Martes	08:30	11:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	DSIC 3-4

Todo el cuatrimestre		Miércoles	08:30	11:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	DSIC 3-4
Observaciones:						
Tutorías segundo cuatrimestre:						
Desde	**Hasta**	**Día**	**Hora inicial**	**Hora final**	**Localización**	**Despacho**
Todo el cuatrimestre		Lunes	15:00	18:00	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	DSIC 3-4
Todo el cuatrimestre		Martes	15:00	18:00	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	DSIC 3-4
Observaciones:						

4. Contextualización de la asignatura en el plan de estudio

Bloque formativo al que pertenece la asignatura:
Perfil profesional:

5. Competencias

Generales

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
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
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

Básicas

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de

estudio
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Específicas

CE4 - Experiencia en el diseño de aplicaciones, incorporando el criterio de seguridad dentro del propio proceso de desarrollo, y en la aplicación de técnicas para auditar y mejorar la seguridad de las aplicaciones

6. Contenidos de la asignatura

Contenidos teóricos y prácticos de la asignatura

Profesorado: Cristofer Juan Expósito Izquierdo

- Vulnerabilidades de los programas informáticos. Exploits.
- Herramientas: Depuradores y compiladores.
- Ofuscación de código. Inyección de Código. Violaciones de Memoria.

Profesorado: Luz Marina Moreno de Antonio

- Diseño y construcción de aplicaciones seguras.
- Ingeniería del software de sistemas seguros.
- Seguridad en desarrollo web.

Actividades a desarrollar en otro idioma

En esta asignatura se impartirán 1,5 horas de clases en inglés. Además se trabajará preferentemente sobre bibliografía en inglés y el alumnado deberá ser capaz de extraer la información necesaria para seguir las asignaturas a partir de dicha documentación, junto con los recursos aportados por el profesorado.

7. Metodología y volumen de trabajo del estudiante

Descripción

La metodología docente de las clases teóricas consistirá en sesiones en las que el profesorado explicará los conceptos fundamentales de cada tema que deben ser asimilados por el alumnado, bien presencialmente, o no presencialmente mediante retransmisión online.
La metodología docente de las clases prácticas consistirá en sesiones supervisadas en grupos reducidos en el laboratorio en las que se realizarán diversas prácticas informáticas de dificultad creciente aplicando los conceptos expuestos en las clases de teoría. Además, el alumnado aprenderá a usar diversas herramientas, en entornos reales o de simulación, así como metodologías relacionadas con el contexto de la materia.
La metodología docente de los informes consistirá en el desarrollo por parte del alumnado de su capacidad para la aplicación

de los conocimientos adquiridos y la resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.
Se plantea una metodología docente para los seminarios que consistirá en sesiones donde se llevará a cabo una explicación más detallada de determinados aspectos concretos de algunos temas teóricos o prácticos especialmente relevantes.
Las tutorías individuales ayudarán a reforzar los diferentes aspectos de la materia y ayudarán al alumnado en la comprensión de la teoría y la realización de las prácticas.

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
Clases teóricas	5,00	5,00	10,0	[CE4], [CG6], [CG4]
Clases prácticas (aula / sala de demostraciones / prácticas laboratorio)	8,00	8,00	16,0	[CE4], [CB10], [CG4]
Realización de seminarios u otras actividades complementarias	1,00	1,00	2,0	[CE4], [CG6], [CG4]
Estudio/preparación de clases teóricas	0,00	10,00	10,0	[CB10], [CG6], [CG3]
Estudio/preparación de clases prácticas	0,00	6,00	6,0	[CB10], [CG6], [CG3]
Realización de exámenes	1,00	0,00	1,0	[CG1]
Asistencia a tutorías	0,00	6,00	6,0	[CG3]
Informes, trabajos y proyectos	0,00	24,00	24,0	[CE4], [CB7], [CG6], [CG4], [CG3], [CG1]
Total horas	15,00	60,00	75,00	
		Total ECTS	3,00	

8. Bibliografía / Recursos

Bibliografía Básica

Taylor, Art; Brian Buege; Randy Layman (2006).
Hacking Exposed J2EE & Java
. McGraw-Hill Primis. p. 426.
ISBN

0-390-59975-1
.

Viega, John; Gary McGraw (2001).
Building Secure Software: How to Avoid Security Problems the Right Way
. MAddison-Wesley Professional. p. 528.
ISBN

978-0201721522
.

Bibliografía Complementaria

Desarrollo de aplicaciones Android seguras. Miguel Moreno. ISBN: 978-84-616-2903-9.
http://absysnetweb.bbtk.ull.es/cgi-bin/abnetopac?TITN=551919

Otros Recursos

https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

9. Sistema de evaluación y calificación

Descripción

La Evaluación de la asignatura se rige por el Reglamento de Evaluación y Calificación de la Universidad de La Laguna (BOC de 19 de enero de 2016), o el que la Universidad tenga vigente, además de por lo establecido en la Memoria de Verificación inicial o posteriores modificaciones.

Se aplica evaluación continua a todo el alumnado matriculado en la asignatura, realizando diversas actividades de aprendizaje. Estas actividades se agrupan en:
- Teoría: Se evaluará mediante pruebas escritas. La Calificación de Teoría (CT) se corresponde con el 40% de la calificación final.
- Prácticas: Se evaluará mediante la realización de memorias de prácticas y proyectos. La Calificación de Prácticas (CP) se corresponde con el 60% de la calificación final.

Ambas calificaciones serán valores entre 0 y 10, de forma que la Calificación Final (CF) se obtendrá mediante la fórmula: CF= 0,40*CT + 0,60*CP, si y solo si CT>=5 y CP>=5. En otro caso, CF= min(CT, CP).

El alumnado que no supere la evaluación continua podrá realizar en las diferentes convocatorias pruebas de evaluación alternativa destinadas exclusivamente a evaluar las mismas competencias y resultados de aprendizaje de la asignatura.

Estrategia Evaluativa

Tipo de prueba	Competencias	Criterios	Ponderación
Pruebas objetivas	[CE4], [CB10], [CB7], [CG6], [CG4], [CG3], [CG1]	• Adecuación a lo solicitado • Concreción en la redacción • Nivel de conocimientos adquiridos • Nivel de aplicabilidad	40,00 %
Trabajos y proyectos	[CE4], [CB10], [CB7], [CG6], [CG4], [CG3], [CG1]	• Regularidad en la entrega de ejercicios por tema • Adecuación a lo solicitado • Asistencia activa e interés demostrado • Nivel de conocimientos adquiridos	40,00 %
Informes memorias de prácticas	[CE4], [CB10], [CB7], [CG6], [CG4], [CG3], [CG1]	• Adecuación a lo solicitado • Asistencia Activa e interés demostrado • Nivel de conocimientos adquiridos	20,00 %

10. Resultados de Aprendizaje

Al finalizar la asignatura el alumnado debe: entender dónde se producen normalmente las vulnerabilidades de los programas informáticos que son fácilmente explotadas por los hackers, y conocer diversas técnicas de programación para diseñar e implementar aplicaciones sin vulnerabilidades.

11. Cronograma / calendario de la asignatura

Descripción

Debido al carácter semipresencial del máster, está previsto que las clases presenciales se desarrollen de la forma siguiente: el alumnado tendrá 3 horas diarias las semanas 1 a 5 y 8 a 12 del primer cuatrimestre, y 3 o 4 horas diarias las semanas 1 a 5 del segundo cuatrimestre.
Todas las asignaturas se desarrollarán en bimestres, y concretamente esta asignatura se impartirá en el bimestre 3 (segundo cuatrimestre). El cronograma que se presenta es a título estimativo, de modo que el profesorado podrá modificar dicha planificación temporal si así lo demanda el desarrollo de la asignatura.

Primer cuatrimestre					
Semana	Temas	Actividades de enseñanza aprendizaje	Horas de trabajo presencial	Horas de trabajo autónomo	Total
Semana 1:			0.00	0.00	0.00
		Total	0.00	0.00	0.00

Segundo cuatrimestre					
Semana	Temas	Actividades de enseñanza aprendizaje	Horas de trabajo presencial	Horas de trabajo autónomo	Total
Semana 1:	Vulnerabilidades de los programas informáticos. Exploits. Herramientas: Depuradores y compiladores.	Clases teóricas y prácticas y seminarios presenciales.	2.00	2.00	4.00
Semana 2:	Herramientas: Depuradores y compiladores. Ofuscación de código. Inyección de Código. Violaciones de Memoria.	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 3:	Ofuscación de código. Inyección de Código. Violaciones de Memoria. Diseño y construcción de aplicaciones seguras.	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 4:	Diseño y construcción de aplicaciones seguras. Ingeniería del software de sistemas seguros.	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 5:	Ingeniería del software de sistemas seguros. Seguridad en desarrollo web.	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 6:	Vulnerabilidades de los programas informáticos. Exploits. Herramientas: Depuradores y compiladores.	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00

Semana 7:	■■■■■■Ofuscación de código. Inyección de Código. Violaciones de Memoria. Diseño y construcción de aplicaciones seguras.	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00
Semana 8:	Ingeniería del software de sistemas seguros. Seguridad en desarrollo web.	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00
Semana 16 a 18:	Evaluación	Evaluación del alumnado	1.00	0.00	1.00
		Total	15.00	60.00	75.00