

17-18

MÁSTER UNIVERSITARIO EN
INGENIERÍA INFORMÁTICA

GUÍA DE ESTUDIO PÚBLICA



DESARROLLO DE SOFTWARE SEGURO (MÁSTER EN INGENIERÍA INFORMÁTICA)

CÓDIGO 31106205



Ámbito: GUJ - La autenticidad, validez e integridad de este documento puede ser verificada mediante el "Código Seguro de Verificación (CSV)" en la dirección <https://sede.uned.es/valida/>



D234FEBEAD56BD6B9683A38EE37093D

ÍNDICE

PRESENTACIÓN Y CONTEXTUALIZACIÓN	
REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA	
EQUIPO DOCENTE	
HORARIO DE ATENCIÓN AL ESTUDIANTE	
COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE	
RESULTADOS DE APRENDIZAJE	
CONTENIDOS	
METODOLOGÍA	
SISTEMA DE EVALUACIÓN	
BIBLIOGRAFÍA BÁSICA	
BIBLIOGRAFÍA COMPLEMENTARIA	
RECURSOS DE APOYO Y WEBGRAFÍA	



Nombre de la asignatura	DESARROLLO DE SOFTWARE SEGURO (MÁSTER EN INGENIERÍA INFORMÁTICA)
Código	31106205
Curso académico	2017/2018
Títulos en que se imparte	MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA
Tipo	CONTENIDOS
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Lamentablemente los denominados “ciberataques” son noticia frecuente en los medios de comunicación. Según los datos publicados por el CERT (Computer Emergency Response Team) las vulnerabilidades de los sistemas informáticos reportadas cada año crecen y aumentan su grado de sofisticación.

En este curso se presentan métodos rigurosos, técnicas y herramientas para desarrollar e implantar software seguro. Los métodos incluyen el análisis de código para detectar las vulnerabilidades habituales, la revisión de código fuente mediante herramientas de análisis estático y buenas prácticas para desarrollar código seguro en lenguajes concretos de programación.

Los métodos y herramientas que se estudian sirven para la realización de pruebas, verificación y validación de software y sistemas, comprobando que se cumplen los requisitos funcionales y de seguridad. Con todos ellos, se aprende a validar y verificar el aseguramiento de la seguridad así como a establecer la diferencia entre vulnerabilidades y errores de programación. Las técnicas de test incluyen las pruebas de caja blanca, caja negra, pruebas contra ataques, amenazas y penetración, pruebas de resiliencia, etc.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

La formación previa que deberían tener los alumnos para el adecuado seguimiento de esta asignatura son los propios de ingreso al posgrado, haciendo especial recomendación en conocimientos de ingeniería de software y lenguajes de programación.

Es muy recomendable que se haya cursado la asignatura "Fundamentos de Programación" para facilitar la comprensión de los ejemplos de la bibliografía escritos en lenguaje C. Se recomienda que el alumno tenga preferiblemente alguna experiencia previa de programación con C++ para seguir los ejemplos de la bibliografía. Los conocimientos básicos de programación orientada a objetos se pueden obtener de la asignatura de Programación Orientada a Objetos perteneciente a la materia Fundamentos de la Programación.

Además es necesario dominar el inglés técnico (leer y escribir) para manejar con facilidad las fuentes bibliográficas.



EQUIPO DOCENTE

Nombre y Apellidos
Correo Electrónico
Teléfono
Facultad
Departamento

DAVID JOSE FERNANDEZ AMOROS
david@issi.uned.es
91398-8241
ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
ING.DE SOFTWARE Y SISTEMAS INFORMÁTICOS

Nombre y Apellidos
Correo Electrónico
Teléfono
Facultad
Departamento

JOSE ANTONIO CERRADA SOMOLINOS
jcerrada@issi.uned.es
91398-6478
ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
ING.DE SOFTWARE Y SISTEMAS INFORMÁTICOS

HORARIO DE ATENCIÓN AL ESTUDIANTE

La tutorización de los alumnos se llevará a cabo fundamentalmente a través de la plataforma aLF. Además se puede utilizar el correo electrónico y las consultas telefónicas:

Profesor: *David Fernández Amorós*

Horario: Jueves de 16:00 a 20:00

david@issi.uned.es,

Teléfono: 91 398 8241

Profesor: *José Antonio Cerrada*

Horario: Jueves de 16:00 a 20:00

jcerrada@issi.uned.es,

Teléfono: 91 398 6478

También es posible una asistencia personalizada (preferentemente previo aviso) en los días y horas de tutorización en la siguiente dirección:

Dpto. de Ingeniería de Software y Sistemas Informáticos

ETSI Informática, UNED

C/ Juan del Rosal, 16

28040 MADRID

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

RESULTADOS DE APRENDIZAJE

La asignatura está enfocada al desarrollo y mantenimiento de software seguro y sin vulnerabilidades. Por tanto, los resultados de aprendizaje que se espera que el estudiante pueda alcanzar son:

- Identificar las principales causas de vulnerabilidad conocidas y desarrollar el código seguro que las evite.
- Conocer y saber aplicar un conjunto de métodos, técnicas y herramientas que permitan probar que el software desarrollado cumple los requisitos de funcionalidad y seguridad.



- Aplicar métodos para verificar formalmente la corrección de componentes de software crítico seguro.
- Realizar, junto con las pruebas tradicionales, otras adicionales específicas de seguridad.
- Usar modelos de penetración, patrones de ataque, de abuso o mal uso del sistema en la fase de pruebas.
- Conocer los procedimientos y programas de mantenimiento de software para que continúe cumpliendo con los requisitos de funcionalidad y seguridad.

CONTENIDOS

METODOLOGÍA

La docencia de esta asignatura se impartirá a distancia, siguiendo el modelo educativo propio de la UNED. El principal instrumento docente será la plataforma aLF en la que se habilitarán diversos foros para canalizar las consultas y comentarios.

Las actividades a realizar por parte del alumno se desglosan de la siguiente manera:

Actividades formativas	Horas
Estudio de contenidos	60
Tutorías	10
Actividades en la plataforma virtual	5
Trabajos individuales	30
Trabajos en equipo	15
Prácticas informáticas	30
Elaboración de informes	0
Resolución de casos	0

Además, el estudiante podrá realizar consultas al equipo docente a través del correo, teléfono y presencialmente en los horarios establecidos para estas actividades. Ver apartado de **Tutorización** en esta guía docente.

SISTEMA DE EVALUACIÓN



BIBLIOGRAFÍA BÁSICA

ISBN(13):9780321822130

Título:SECURE CODING IN C AND C++ (Second Edition)

Autor/es:Robert C. Seacord ;

Editorial:ADDISON WESLEY

ISBN(13):9781439826966

Título:SECURE AND RESILIENT SOFTWARE DEVELOPMENT

Autor/es:Mark S. Merkow And Lakshmikanth Raghavan ;

Editorial:CRC Press

Los dos libros están accesibles desde el portal de la UNED. Hay que autenticarse, y a partir de ahí.

- El libro de Seacord está aquí: (enlace). En este primer libro se estudian los aspectos generales relativos a todo el ciclo de vida del desarrollo de software seguro y sus particularidades.
- El libro de Merkow está aquí: (enlace). Este segundo libro está dedicado específicamente a estudiar las vulnerabilidades y las técnicas de programación segura en el lenguaje C y C++.

Hay un artículo que forma parte de la bibliografía recomendada:

- Tsipenyuk, Katrina; Chess, Brian & McGraw, Gary. ***Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors***. IEEE Security & Privacy, 2005

Este artículo se utiliza para clasificar los ciberataques y está disponible en la plataforma aLF de la asignatura.

BIBLIOGRAFÍA COMPLEMENTARIA

Aunque no se consideran necesarios para el estudio de la asignatura, los libros y documentos de esta bibliografía complementaria pueden ser muy interesantes para un estudio en mayor profundidad de la asignatura. La relación de documentos se incluye en la parte 2 de esta guía de la asignatura.

RECURSOS DE APOYO Y WEBGRAFÍA

Los alumnos tendrán a su disposición los siguientes recursos de apoyo al estudio:

- Guía de la asignatura: Incluye el plan de trabajo y orientaciones para su desarrollo. Esta guía será accesible desde el curso virtual.
- Curso virtual: A través de esta plataforma los alumnos pueden consultar información de la asignatura, acceder a material complementario, enunciados de ejercicios resueltos para que el alumno pueda autoevaluar sus conocimientos, realizar consultas al equipo docente y/o tutores a través de los foros correspondientes e intercambiar información con el resto de compañeros.



- Tutorías. En el Centro Asociado al que pertenezca el estudiante, éste deberá consultar si existe la posibilidad de disponer de una tutoría presencial con un tutor/a que le atienda presencialmente.
- Biblioteca: el acceso a las bibliotecas de los Centros Asociados y de la Sede Central permitirán al estudiante encontrar la bibliografía que podrá serle de utilidad durante el proceso de aprendizaje. De particular interés es el acceso electrónico a la colección de Safari Books Online a la que tienen acceso los estudiantes de la UNED.

Se ofrecerán las herramientas necesarias para que, tanto el equipo docente como el alumnado, encuentren la manera de compaginar el trabajo individual y el aprendizaje cooperativo (Skype, Moodle, Alf, etc.) si este se considerará necesario. Además de ello se podrá contactar con el equipo docente por teléfono y correo electrónico.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no hayan sido sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.

