



**SEGURIDAD
GUÍA DOCENTE CURSO 2018-19**

Titulación:	Grado en Ingeniería Informática			801G
Asignatura:	Seguridad			450
Materia:	Ingeniería del software y sistemas de información			
Módulo:	Ingeniería del software y sistemas de información			
Modalidad de enseñanza de la titulación:	Presencial	Carácter:	Obligatoria	
Curso:	4	Créditos ECTS:	6,00	Duración: Semestral
Horas presenciales:	60,00		Horas estimadas de trabajo autónomo:	90,00
Idiomas en que se imparte la asignatura:	Español			
Idiomas del material de lectura o audiovisual:	Inglés, Español			

DEPARTAMENTOS RESPONSABLES DE LA DOCENCIA

MATEMÁTICAS Y COMPUTACIÓN				R111
Dirección:	C/ Madre de Dios, 53		Código postal:	26006
Localidad:	Logroño	Provincia:	La Rioja	
Teléfono:	941299452	Fax:	941299460	Correo electrónico: dpto.dmc@unirioja.es

PROFESORADO PREVISTO

Profesor:	Rodríguez Priego, Emilio	Responsable de la asignatura
Teléfono:		Correo electrónico: emilio.rodriguez@unirioja.es
Despacho:	Edificio:	Tutorías: Consultar

DESCRIPCIÓN DE LOS CONTENIDOS

- Introducción: definiciones y principios de seguridad
- Seguridad física. Copias de seguridad
- Aspectos organizativos, sociales y legales
- Criptografía clásica y moderna
- Certificados digitales. Firma digital.
- Seguridad en las comunicaciones. Protocolos seguros
- Seguridad en redes. Sistemas de detección y prevención.
- Seguridad en sistemas operativos. Malware
- Técnicas de defensa. Hacking ético y análisis forense
- Seguridad en la programación. Protección del software
- Desarrollo de aplicaciones web seguras
- Planificación y gestión de la seguridad. SGSI. Análisis de riesgos

REQUISITOS PREVIOS DE CONOCIMIENTOS Y COMPETENCIAS PARA PODER CURSAR CON ÉXITO LA ASIGNATURA

Recomendados para poder superar la asignatura.

Conocimientos de redes, de sistemas distribuidos y de aplicaciones web

Asignaturas que proporcionan los conocimientos y competencias:

- Programación de aplicaciones web
- Redes de computadores
- Sistemas distribuidos

CONTEXTO

COMPETENCIAS

Competencias generales

CG1-Estar capacitado para analizar, razonar y evaluar de modo crítico, lógico y, en caso necesario, formal, sobre problemas que se planteen en su entorno.

CG2-Estar capacitado para, utilizando el nivel adecuado de abstracción, establecer y evaluar modelos que representen situaciones reales.

CG3-Estar capacitado para encontrar, relacionar, estructurar e interpretar datos, información y conocimiento provenientes de

diversas fuentes.

CG5-Estar capacitado tanto para trabajar autónomamente, como para integrarse de modo eficaz en equipos de trabajo.

CG7-Haber desarrollado aquellas habilidades de aprendizaje necesarias para continuar su formación.

CG10-Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.

CG12-Capacidad para concebir, desarrollar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería del software como instrumento para el aseguramiento de su calidad.

CG14-Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento.

CG15-Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

CG17-Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática.

CG18-Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática.

Competencias específicas

CE7-Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

CE11-Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas.

CE14-Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.

CE29-Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.

RESULTADOS DEL APRENDIZAJE

- Tener una visión global de las diferentes áreas que abarca la Seguridad Informática y de los problemas de seguridad derivados del uso de equipos y aplicaciones informáticas
- Ser capaces de concebir, planificar e implantar políticas y medidas de seguridad razonables en entornos profesionales
- Conocer las características de los algoritmos de cifrado más importantes y saber decidir cuál de ellos utilizar en cada situación
- Configurar dispositivos físicos de seguridad
- Conocer los conceptos asociados a la firma digital así como alguna herramienta que permita implantarla
- Reconocer vulnerabilidades en una determinada aplicaciones web así como proponer mecanismos que las mitiguen
- Reconocer las principales amenazas y vulnerabilidades a nivel de infraestructuras de redes e Internet y las diferentes técnicas de defensa aplicables.

TEMARIO

1. Introducción: definiciones y principios de seguridad
2. Seguridad física. Copias de seguridad
3. Aspectos organizativos, sociales y legales
4. Criptografía clásica y moderna
5. Certificados digitales. Firma digital
6. Seguridad en las comunicaciones. Protocolos seguros
7. Seguridad en redes. Sistemas de detección y prevención
8. Seguridad en sistemas operativos. Malware
9. Técnicas de defensa. Hacking ético y análisis forense
10. Seguridad en la programación. Protección del software
11. Desarrollo de aplicaciones web seguras
12. Planificación y gestión de la seguridad. SGSI. Análisis de riesgos

BIBLIOGRAFÍA

Tipo:	Título
Básica	Enciclopedia de la seguridad informática / Alvaro Gómez Vieites Absys Biba
Complementaria	Applied Information Security: A Hands-on Approach / David Basin, Patrick Schaller, Michael Schlpfer Absys Biba
Complementaria	Security engineering : a guide to building dependable distributed systems / Ross J. Anderson.
Complementaria	Seguridad informática : Hacking Ético - Conocer el ataque para una mejor defensa / Marion Agé, Franck Ebel, Raphaël Rault, Robert Crocfer, David Dumas, Laurent Schal http://www.eni-training.com/cs/unirioja/?library_guid=30920814-dd55-4cfe-8c5d-1a45f2e11a11
	Understanding Cryptography: A Textbook for Students and Practitioners / Christof Paar, Jan Pezl

Complementaria	Absys Biba
Complementaria	Los códigos secretos : el arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet / Simon Singh Absys Biba
Complementaria	Los delitos del futuro. Todo está conectado, todos somos vulnerables, ¿qué podemos hacer al respecto? / Marc Goodman

Recursos en Internet

Guías INCIBE

<https://www.incibe.es/protege-tu-empresa/guias>

Guías Centro Criptológico Nacional

<https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic.html>

Herramientas de seguridad

<http://sectools.org>

Herramientas - Oficina de seguridad del internauta

<https://www.osi.es/es/herramientas-gratuitas>

Recursos seguridad en aplicaciones web (OWASP)

<https://www.owasp.org>

Recursos sobre ISO27000

<http://www.iso27000.es/>**METODOLOGÍA****Modalidades organizativas**

Clases teóricas

Clases prácticas

Estudio y trabajo autónomo individual

Métodos de enseñanza

Método expositivo - Lección magistral

Estudio de casos

Resolución de ejercicios y problemas

ORGANIZACIÓN

Actividades presenciales	Tamaño de grupo	Horas
Clases prácticas de laboratorio o aula informática	Informática	28,00
Clases teóricas	Grande	32,00
Total de horas presenciales		60,00
Trabajo autónomo del estudiante		Horas
Estudio autónomo individual o en grupo		50,00
Preparación de las prácticas y elaboración de cuaderno de prácticas		20,00
Preparación en grupo de trabajos, presentaciones (orales, debates, ...), actividades en biblioteca o similar		5,00
Resolución individual de ejercicios, cuestiones u otros trabajos, actividades en biblioteca o similar		15,00
Total de horas de trabajo autónomo		90,00
Total de horas		150,00

EVALUACIÓN

Sistemas de evaluación	Recuperable	No Recup.
Pruebas escritas	60%	
Trabajos y proyectos		5%
Informes y memorias de prácticas		35%
Total		100%

Comentarios

Para los estudiantes a tiempo parcial (reconocidos como tales por la Universidad), las actividades de evaluación no recuperable podrán ser sustituidas por otras, a especificar en cada caso. Esta posibilidad se habilitará siempre y cuando la causa que le impida la realización de la actividad de evaluación programada sea la que ha llevado al reconocimiento de la dedicación a tiempo parcial.



La evaluación final de la asignatura corresponde con la actividad de evaluación "Pruebas escritas" (60%) que consta de una parte teórica y un supuesto práctico.

El material didáctico se encontrará disponible en un aula virtual para todos los alumnos matriculados en esta asignatura.

Criterios críticos para superar la asignatura

Será necesario superar las "pruebas escritas" para aprobar la asignatura.

La nota final de las "pruebas escritas" se obtiene como la media de la parte teórica y el supuesto práctico. Para realizar dicha media se exige una nota mínima de 4 puntos en cada parte.