



## Guía Docente

Datos Identificativos					2013/14
Asignatura (*)	Seguridade nos sistemas Informáticos	Código	614G01079		
Titulación					
Descritores					
Ciclo	Período	Curso	Tipo	Créditos	
Grao	1º cuatrimestre	Cuarto	Obrigatoria	6	
Idioma	Castelán				
Prerrequisitos					
Departamento	Tecnoloxías da Información e as Comunicaci3ns				
Coordinaci3n	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es		
Profesorado	Vázquez Naya, José Manuel	Correo electrónico	jose.manuel.vazquez.naya@udc.es		
Web	campusvirtual.udc.es				
Descrici3n xeral	<p>La seguridad en los sistemas de informaci3n es crucial en todos y cada uno de los servicios ofertados por la denominada sociedad de la informaci3n. Incluso en este 3mbito, todavía en desarrollo, los requisitos de seguridad cambian a un ritmo vertiginoso. Puesto que cada vez m3s informaci3n est3 accesible, cada vez se requieren controles de seguridad m3s estrictos. El avance tecnol3gico en este caso funciona de catalizador en ambas direcciones: por un lado favorece el acceso a nuevos tipos y a mayor cantidad de informaci3n (lo que requiere un aumento de los controles de seguridad) y por otro lado posibilita la implantaci3n de mecanismos de seguridad m3s refinados (que posibilitan el acceso seguro a nuevos tipos de informaci3n).</p> <p>La asignatura est3 planteada para proporcionar al alumno el conocimiento necesario de los conceptos b3sicos y t3cnicas empleadas para la protecci3n de los sistemas de informaci3n, desde el punto de vista f3sico, l3gico y administrativo. Estos conceptos b3sicos incluir3n, como paso de inicio, la evoluci3n de los diferentes m3todos y algoritmos de cifrado. Debido al enorme auge de los diversos medios electr3nicos de intercambio de informaci3n (correo electr3nico, p3ginas web, e-commerce, firma digital, etc.) un aspecto fundamental cuando se trabaja en este 3mbito ser3 tener la formaci3n suficiente en la seguridad de este tipo de sistemas. Para el correcto funcionamiento de los servicios referidos se exige la existencia de una infraestructura (redes de comunicaciones y sistemas operativos) que funcione de modo seguro y confiable. Por lo tanto ser3 necesario conocer los aspectos fundamentales de los componentes, protocolos de funcionamiento, configuraci3n, etc. de dicha infraestructura.</p> <p>Dichos conocimientos ser3n los que le permitan entender y solucionar los riesgos actuales, y los que inevitablemente surgir3n en el futuro, que afectan a todo sistema de informaci3n.</p> <p>Objetivos:</p> <ul style="list-style-type: none"><li>- Familiarizarse con el proceso de la seguridad</li><li>- Identificar los riesgos de los sistemas de informaci3n</li><li>- Conocer distintos mecanismos para dotar de seguridad a un sistema de informaci3n</li><li>- Comprender los conceptos fundamentales de la criptografía</li><li>- Entender qu3 es, c3mo se define y c3mo se aplica una política de seguridad</li></ul>				

## Competencias da titulaci3n

C3digo	Competencias da titulaci3n
--------	----------------------------

## Resultados da aprendizaxe

Competencias de materia (Resultados de aprendizaxe)	Competencias da titulaci3n
---	----------------------------



Resumir los fundamentos de los criptosistemas	A5 A7 A29 A36 A47 A50 A58	B5 B7	
Definir los riesgos y vulnerabilidades de un sistema de información	A4 A6 A7 A11 A14 A16	B2 B3 B7 B8	C1 C3 C6
Analizar los nuevos avances en seguridad y sus repercusiones		B3 B7	C6 C7
Utilizar las herramientas de seguridad	A11 A24 A38 A58		C3
Organizar la seguridad de un sistema de información	A7 A36 A47 A58		C3
Expresar de forma clara y efectiva la necesidad, implantación, ventajas y desventajas de las medidas de seguridad		B2 B3 B7	C1 C3
Asumir la existencia de vulnerabilidades en los sistemas de información e intentar su minimización			C4 C6
Colaborar con otros profesionales (administradores de sistemas, redes, bases de datos, aplicaciones, etc.) en la puesta en marcha y mantenimiento de las medidas de seguridad		B1 B2 B4	

Contidos	
Temas	Subtemas
Análisis de Riesgos y Medidas de Seguridad	Análisis de Riesgos Gestión del Riesgo Medidas de Seguridad
Criptografía	Sistemas criptográficos clásicos Sistemas criptográficos de clave secreta Sistemas criptográficos de clave pública Firma digital
Malware	Virus Trojanos Rootkits Exploits
Análisis forense	Fases del Análisis Forense Herramientas HW y SW
Normativa	ISO 27001
Estudios de casos	Estudio de casos reales de ataques a sistemas de información.
Prácticas	Prueba de distintas herramientas de seguridad, relacionadas con los temas de teoría.



## Planificación

Metodoloxías / probas	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Sesión maxistral	15	22.5	37.5
Prácticas de laboratorio	12	24	36
Seminario	7.5	15	22.5
Traballos tutelados	3	18	21
Estudo de casos	3	3	6
Presentación oral	5	5	10
Proba mixta	1.5	7.5	9
Eventos científicos e/ou divulgativos	2	0	2
Atención personalizada	6	0	6

\*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado

## Metodoloxías

Metodoloxías	Descrición
Sesión maxistral	Introducción conceptos y aspectos clave de cada uno de los temas
Prácticas de laboratorio	Prueba de herramientas de seguridad relacionadas con los temas explicados en la sesión magistral
Seminario	Los seminarios se configurarán como una extensión de las prácticas de laboratorio. A diferencia de estas, se potenciará el desarrollo práctico en grupos, frente al trabajo individual en las prácticas de laboratorio. El trabajo en común con los alumnos permitirá valorar el progreso de la clase hacia los objetivos marcados.
Traballos tutelados	Trabajos académicos relativos al contenido teórico de la asignatura
Estudo de casos	Estudio de casos reales de temas relacionados con la seguridad de sistemas
Presentación oral	Presentación trabajos tutelados
Proba mixta	Realización examen
Eventos científicos e/ou divulgativos	Asistencia a eventos de interés (conferencias, seminarios, etc.)

## Atención personalizada

Metodoloxías	Descrición
Traballos tutelados	Resolución de dudas.
Prácticas de laboratorio	Tutorización personalizada trabajos individuales.
Seminario	

## Avaliación

Metodoloxías	Descrición	Cualificación
Traballos tutelados	Realización de trabajos tutelados:  Criterios evaluación: calidad trabajos y presentaciones, participación activa en las defensas de los compañeros, actitud	20
Prácticas de laboratorio	Realización de prácticas  Criterios de evaluación: Aprovechamiento horas laboratorio, defensa de la práctica	20
Proba mixta	Asimilación de Conceptos Teóricos, relativos a los bloques de teoría, prácticas de laboratorio y trabajos tutelados).  Nota mínima exigida: 5	50



Seminario	Realización de prácticas en grupos reducidos	10
	Criterios de evaluación: Aprovechamiento horas laboratorio, defensa de la práctica	
Outros		

### Observacións avaliación

### Fontes de información

<b>Bibliografía básica</b>	<ul style="list-style-type: none"><li>- Jorge Ramió (1999). Aplicaciones Criptográficas. UPM</li><li>- S. Harris (2010). CISSP All in one. 5ª Edición. Mc-Graw Hill</li><li>- W. Stallings (2004). Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. 2ª Edición. Pearson Educación</li><li>- M. Mackrill, C. Nowell, K. Stopford, C. Trautwein (2011). Official ISC2 Guide to the SSCP CBK. 2ª Edición. Ed. Harold F. Tripton</li></ul>
<b>Bibliografía complementaria</b>	<ul style="list-style-type: none"><li>- Manuel J. Lucena (). Critpografía y seguridad en Computadores. <a href="http://www.di.ujaen.es/~mlucena">http://www.di.ujaen.es/~mlucena</a></li><li>- Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly</li><li>- Information Security Forum (). The Standard of good Practice for Information Security. <a href="http://www.isfsecuritystandard.com">http://www.isfsecuritystandard.com</a></li></ul>

### Recomendacións

#### Materias que se recomenda ter cursado previamente

#### Materias que se recomenda cursar simultaneamente

#### Materias que continúan o temario

Lexislación e Seguridade Informática/614G01024

### Observacións

Otros materiais de apoio:

Se proporcionarán al alumno las diapositivas empleadas para el desarrollo de las clases, así como referencias bibliográficas en las que pueda profundizar en el estudio de determinados puntos del temario.

(\*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías