



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 Comunicaciós				
Coordinación	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				
Descrición xeral	<p>La seguridad en los sistemas de información es crucial en todos y cada uno de los servicios ofertados por la denominada sociedad de la información. Incluso en este ámbito, todavía en desarrollo, los requisitos de seguridad cambian a un ritmo vertiginoso. Puesto que cada vez más información está accesible, cada vez se requieren controles de seguridad más estrictos. El avance tecnológico en este caso funciona de catalizador en ambas direcciones: por un lado favorece el acceso a nuevos tipos y a mayor cantidad de información (lo que requiere un aumento de los controles de seguridad) y por otro lado posibilita la implantación de mecanismos de seguridad más refinados (que posibilitan el acceso seguro a nuevos tipos de información).</p> <p>La asignatura está planteada para proporcionar al alumno el conocimiento necesario de los conceptos básicos y técnicas empleadas para la protección de los sistemas de información, desde el punto de vista físico, lógico y administrativo. Estos conceptos básicos incluirán, como paso de inicio, la evolución de los diferentes métodos y algoritmos de cifrado. Debido al enorme auge de los diversos medios electrónicos de intercambio de información (correo electrónico, páginas web, e-commerce, firma digital, etc.) un aspecto fundamental cuando se trabaja en este ámbito será tener la formación 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 será necesario conocer los aspectos fundamentales de los componentes, protocolos de funcionamiento, configuración, etc. de dicha infraestructura.</p> <p>Dichos conocimientos serán los que le permitan entender y solucionar los riesgos actuales, y los que inevitablemente surgirán en el futuro, que afectan a todo sistema de información.</p> <p>Objetivos:</p> <ul style="list-style-type: none">- Familiarizarse con el proceso de la seguridad- Identificar los riesgos de los sistemas de información- Conocer distintos mecanismos para dotar de seguridad a un sistema de información- Comprender los conceptos fundamentales de la criptografía- Entender qué es, cómo se define y cómo se aplica una política de seguridad				

Competencias da titulación

Código	Competencias da titulación
--------	----------------------------

Resultados da aprendizaxe

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



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

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

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