Guía Docente				
Datos Identificativos				2013/14
Asignatura (*)	Seguridade nos sistemas Informáticos		Código	614G01079
Titulación	Grao en Enxeñaría Informática			
Descriptores				
Ciclo	Período	Curso	Tipo	Créditos
Grao	1º cuadrimestre	Cuarto	Obrigatoria	6
Idioma	Castelán			
Prerrequisitos				
Departamento	Tecnoloxías da Información e as Comunicacións			
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	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). 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. 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. Objetivos: - 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
A4	Coñecementos básicos sobre o uso e a programación dos ordenadores, sistemas operativos, bases de datos e programas informáticos con aplicación na enxeñaría.
A5	Coñecemento da estrutura, organización, funcionamento e interconexión dos sistemas informáticos, os fundamentos da súa programación e a súa aplicación para a resolución de problemas propios da enxeñaría.
A6	Coñecemento adecuado do concepto de empresa, marco institucional e xurídico da empresa. Organización e xestión de empresas.

A7	Capacidade para deseñar, desenvolver, seleccionar e avaliar aplicacións e sistemas informáticos que aseguren a súa fiabilidade, seguranza e calidade, conforme a principios éticos e á lexislación e normativa vixente.
A11	Coñecemento, administración e mantemento de sistemas, servizos e aplicacións informáticas.
A14	Capacidade para analizar, deseñar, construír e manter aplicacións de forma robusta, segura e eficiente, elixindo o paradigma e as linguaxes de programación máis adecuados.
A16	Coñecemento das características, funcionalidades e estrutura dos sistemas operativos, e deseñar e implementar aplicacións baseadas nos seus servizos.
A24	Coñecemento da normativa e a regulación da informática nos ámbitos nacional, europeo e internacional.
A29	Capacidade de identificar, avaliar e xestionar os riscos potencias asociados que se puideren presentar.
A36	Capacidade para comprender, aplicar e xestionar a garantía e a seguridade dos sistemas informáticos.
A38	Capacidade para deseñar, despregar, administrar e xestionar redes de computadores.
A47	Capacidade para determinar os requisitos dos sistemas de información e comunicación dunha organización de acordo cos aspectos de seguridade e cumprimento da normativa e a lexislación vixente.
A50	Capacidade para comprender e aplicar os principios da avaliación de riscos e aplicalos correctamente na elaboración e execución de plans de actuación.
A58	Capacidade para comprender, aplicar e xestionar a garantía e seguranza dos sistemas informáticos.
B1	Capacidade de resolución de problemas
B2	Traballo en equipo
B3	Capacidade de análise e síntese
B4	Capacidade para organizar e planificar
B5	Habilidades de xestión da información
B7	Preocupación pola calidade
B8	Capacidade de traballar nun equipo interdisciplinar
C1	Expresarse correctamente, tanto de forma oral coma escrita, nas linguas oficiais da comunidade autónoma.
C3	Utilizar as ferramentas básicas das tecnoloxías da información e as comunicacións (TIC) necesarias para o exercicio da súa profesión e para a aprendizaxe ao longo da súa vida.
C4	Desenvolverse para o exercicio dunha cidadanía aberta, culta, crítica, comprometida, democrática e solidaria, capaz de analizar a realidade, diagnosticar problemas, formular e implantar solucións baseadas no coñecemento e orientadas ao ben común.
C6	Valorar criticamente o coñecemento, a tecnoloxía e a información dispoñible para resolver os problemas cos que deben enfrontarse.
C7	Asumir como profesional e cidadán a importancia da aprendizaxe ao longo da vida.

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 Troyanos 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 nos 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 Prácticas de laboratorio Seminario	Resolución de dudas. Tutorización personalizada trabajos individuales.

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 Criterios de evaluación: Aprovechamiento horas laboratorio, defensa de la práctica	10
Outros		

Observacións avaliación

Fontes de información	
Bibliografía básica	- 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	- Manuel J. Lucena (). Critpografía y seguridad en Computadores. http://wwwdi.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 materiales de apoyo: 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.