Guia docente				
Datos Identificativos				2014/15
Asignatura (*)	Seguridad en los sistemas Informáticos		Código	614G01079
Titulación	Grao en Enxeñaría Informática			
Descriptores				
Ciclo	Periodo	Curso	Tipo	Créditos
Grado	1º cuatrimestre	Cuarto	Obligatoria	6
Idioma	Castellano			
Prerrequisitos				
Departamento	Tecnoloxías da Información e as Comunicacións			
Coordinador/a	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			
Descripción general	A seguridade nos sistemas de información é crucial en todos e cada un dos servizos ofertados pola denominada sociedade da información. Mesmo neste ámbito, aínda en desenvolvemento, os requisitos de seguridade cambian a un ritmo vertixinoso. Posto que cada vez máis información está accesible, cada vez requírense controis de seguridade máis estritos. O avance tecnolóxico neste caso funciona de catalizador en ambas as direccións: por unha banda favorece o acceso a novos tipos e a maior cantidade de información (o que require un aumento dos controis de seguridade) e doutra banda posibilita a implantación de mecanismos de seguridade máis refinados (que posibilitan o acceso seguro a novos tipos de información). A materia está exposta para proporcionar ao alumno o coñecemento necesario dos conceptos básicos e técnicas empregadas para a protección dos sistemas de información, desde o punto de vista físico, lóxico e administrativo. Estes conceptos básicos incluirán, como paso de inicio, a evolución dos diferentes métodos e algoritmos de cifrado. Debido ao enorme auxe dos diversos medios electrónicos de intercambio de información (correo electrónico, páxinas web, e-commerce, firma dixital, etc.), un aspecto fundamental cando se traballa neste ámbito será ter a formación suficiente na seguridade deste tipo de sistemas. Para o correcto funcionamento dos servizos referidos esíxese a existencia dunha infraestrutura (redes de comunicacións e sistemas operativos) que funcione de modo seguro e fiable. Por tanto será preciso coñecer os aspectos fundamentais dos compoñentes, protocolos de funcionamento, configuración, etc. da devandita infraestrutura. Este coñecemento será o que lle permita ao alumno entender e solucionar os riscos actuais, e os que inevitablemente xurdirán no futuro, que afectan a todo sistema de información. Obxectivos: - Familiarizarse co proceso da seguridade - Identificar os riscos dos sistemas de información - Coñecer distintos mecanismos para dotar de seguridade a un sistema de información - Comprender os conceptos fundamentais da criptografía - Entender que é, como se define e como se aplica unha política de seguridade			

Competencias de la titulación	
Código	Competencias de la titulación
A36	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
A58	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
B1	Capacidad de resolución de problemas
B3	Capacidad de análisis y síntesis
C2	Dominar la expresión y la comprensión de forma oral y escrita de un idioma extranjero.
C3	Utilizar las herramientas básicas de las tecnologías de la información y las comunicaciones (TIC) necesarias para el ejercicio de su profesión y para el aprendizaje a lo largo de su vida.
C4	Desarrollarse para el ejercicio de una ciudadanía abierta, culta, crítica, comprometida, democrática y solidaria, capaz de analizar la realidad, diagnosticar problemas, formular e implantar soluciones basadas en el conocimiento y orientadas al bien común.
C6	Valorar críticamente el conocimiento, la tecnología y la información disponible para resolver los problemas con los que deben enfrentarse.

C7	Asumir como profesional y ciudadano la importancia del aprendizaje a lo largo de la vida.
C8	Valorar la importancia que tiene la investigación, la innovación y el desarrollo tecnológico en el avance socioeconómico y cultural de la sociedad.

Resultados de aprendizaje			
Competencias de materia (Resultados de aprendizaje)	Competencias de la titulación		
Identificar los fundamentos de los criptosistemas e identificar los mecanismos de seguridad así como su integración en las organizaciones	A36 A58	B3	C2 C3 C4 C6 C7 C8
Definir los riesgos y vulnerabilidades de un sistema de información y su aplicación en entornos reales.	A36 A58	B1	C2 C3 C4 C6 C7 C8
Utilizar las herramientas de seguridad	A36 A58	B1	C3
Organizar la seguridad de un sistema de información	A36 A58	B1	C3 C4 C6 C7 C8
Expresar de forma clara y efectiva la necesidad, implantación, ventajas y desventajas de las medidas de seguridad	A36 A58	B3	C3 C4 C6 C8

Contenidos	
Tema	Subtema
Criptografía	Sistemas criptográficos clásicos Sistemas criptográficos de clave secreta Sistemas criptográficos de clave pública Firma digital
Normativa	ISO 27001
Análisis de Riesgos y Medidas de Seguridad	Análisis de Riesgos Gestión del Riego Medidas de Seguridad
Malware	Virus "Trojans" "Rootkits" "Exploits"
Análisis Forense	Fases del Análisis Forense Herramientas HW y SW
Estudio 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			
Metodologías / pruebas	Horas presenciales	Horas no presenciales / trabajo autónomo	Horas totales
Sesión magistral	16	32	48
Prácticas de laboratorio	18	36	54
Trabajos tutelados	10	30	40
Prueba objetiva	2	0	2
Atención personalizada	6	0	6
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos			

Metodologías	
Metodologías	Descripción
Sesión magistral	Clases expositivas de presentación de los conocimientos teóricos de cada uno de los temas. Se fomentará la participación del alumnado. El material utilizado en estas clases estará disponible en la plataforma de formación de la Universidad de A Coruña.
Prácticas de laboratorio	Sesiones prácticas en ordenador, en las que se deben resolver una serie de boletines de ejercicios prácticos propuestos por el profesor. Los ejercicios buscan consolidar los conocimientos presentados en las sesiones magistrales y también fomentar el aprendizaje autónomo del alumno. En la resolución de los ejercicios, se utilizarán distintas herramientas de seguridad, con el objetivo de que el alumno las conozca y adquiera destreza en su uso. La mayor parte de los ejercicios tienen carácter individual, aunque algunos serán realizados en grupo. Una vez completado el boletín de ejercicios, el profesor evaluará el trabajo realizado por el alumno mediante una sesión de trabajo en ordenador. Los boletines de ejercicios se publicarán a través de la plataforma de formación de la Universidad de A Coruña. Se impondrá una fecha máxima de defensa para cada boletín, con el objetivo de fomentar el estudio continuo.
Trabajos tutelados	Trabajos académicos relativos al contenido teórico de la asignatura. El profesor propondrá un listado de temas, relacionados con el temario de la asignatura. Los alumnos deberán escoger una temática y consensuar la estructura del trabajo con el profesor. Finalmente, los alumnos presentarán el trabajo en clase. El objetivo de los trabajos es que el alumno profundice en un tema de su interés. Los trabajos se realizarán en grupo. Se fomentará la participación del alumnado.
Prueba objetiva	Prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridas por el alumno.

Atención personalizada	
Metodologías	Descripción
Trabajos tutelados Prácticas de laboratorio	Resolución de dudas. Supervisión de los trabajos tutelados.

Evaluación		
Metodologías	Descripción	Calificación
Prueba objetiva	Al finalizar el cuatrimestre, se realizará una prueba escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno. Es condición necesaria (pero no suficiente) obtener una puntuación mínima de 5 sobre 10 en la prueba objetiva para poder superar la asignatura.	50

Trabajos tutelados	Realización del trabajo tutelado y su presentación en clase. Criterios evaluación: dificultad y contenido del trabajo, existencia de componente práctica, calidad de la memoria y presentación. También se valorará la participación activa en clase durante la presentación del resto de trabajos. Es condición necesaria (pero no suficiente) obtener una puntuación mínima de 5 sobre 10 en el trabajo tutelado para poder superar la asignatura. Es obligatorio asistir a las presentaciones de los trabajos tutelados. La ausencia no justificada a más del 20% de los trabajos supondrá la imposibilidad de superar la asignatura.	20
Prácticas de laboratorio	Realización y defensa de las prácticas en ordenador, dentro de las horas de prácticas y antes de la fecha límite establecida. Es condición necesaria (pero no suficiente) obtener una puntuación mínima de 4 sobre 10 en las prácticas para poder superar la asignatura.	30
Otros		

Observaciones evaluación

Alumnos a tiempo parcial
Alumnado con reconocimiento de dedicación a tiempo parcial y
dispensa académica de exención de asistencia, según establece la "NORMA
QUE REGULA O RÉXIME DE DEDICACIÓN AO ESTUDIO DOS ESTUDANTES DE GRAO NA UDC
(Art. 2.3; 3.b e 4.5)(29/5/2012)".
Los alumnos que cursen la asignatura a tiempo parcial deben realizar las mismas pruebas de evaluación que los alumnos que las cursen a tiempo completo, con las siguientes consideraciones:
Quedan exentos de la asistencia a clase.En cuanto a la defensa de las prácticas, si el alumno no pudiese asistir a la defensa en el horario de prácticas, se convendrá con él un horario alternativo.En cuanto a la realización del trabajo tutelado, se exime al alumno de la necesidad de realizar el trabajo en grupo, pudiendo realizarlo individualmente, y, en caso de no poder presentar el trabajo en clase por incompatibilidad en el horario, el alumno podrá realizar la presentación al profesor en el horario convenido por ambos. El alumno deberá notificar al coordinador de la asignatura su condición de estudiante a tiempo parcial tan pronto como le sea
reconocida, de cara a que el profesor pueda realizar una correcta planificación
de las actividades docentes.
Segunda oportunidad y oportunidad adelantada de Diciembre
Aspectos a tener en cuenta:
En caso de no haber presentado (o no haber superado) las prácticas de laboratorio en primera oportunidad, el alumno deberá someterse a un (nuevo) examen de prácticas, con ordenador. En caso de no haber presentado (o no haber superado) el trabajo tutelado en primera oportunidad, el alumno deberá acordar con el coordinador de la asignatura una temática para la realización de un nuevo trabajo. Tanto el examen de prácticas como la presentación del trabajo tutelado se realizarán, salvo que el alumno haya acordado otra cosa con el coordinador, con anterioridad al día fijado oficialmente para el examen correspondiente a la convocatoria en cuestión (Julio o Diciembre). Para ello, el alumno debe contactar con el coordinador y convenir con él una fecha y hora para la realización del examen y/o la presentación del trabajo.Condición de "No Presentado"Se considerarán como "no presentados" a los alumnos que no realicen la prueba objetiva.

Fuentes de información

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
Complementária	- 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

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Legislación y Seguridad Informática/614G01024 Administración de Sistemas Operativos/614G01047 Administración de Redes/614G01048 Administración de Bases de Datos/614G01050
Otros comentarios

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías