



Guía Docente				
Datos Identificativos			2014/15	
Asignatura (*)	Seguridade nos Sistemas Informáticos	Código	614G01214	
Titulación	Grao en Enxeñaría Informática			
Descritores				
Ciclo	Período	Curso	Tipo	Créditos
Grao	2º cuatrimestre	Curso de Adaptación Enxeñeiros Téc. en Informática	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>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).</p> <p>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 incluírán, 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.</p> <p>Obxectivos:</p> <ul style="list-style-type: none"><li>- Familiarizarse co proceso da seguridade</li><li>- Identificar os riscos dos sistemas de información</li><li>- Coñecer distintos mecanismos para dotar de seguridade a un sistema de información</li><li>- Comprender os conceptos fundamentais da criptografía</li><li>- Entender que é, como se define e como se aplica unha política de seguridade</li></ul>			

Competencias da titulación	
Código	Competencias da titulación
A36	Capacidade para comprender, aplicar e xestionar a garantía e a seguridade dos sistemas informáticos.
A58	Capacidade para comprender, aplicar e xestionar a garantía e seguranza dos sistemas informáticos.
B1	Capacidade de resolución de problemas
B3	Capacidade de análise e síntese
C2	Dominar a expresión e a comprensión de forma oral e escrita dun idioma estranxeiro.
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.
C8	Valorar a importancia que ten a investigación, a innovación e o desenvolvemento tecnolóxico no avance socioeconómico e cultural da sociedade.

Resultados da aprendizaxe			
Competencias de materia (Resultados de aprendizaxe)	Competencias da titulación		
Identificar os fundamentos dos criptosistemas e identificar os mecanismos de seguridade así como a súa integración nas organizacións	A36 A58	B3	C2 C3 C4 C6 C7 C8
Definir os riscos e vulnerabilidades dun sistema de información e a súa aplicación en contornas reais	A36 A58	B1	C2 C3 C4 C6 C7 C8
Utilizar as ferramentas de seguridade	A36 A58	B1	C2 C3 C4 C6 C7 C8
Organizar a seguridade dun sistema de información	A36 A58	B1	C3 C4 C6 C7 C8
Expresar de forma clara e efectiva a necesidade, implantación, vantaxes e desvantaxes das medidas de seguridade	A36 A58	B3	C2 C3 C4 C6 C7 C8

Contidos	
Temas	Subtemas
Criptografía	Sistemas criptográficos clásicos Sistemas criptográficos de clave secreta Sistemas criptográficos de clave pública Firma dixital
Normativa	ISO 27001
Análise de Riscos e Medidas de Seguridade	Análise de Riscos Xestión do Risco Medidas de Seguridade



Malware	Virus &quot;Trojans&quot; &quot;Rootkits&quot; &quot;Exploits&quot;
Análise Forense	Fases da Análise Forense Ferramentas HW e SW
Estudio de casos	Estudo de casos reais de ataques a sistemas de información
Prácticas	Proba de distintas ferramentas de seguridade, relacionadas cos temas de teoría

Planificación			
Metodoloxías / probas	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Sesión maxistral	16	32	48
Prácticas de laboratorio	18	36	54
Traballos tutelados	10	30	40
Proba obxectiva	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	Clases expositivas de presentación dos coñecementos teóricos de cada un dos temas. Fomentarase a participación do alumnado. O material utilizado nestas clases estará dispoñible na plataforma de formación da Universidade da Coruña.
Prácticas de laboratorio	Sesións prácticas en computador, nas que se deben resolver unha serie de boletíns de exercicios prácticos propostos polo profesor. Os exercicios buscan consolidar os coñecementos presentados nas sesións maxistras e tamén fomentar a aprendizaxe autónoma do alumno. Na resolución dos exercicios, utilizaranse distintas ferramentas de seguridade, co obxectivo de que o alumno as coñeza e adquira destreza no seu uso. A maior parte dos exercicios teñen carácter individual, aínda que algúns serán realizados en grupo. Unha vez completado o boletín de exercicios, o profesor avaliará o traballo realizado polo alumno mediante unha sesión de traballo en computador. Os boletíns de exercicios publicaranse a través da plataforma de formación da Universidade da Coruña. Imporase unha data máxima de defensa para cada boletín, co obxectivo de fomentar o estudo continuo.
Traballos tutelados	Traballos académicos relativos ao contido teórico da materia. O profesor proporá unha listaxe de temas, relacionados co temario da materia. Os alumnos deberán escoller unha temática e acordar a estrutura do traballo co profesor. Finalmente, os alumnos presentarán o traballo en clase. O obxectivo dos traballos é que o alumno profunde nun tema do seu interese. Os traballos realizaranse en grupo. Fomentarase a participación do alumnado.
Proba obxectiva	Proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.

Atención personalizada	
Metodoloxías	Descrición
Traballos tutelados	Resolución de dúbidas.
Prácticas de laboratorio	Supervisión dos traballos tutelados.

Avaliación		
Metodoloxías	Descrición	Cualificación



Traballos tutelados	<p>Realización do traballo tutelado e a súa presentación en clase.</p> <p>Criterios avaliación: dificultade e contido do traballo, existencia de compoñente práctica, calidade da memoria e presentación. Tamén se valorará a participación activa en clase durante a presentación do resto de traballos.</p> <p>É condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 no traballo tutelado para poder superar a materia.</p> <p>É obrigatorio asistir ás presentacións dos traballos tutelados. A ausencia non xustificada a máis do 20% dos traballos suporá a imposibilidade de superar a materia.</p>	20
Prácticas de laboratorio	<p>Realización e defensa das prácticas en computador, dentro das horas de prácticas e antes da data límite establecida.</p> <p>É condición necesaria (pero non suficiente) obter unha puntuación mínima de 4 sobre 10 nas prácticas para poder superar a materia.</p>	30
Proba obxectiva	<p>Ao finalizar o cuadrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.</p> <p>É condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 na proba obxectiva para poder superar a materia.</p>	50
Outros		

Observacións avaliación



Alumnos a

tempo parcial

Alumnado con

recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia, segundo establece a "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)".

Os alumnos que

cursen a materia a tempo parcial deben realizar as mesmas probas de avaliación que os alumnos que as cursen a tempo completo, coas seguintes consideracións:

Quedan exentos da asistencia a clase.

En canto á defensa das prácticas, se

o alumno non puidese asistir á defensa no horario de prácticas, convírase con el un horario alternativo. En canto á realización do traballo

tutelado, exímese ao alumno da necesidade de realizar o traballo en grupo,

podendo realizalo individualmente, e, en caso de non poder presentar o

traballo en clase por incompatibilidade no horario, o alumno poderá

realizar a presentación ao profesor no horario convindo por ambos. O alumno deberá

notificar ao coordinador da materia a súa condición de estudante a tempo

parcial tan pronto como lle sexa recoñecida, de face a que o profesor poida

realizar unha correcta planificación das actividades docentes.

Segunda

oportunidade e oportunidade adiantada de Decembro

Aspectos a ter en

conta:

En caso de non presentar (ou non

superar) as prácticas de laboratorio en primeira oportunidade, o alumno

deberá someterse a un (novo) exame de prácticas, con computador. En caso de non presentar (ou non

superar) o traballo tutelado en primeira oportunidade, o alumno deberá

acordar co coordinador da materia unha temática para a realización dun

novo traballo. Tanto o exame de prácticas como a

presentación do traballo tutelado realizaranse, salvo que o alumno

acordase outra cousa co coordinador, con anterioridade ao día fixado

oficialmente para o exame correspondente á convocatoria en cuestión (Xullo

ou Decembro). Para iso, o alumno debe contactar co coordinador e convir

con el unha data e hora para a realización do exame e/ou a presentación do

traballo. Condición

de "Non Presentado"

Consideraranse

como "non presentados" aos alumnos que non realicen a proba

obxectiva.



<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

Administración de Sistemas Operativos/614G01047

Administración de Redes/614G01048

Administración de Bases de Datos/614G01050

### Observacións

(\*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