



Guía Docente				
Datos Identificativos			2016/17	
Asignatura (*)	Seguridade nos Sistemas Informáticos	Código	614G01214	
Titulación				
Descritores				
Ciclo	Período	Curso	Tipo	Créditos
Grao	2º cuatrimestre	Curso de Adaptación Enxeñeiros Téc. en Informática	Obrigatoria	6
Idioma	Castelán			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Tecnoloxías da Información e as Comunicaciós			
Coordinación		Correo electrónico		
Profesorado		Correo electrónico		
Web	<a href="http://guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614G01&amp;assignatura=614G01079&amp;any_academic=2016_17&amp;">guiadocente.udc.es/guia_docent/index.php?centre=614&amp;ensenyament=614G01&amp;assignatura=614G01079&amp;any_academic=2016_17&amp;</a>			
Descrición xeral	614G01079 Cuarto 1º cuatrimestre Seguridade nos sistemas Informáticos 6 0 Grao en Enxeñaría Informática Obrigatoria Tecnoloxías da Información e as Comunicaciós  Vázquez Naya, José Manuel			

Competencias / Resultados do título	
Código	Competencias / Resultados do título

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Identificar os fundamentos dos criptosistemas e identificar os mecanismos de seguridade así como a súa integración nas organizacións	A58	B3	C3 C6
Definir os riscos e vulnerabilidades dun sistema de información e a súa aplicación en contornas reais.	A58	B1	C3 C6
Utilizar ferramentas de seguridade.	A58	B1	C3
Organizar a seguridade dun sistema de información.	A58	B1	C3 C6
Expresar de forma clara e efectiva a necesidade, implantación, vantaxes e desvantaxes das medidas de seguridade.	A58	B3	C3 C6

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 Trojans Rootkits Exploits
Análise Forense	Fases da Análise Forense Ferramentas HW e SW
Estudo 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	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	B3	16	32	48
Prácticas de laboratorio	A58 B1 C3 C6	18	36	54
Traballos tutelados	A58 B3 C3 C6	10	30	40
Proba obxectiva	A58 B1	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. Fomentárase 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 maxistrais 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. Fomentárase 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	Competencias / Resultados	Descrición	Cualificación



Traballos tutelados	A58 B3 C3 C6	Realización do traballo tutelado e a súa presentación en clase.  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.  É condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 no traballo tutelado para poder superar a materia.  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.	20
Prácticas de laboratorio	A58 B1 C3 C6	Realización e defensa das prácticas en computador, dentro das horas de prácticas e antes da data límite establecida.  É condición necesaria (pero non suficiente) obter unha puntuación mínima de 4 sobre 10 nas prácticas para poder superar a materia.	30
Proba obxectiva	A58 B1	Ao finalizar o cuatrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.  É condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 na proba obxectiva para poder superar a materia.	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.

## Fontes de información



<b>Bibliografía básica</b>	<ul style="list-style-type: none"><li>- Jorge Ramió (1999). Aplicaciones Criptográficas. UPM</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><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></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>- Information Security Forum (). The Standard of good Practice for Information Security. <a href="http://www.isfsecuritystandard.com">http://www.isfsecuritystandard.com</a></li><li>- Simson Garfinkel, Gene Spafford, Alan Schwartz (2003). Practical UNIX and Internet Security, Third Edition. O'Reilly</li></ul>

## Recomendacións

### Materias que se recomenda ter cursado previamente

Lexislación e Seguridade Informática/614G01024  
Administración de Sistemas Operativos/614G01047  
Administración de Redes/614G01048  
Administración de Bases de Datos/614G01050

### Materias que se recomenda cursar simultaneamente

### Materias que continúan o temario

### 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