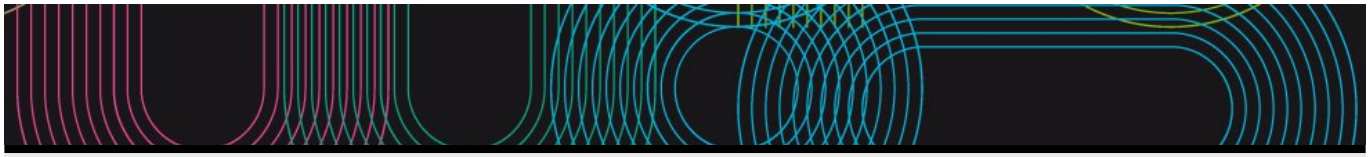

DATOS IDENTIFICATIVOS				
Seguridade en sistemas de información				
Materia	Seguridade en sistemas de información			
Código	P52M182V01207			
Titulación	Master Universitario en Dirección TIC para a defensa			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	4	OP	1	2c
Lingua de impartición	Castelán			
Departamento				
Coordinador/a	Fernández Gavilanes, Milagros			
Profesorado	Fernández Gavilanes, Milagros Vales Alonso, Javier			
Correo-e	mfgavilanes@cud.uvigo.es			
Web	http://campus.defensa.gob.es | https://moovi.uvigo.gal			
Descrición xeral	A materia de Seguridade en sistemas de información mostrará as técnicas, protocolos e arquitecturas relacionadas coa seguridade que existen nos distintos niveis de implementación dun sistema de información moderno, cunha énfase particular na parte das comunicacións. A materia enfocarase á exposición clara destes problemas, e á resolución práctica dos mesmos mediante casos de estudo prácticos.			

Competencias	
Código	
A6	CB6 - Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e/ou aplicación de ideas, a miúdo nun contexto de investigación.
A7	CB7 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo.
A8	CB8 - Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formular xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos.
A9	CB9 - Que os estudantes saiban comunicar as súas conclusións e os coñecementos e razóns últimas que as sustentan a públicos especializados e non especializados dun modo claro e sen ambigüidades.
A10	CB10 - Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en gran medida autodirixido ou autónomo.
B1	CG1 - Posuír coñecementos avanzados e altamente especializados e demostrar unha comprensión detallada e fundamentada dos aspectos teóricos e prácticos tratados nas diferentes áreas de estudo.
B2	CG2 - Integrar e aplicar os coñecementos adquiridos, e posuír capacidade de resolución de problemas en contornas novas ou definidas de forma imprecisa, incluíndo contextos de carácter multidisciplinar relacionados co seu ámbito de estudo.
B7	CG7 - Valorar a importancia dos aspectos de seguridade na xestión de sistemas e información, identificando necesidades de seguridade, analizando posibles ameazas e riscos e contribuíndo á definición e avaliación de criterios e políticas de seguridade.
C18	CISTI4 - Definir, analizar e implantar os mecanismos de seguridade durante todo o ciclo de vida dos sistemas de información.
D4	CT4 - Capacidade de comunicación oral e escrita de coñecementos.
D6	CT6 - Manexar apropiadamente recursos de información.

Resultados de aprendizaxe	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

RA1. Coñecer as ameazas e vulnerabilidades inherentes ao desenvolvemento de software mostrando como este pode facerse máis seguro	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA2. Describir os problemas, ameazas e solucións empregadas nos distintos niveis dun sistema/servizo de comunicacións	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA3. Describir as bases técnicas modernas da criptografía nos que se basean os sistemas de clave simétrica e de clave pública	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA4. Estudar os sistemas de infraestrutura de clave pública, recollendo en detalle como se abordará a creación, mantemento, distribución, uso, almacenaxe e revogación de certificados dixitais	A6 A7 A8 A9 A10 B1 B2 B7 C18
RA5. Describir novas aplicacións e tendencias no ámbito da seguridade nos sistemas de información	A6 A7 A8 A9 A10 B1 B2 B7 C18 D4 D6

Contidos	
Tema	
Tema 1. Introdución á seguridade en sistemas de información.	- Introdución aos Centros de Datos. - Estrutura habitual - Administración de Centros e Proceso de Datos
Tema 2. Seguridade no desenvolvemento de software.	- sSDLC - Vulnerabilidades - Contramedidas
Tema 3. Cifrado de clave simétrica.	- Principios matemáticos - Codificadores de bloque (DES, Triple-DES, AES) - Codificadores de fluxo (RC4)
Tema 4. Criptografía de clave pública.	- Motivación - Principios matemáticos - Diffie-Hellman - RSA - Criptografía de curvas elípticas (ECC)
Tema 5. Firmas dixitais.	- Sistemas de MAC e Hash - MD5 - SHA - HMAC

Tema 6. Sistemas de distribución de claves e autenticación.	- Introdución - Kerberos - X509 - Infraestrutura de clave pública (PKI)
Tema 7. Seguridade en transporte e web.	- Motivación - SSL - TLS - SSH
Tema 8. Seguridade en redes.	- IPSec - Firewalls - VPNs - Cloud systems
Tema 9. Tendencias no emprego dos sistemas de seguridade.	- Blockchain - Deep web - Anonimización - Criptomonedas - Criptografía de Proba de coñecemento cero - Cifrado negable - Criptografía de caixa branca - Compartición de secretos - Esteganografía - Criptografía cuántica - Voto electrónico

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Resolución de problemas de forma autónoma	0	8	8
Estudo previo	0	52	52
Lección maxistral	8	8	16
Resolución de problemas	2	2	4
Prácticas con apoio das TIC	4	0	4
Seminario	3	0	3
Foros de discusión	0	4	4
Autoavaliación	0	4	4
Presentación	4	0	4
Exame de preguntas de desenvolvemento	1	0	1

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Resolución de problemas de forma autónoma	Actividade na que o alumnado analiza e resolve problemas e/ou exercicios relacionados coa materia de forma autónoma.
Estudo previo	Procura, lectura, traballo de documentación e/ou realización de forma autónoma de calquera outra actividade que o alumno/a considere necesaria para permitirlle a adquisición de coñecementos e habilidades relacionadas coa materia. Adóitase levar a cabo con anterioridade ás clases, prácticas de laboratorio e/ou probas de avaliación.
Lección maxistral	Exposición por parte dun profesor/a de os contidos da materia obxecto de estudo, bases teóricas e/ou directrices dun traballo ou exercicio que o/a estudante ten de desenvolver.
Resolución de problemas	Actividade na que se formulan problemas e/ou exercicios relacionados coa materia. O alumno/a debe desenvolver as solucións adecuadas e correctas mediante a exercitación de rutinas, aplicación de fórmulas ou algoritmos, a aplicación de procedementos de transformación da información dispoñible e a interpretación dos resultados.
Prácticas con apoio das TIC	Actividades de aplicación dos coñecementos nun contexto determinado e de adquisición de habilidades básicas e procedimentales en relación coa materia, a través do uso do TIC.
Seminario	Actividade enfocada ao traballo sobre un tema específico, que permite profundar ou complementar nos contidos da materia.
Foros de discusión	Actividade desenvolvida nunha contorna virtual na que se debate sobre temas diversos e de actualidade relacionados co ámbito académico e/ou profesional.

Atención personalizada

Metodoloxías	Descrición

Lección maxistral	Dado o carácter semipresencial do curso, distinguiremos dous casos: (1) Atención na fase a distancia: levará a cabo mediante o uso de medios telemáticos. Os alumnos que o desexen poderán expor dúbidas ao profesorado en foros ou mediante correo electrónico. Tamén poderán concertar titorías individuais co profesor, que se desenvolverán mediante videoconferencia. (2) Atención na fase presencial: aínda que segue sendo posible o uso de mecanismos telemáticos de atención ao alumno, durante esta fase empregaranse tamén mecanismos de titoría presencial.
Resolución de problemas	Dado o carácter semipresencial do curso, distinguiremos dous casos: (1) Atención na fase a distancia: levará a cabo mediante o uso de medios telemáticos. Os alumnos que o desexen poderán expor dúbidas ao profesorado en foros ou mediante correo electrónico. Tamén poderán concertar titorías individuais co profesor, que se desenvolverán mediante videoconferencia. (2) Atención na fase presencial: aínda que segue sendo posible o uso de mecanismos telemáticos de atención ao alumno, durante esta fase empregaranse tamén mecanismos de titoría presencial.
Prácticas con apoio das TIC	Dado o carácter semipresencial do curso, distinguiremos dous casos: (1) Atención na fase a distancia: levará a cabo mediante o uso de medios telemáticos. Os alumnos que o desexen poderán expor dúbidas ao profesorado en foros ou mediante correo electrónico. Tamén poderán concertar titorías individuais co profesor, que se desenvolverán mediante videoconferencia. (2) Atención na fase presencial: aínda que segue sendo posible o uso de mecanismos telemáticos de atención ao alumno, durante esta fase empregaranse tamén mecanismos de titoría presencial.
Seminario	Dado o carácter semipresencial do curso, distinguiremos dous casos: (1) Atención na fase a distancia: levará a cabo mediante o uso de medios telemáticos. Os alumnos que o desexen poderán expor dúbidas ao profesorado en foros ou mediante correo electrónico. Tamén poderán concertar titorías individuais co profesor, que se desenvolverán mediante videoconferencia. (2) Atención na fase presencial: aínda que segue sendo posible o uso de mecanismos telemáticos de atención ao alumno, durante esta fase empregaranse tamén mecanismos de titoría presencial.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe			
Prácticas con apoio das TIC	Actividades de aplicación dos coñecementos nun contexto determinado e de adquisición de habilidades básicas e procedimentales en relación coa materia, a través do uso do TIC. Permiten avaliar os coñecementos e habilidades do alumno/a. Avaliaranse mediante entregables.	30	A6 A7 A8 A9 A10	B1 B2 B7	C18	D4
Foros de discusión	Actividade desenvolvida nunha contorna virtual na que se debate sobre temas diversos e de actualidade relacionados co ámbito académico e/ou profesional. Permite avaliar as habilidades, os coñecementos e, en menor medida, as actitudes do alumno/a. Avaliarase a participación nos foros.	10	A6 A7 A8 A9 A10	B1 B2 B7	C18	
Autoavaliación	Mecanismo no que, por medio dunha serie de preguntas ou actividades, posibilítase que o alumno/a avalíe de maneira autónoma o seu grao de adquisición de coñecementos e habilidades sobre a materia, permitindo unha autorregulación do proceso de aprendizaxe persoal.	10	A6 A7 A8 A9 A10	B1 B2 B7	C18	D4 D6
Presentación	Exposición por parte do alumnado, de maneira individual ou en grupo, dun tema relacionado cos contidos da materia ou dos resultados dun traballo, exercicio, proxecto, etc. A través da presentación pódense avaliar coñecementos, habilidades e actitudes.	30	A6 A7 A8 A9 A10	B1 B2 B7	C18	D4 D6
Exame de preguntas de desenvolvemento	Proba de avaliación que inclúe preguntas abertas e/ou exercicios, sobre un tema. Os alumnos/as deben desenvolver, relacionar, organizar e presentar os coñecementos que teñan sobre a materia nunha resposta argumentada. Pódese utilizar para avaliar coñecementos e habilidades.	20	A6 A7 A8 A9 A10	B1 B2 B7	C18	D4

Outros comentarios sobre a Avaliación

Será necesario sacar unha calificación non inferior ao 50% para superar a materia.

En caso de avaliación en convocatoria extraordinaria o alumno terá a opción de volver realizar (total ou parcialmente) as seguintes actividades de avaliación:

- Actividades de autoavaliación (test)
- Avaliación de entregables (prácticas)
- Presentacións e/ou exposicións

- Proba escrita

Mentres que a participación en foros incluirase dentro das actividades de autoavaliación

Aquelas actividades que o alumno decida repetir re-avaliaranse, perdendo a nota da convocatoria anterior. A proba escrita realizarase on-line.

A fraude ou intento de fraude por parte do alumno no proceso de avaliación (copia ou plaxio ou facilitalo a terceiros) será penalizado outorgándolle directamente unha calificación de suspenso (0.0) na convocatoria na que se produza.

No caso de que exista algunha diferencia entre as guías en galego/español/inglés relacionada coa avaliación prevalecerá sempre o indicado na guía docente en español.

Bibliografía. Fontes de información

Bibliografía Básica

William Stallings, **Network Security Essentials. Applications and Standards**, 5, Prentice Hall, 2013

Joshua Davies, **Implementing SSL/TLS. Using Cryptography and PKI**, Wiley, 2011

Bibliografía Complementaria

Tanenbaum Andrew, Wetherall David, **Computer Networks**, 5, Prentice Hall, 2010

Stuart McClure, Joel Scambray, George Kurtz, **Hacking exposed 7 network security secrets and solution**, 7, McGraw‐Hill, 2012

Recomendacións

Materias que se recomenda ter cursado previamente

Seguridade da información/P52M182V01106