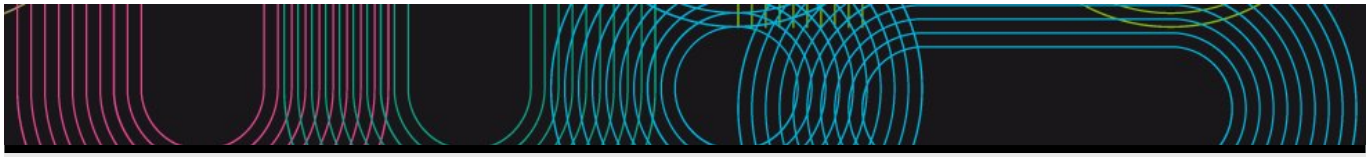

DATOS IDENTIFICATIVOS				
Seguridade da información				
Materia	Seguridade da información			
Código	P52M182V01106			
Titulación	Master Universitario en Dirección TIC para a defensa			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	3	OB	1	1c
Lingua de impartición	Castelán			
Departamento				
Coordinador/a	Rodelgo Lacruz, Miguel			
Profesorado	Rodelgo Lacruz, Miguel			
Correo-e	mrodelgo@cud.uvigo.es			
Web	http://moovi.uvigo.gal			
Descrición xeral	Esta materia persegue dotar ao alumnado dunha formación sobre os conceptos fundamentais da seguridade da información: as ameazas e vulnerabilidades que representan as novas tecnoloxías, os tipos de ataques informáticos máis habituais e as maneiras de protexerse contra eles, os fundamentos usos e aplicacións da criptografía, os métodos de autenticación dos usuarios e a xestión de permisos. As clases de aula utilizaranse para a introdución dos conceptos teóricos, que se complementarán con distintas prácticas de laboratorio.			

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.
B3	CG3 - Dirixir, planificar, coordinar, organizar e/ou supervisar tarefas, proxectos e/ou grupos humanos. Traballar cooperativamente en equipos multidisciplinares actuando, no seu caso, como integrador/a de coñecementos e liñas de traballo.
B6	CG6 - Ser capaz de tomar decisións en contornas caracterizadas pola complexidade e incerteza, avaliando as distintas alternativas existentes co obxectivo de seleccionar aquela cuxo resultado esperado sexa máis favorable, xestionando adecuadamente o risco asociado á decisión.
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.
C9	CE9 - Xestionar a seguridade da información nos aspectos normativo, técnico e metodolóxico.
D5	CT5 - Aprendizaxe e traballo autónomos.

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
RA1 - Relacionar a terminoloxía e os conceptos esenciais, tanto desde o punto de vista conceptual como técnico en materia de seguridade da información.	A6 A7 A8 A9 A10 B1 B6 B7 C9 D5
RA2 - Coñecer as ameazas e vulnerabilidades que representan as novas tecnoloxías, os tipos de ataques informáticos máis habituais e as maneiras de protexerse contra eles.	A6 A7 A8 A9 A10 B1 B3 B6 B7 C9 D5
RA3 - Coñecer os fundamentos, aplicacións e usos da criptografía moderna.	A6 A7 A8 A9 A10 B1 B7 C9 D5
RA4 - Ser capaz de deseñar e avaliar medidas apropiadas para a identificación e autenticación de usuarios, así como a xestión das identidades e as autorizacións asociadas.	A6 A7 A8 A9 A10 B1 B3 B6 B7 C9 D5

Contidos	
Tema	
Definicións, conceptos e principios básicos	- Introdución - Propiedades da seguridade da información - Conceptos básicos - Principios fundamentais. - Novo escenario da ciberdefensa
Ameazas e vulnerabilidades	- Malware - Ameazas de aplicación - Ameazas de rede - Enxeñaría social
Seguridade física	- Ameazas ambientais - Ameazas técnicas - Ameazas de orixe humana - Recuperación de danos e apoio - Integración da seguridade física e lóxica
Seguridade operacional	- Recursos humanos - Operación de sistemas
Técnicas criptográficas	- Criptografía simétrica - Criptografía asimétrica - Hash criptográfico

Identificación e autenticación	- Introdución: Proceso de autenticación, Risco na autenticación. - Métodos de autenticación: Contrasinais, Tokens, Biometría - Autenticación remota - Xestión de identidades
Autorización e control de acceso	- Compoñentes do control de acceso: Autenticación, Autorización e Auditoría. - Protocolos AAA - Políticas de control de accesos: DAC, MAC, RBAC, ABAC. - Federación de identidade

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Estudo previo	0	25	25
Lección maxistral	8	8	16
Prácticas con apoio das TIC	6	0	6
Seminario	1	0	1
Foros de discusión	0	5	5
Exame de preguntas obxectivas	2	0	2
Traballo	0	20	20

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

Metodoloxía docente

	Descrición
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.
Prácticas con apoio das TIC	Actividades de aplicación dos coñecementos nun contexto determinado e de adquisición de habilidades básicas e procedimentais 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	Levarase 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 tutorías individuais co profesor, que se desenvolverán mediante videoconferencia.
Prácticas con apoio das TIC	Aínda que segue sendo posible o uso de mecanismos telemáticos de atención ao alumno, durante neste caso empregaranse tamén mecanismos de tutoría presencial.
Seminario	Aínda que segue sendo posible o uso de mecanismos telemáticos de atención ao alumno, durante neste caso empregaranse tamén mecanismos de tutoría presencial.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe			
Exame de preguntas obxectivas	Proba que avalía o coñecemento e que inclúe preguntas pechadas con diferentes alternativas de resposta (verdadeiro ou falso, elección múltiple, emparellamento de elementos, etc.). Os alumnos/as seleccionan unha resposta de entre un número limitado de posibilidades.	70	A6 A7 A8 A9 A10	B1 B6 B7	C9	D5
Traballo	Texto ou documento elaborado sobre un tema que debe redactarse seguindo unhas normas establecidas de estilo e lonxitude. Permite avaliar as habilidades, os coñecementos e, en menor medida, as actitudes do alumno/a.	30	A6 A7 A8 A9 A10	B1 B3 B7	C9	D5

Outros comentarios sobre a Avaliación

Será necesario sacar o 50% da cualificación para poder superar a materia.

Utilizarase un mecanismo de avaliación continua, co que se pretende realizar un seguimento da evolución do alumno ao longo do curso, valorando o seu esforzo de maneira global. Realizaranse dúas probas escritas: unha ao comezo da fase presencial, na que se avaliarán os contidos impartidos na fase a distancia, que suporá un 20% da cualificación; e unha ao final da fase presencial, na que se avaliarán todos os contidos da materia (incluíndo os contidos da fase a distancia e da presencial), que suporá un 50% da cualificación.
No caso de que o alumno non consiga aprobar a materia na convocatoria ordinaria, terá dereito a unha segunda oportunidade de avaliación (convocatoria extraordinaria) que se realizará na modalidade a distancia nas datas establecidas para ese efecto pola Comisión Académica de Máster. A avaliación consistirá nese caso nunha única proba escrita que suporá o 100% da cualificación, sendo necesario obter polo menos o 50% para superar a materia.
A fraude ou intento de fraude por parte do alumno no proceso de avaliación (copia ou plaxio ou o seu facilitación a terceiros) será penalizado outorgándolle directamente unha cualificación de 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

Bibliografía Complementaria

William, Stallings, **Computer Security: Principles and Practice**, 4ª Ed., Pearson Education India, 2017

White, Gregory, et al., **CompTIA Security+ all-in-one exam guide**, 5ª Ed., McGraw-Hill, Inc., 2018

Centro Criptológico Nacional, **CCN-STIC guides**,

Recomendacións

Outros comentarios

Recoméndase aos alumnos que cursen esta materia ter coñecementos básicos do funcionamento dos sistemas informáticos e as redes de computadores.