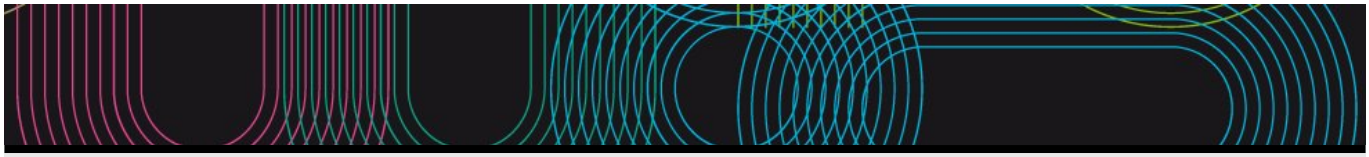

DATOS IDENTIFICATIVOS				
Seguridad de la información				
Asignatura	Seguridad de la información			
Código	P52M182V01106			
Titulacion	Master Universitario en Dirección TIC para la defensa			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OB	1	1c
Lengua Impartición	Castellano			
Departamento				
Coordinador/a	Rodelgo Lacruz, Miguel			
Profesorado	Rodelgo Lacruz, Miguel			
Correo-e	mrodelgo@cud.uvigo.es			
Web	http://moovi.uvigo.gal			
Descripción general	Esta materia persigue dotar al alumnado de una formación sobre los conceptos fundamentales de la seguridad de la información: las amenazas y vulnerabilidades que representan las nuevas tecnologías, los tipos de ataques informáticos más habituales y las maneras de protegerse contra ellos, los fundamentos usos y aplicaciones de la criptografía, los métodos de autenticación de los usuarios y la gestión de permisos. Las clases de aula se utilizarán para la introducción de los conceptos teóricos, que se complementarán con distintas prácticas de laboratorio.			

Resultados de Formación y Aprendizaje	
Código	
A6	CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
A7	CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
A8	CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
A9	CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
A10	CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
B1	CG1 - Poseer conocimientos avanzados y altamente especializados y demostrar una comprensión detallada y fundamentada de los aspectos teóricos y prácticos tratados en las diferentes áreas de estudio.
B3	CG3 - Dirigir, planificar, coordinar, organizar y/o supervisar tareas, proyectos y/o grupos humanos. Trabajar cooperativamente en equipos multidisciplinares actuando, en su caso, como integrador/a de conocimientos y líneas de trabajo.
B6	CG6 - Ser capaz de tomar decisiones en entornos caracterizados por la complejidad e incertidumbre, evaluando las distintas alternativas existentes con el objetivo de seleccionar aquella cuyo resultado esperado sea más favorable, gestionando adecuadamente el riesgo asociado a la decisión.
B7	CG7 - Valorar la importancia de los aspectos de seguridad en la gestión de sistemas e información, identificando necesidades de seguridad, analizando posibles amenazas y riesgos y contribuyendo a la definición y evaluación de criterios y políticas de seguridad.
C9	CE9 - Gestionar la seguridad de la información en los aspectos normativo, técnico y metodológico.
D5	CT5 - Aprendizaje y trabajo autónomos.

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
RA1 - Relacionar la terminología y los conceptos esenciales, tanto desde el punto de vista conceptual como técnico en materia de seguridad de la información.	A6 A7 A8 A9 A10 B1 B6 B7 C9 D5
RA2 - Conocer las amenazas y vulnerabilidades que representan las nuevas tecnologías, los tipos de ataques informáticos más habituales y las maneras de protegerse contra ellos.	A6 A7 A8 A9 A10 B1 B3 B6 B7 C9 D5
RA3 - Conocer los fundamentos, aplicaciones y usos de la criptografía moderna.	A6 A7 A8 A9 A10 B1 B7 C9 D5
RA4 - Ser capaz de diseñar y evaluar medidas apropiadas para la identificación y autenticación de usuarios, así como la gestión de las identidades y las autorizaciones asociadas.	A6 A7 A8 A9 A10 B1 B3 B6 B7 C9 D5

Contenidos	
Tema	
Definiciones, conceptos y principios básicos	- Introducción - Propiedades de la seguridad de la información - Conceptos básicos - Principios fundamentales. - Nuevo escenario de la ciberdefensa
Amenazas y vulnerabilidades	- Malware - Amenazas de aplicación - Amenazas de red - Ingeniería social
Seguridad física	- Amenazas medioambientales - Amenazas técnicas - Amenazas de origen humano - Recuperación de daños y respaldo - Integración de la seguridad física y lógica
Seguridad operacional	- Recursos humanos - Operación de sistemas
Técnicas criptográficas	- Criptografía simétrica - Criptografía asimétrica - Hash criptográfico

Identificación y autenticación	- Introducción: Proceso de autenticación, Riesgo en la autenticación. - Métodos de autenticación: Contraseñas, Tokens, Biometría - Autenticación remota - Gestión de identidades
Autorización y control de acceso	- Componentes del control de acceso: Autenticación, Autorización y Auditoría. - Protocolos AAA - Políticas de control de accesos: DAC, MAC, RBAC, ABAC. - Federación de identidad

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Estudio previo	0	25	25
Lección magistral	8	8	16
Prácticas con apoyo de las TIC	6	0	6
Seminario	1	0	1
Foros de discusión	0	5	5
Examen de preguntas objetivas	2	0	2
Trabajo	0	20	20

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Estudio previo	Búsqueda, lectura, trabajo de documentación y/o realización de forma autónoma de cualquier otra actividad que el alumno/a considere necesaria para permitirle la adquisición de conocimientos y habilidades relacionadas con la materia. Se suele llevar a cabo con anterioridad a las clases, prácticas de laboratorio y/o pruebas de evaluación.
Lección magistral	Exposición por parte de un profesor/a de los contenidos de la materia objeto de estudio, bases teóricas y/o directrices de un trabajo o ejercicio que el/la estudiante tiene de desarrollar.
Prácticas con apoyo de las TIC	Actividades de aplicación de los conocimientos en un contexto determinado y de adquisición de habilidades básicas y procedimentales en relación con la materia, a través del uso de las TIC.
Seminario	Actividad enfocada al trabajo sobre un tema específico, que permite ahondar o complementar en los contenidos de la materia.
Foros de discusión	Actividad desarrollada en un entorno virtual en la que se debate sobre temas diversos y de actualidad relacionados con el ámbito académico y/o profesional.

Atención personalizada

Metodologías	Descripción
Lección magistral	Se llevará a cabo mediante el uso de medios telemáticos. Los alumnos que lo deseen podrán plantear dudas al profesorado en foros o mediante correo electrónico. También podrán concertar tutorías individuales con el profesor, que se desarrollarán mediante videoconferencia.
Prácticas con apoyo de las TIC	Si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante en este caso se emplearán también mecanismos de tutoría presencial.
Seminario	Si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante en este caso se emplearán también mecanismos de tutoría presencial.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Examen de preguntas objetivas	Prueba que evalúa el conocimiento y que incluye preguntas cerradas con diferentes alternativas de respuesta (verdadero o falso, elección múltiple, emparejamiento de elementos, etc.). Los alumnos/as seleccionan una respuesta de entre un número limitado de posibilidades. Durante la fase a distancia se realizarán tres cuestionarios de autoevaluación puntuable (P1, P2, y P3) que abarcarán los bloques I (temas 1, y 2), II (temas 3 y 4) y III (temas 5, 6 y 7), respectivamente, y un cuestionario específico sobre ingeniería social (IS). Al final de la fase presencial se realizará un examen final (EF) que abarca todos los temas teóricos y contenidos prácticos de la materia.	75	A6 A7 A8 A9 A10 B1 B6 B7 C9 D5

Trabajo	Texto o documento elaborado sobre un tema que debe redactarse siguiendo unas normas establecidas de estilo y longitud. Permite evaluar las habilidades, los conocimientos y, en menor medida, las actitudes del alumno/a. Se realizará un trabajo (T) que será evaluado durante la fase a distancia: la actividad T abarca el bloque I (temas 1 y 2).	25	A6 A7 A8 A9 A10	B1 B3 B7	C9	D5

Otros comentarios sobre la Evaluación

Si denominamos MED_CON a la nota media de evaluación continua, que se calcula como:

MED_CON = 0.1*P1 + 0.1*P2 + 0.1*P3 + 0.05*IS + 0.25*T + 0.4*EF.

Para poder superar la asignatura será necesario obtener el 50% de la calificación y al menos un 4 sobre 10 en el examen final. La nota de evaluación continua de los alumnos que no obtengan al menos un 4 sobre 10 en el examen final se calculará como: MED_CON_FINAL = min(4,MED_CON).

En caso de que el alumno no consiga aprobar la asignatura en la convocatoria ordinaria, tendrá derecho a una segunda oportunidad de evaluación (convocatoria extraordinaria) que se realizará en la modalidad a distancia en las fechas establecidas a tal efecto por la Comisión Académica de Máster. La evaluación consistirá en ese caso en una única prueba escrita que supondrá el 100% de la calificación, siendo necesario obtener al menos el 50% para superar la asignatura.

COMPROMISO ÉTICO:

Se espera que el alumnado tenga un comportamiento ético adecuado, comprometiéndose a actuar con honestidad. En base al artículo 42.1 del Reglamento sobre la evaluación, la calificación y la calidad de la docencia y del proceso de aprendizaje del estudiantado de la Universidad de Vigo, **la utilización de procedimientos fraudulentos en pruebas de evaluación, así como la cooperación en ellos implicará la calificación de cero (suspenso) en el acta de la convocatoria correspondiente**, con independencia del valor que sobre la calificación global tuviese la prueba en cuestión y sin perjuicio de las posibles consecuencias de índole disciplinaria que puedan producirse.

En el caso de que exista alguna diferencia entre las guías en galego/español/inglés relacionada con la evaluación prevalecerá siempre lo indicado en la guía docente en español.

Fuentes 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**,

Recomendaciones

Otros comentarios

Se recomienda a los alumnos que cursen esta asignatura tener conocimientos básicos del funcionamiento de los sistemas informáticos y las redes de ordenadores.