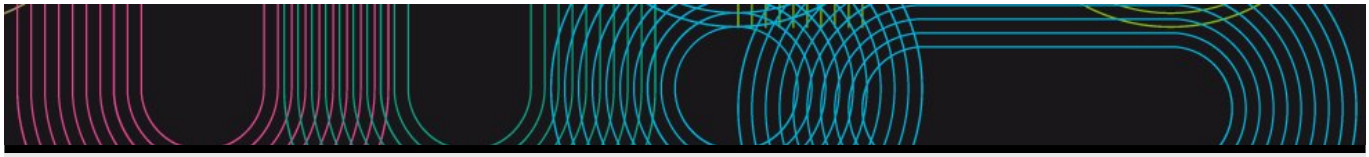

DATOS IDENTIFICATIVOS				
Gestión de la seguridad de la información				
Asignatura	Gestión de la seguridad de la información			
Código	V05M175V01101			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OB	1	1c
Lengua Impartición	Castellano Gallego			
Departamento				
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel Dafonte Vázquez, José Carlos Fernández Vilas, Ana			
Correo-e	mcaeiro@det.uvigo.es			
Web	http://faitic.uvigo.es			
Descripción general	En esta asignatura se introducen los conceptos fundamentales relacionados con la gestión de la seguridad de la información (e.g. vulnerabilidad, amenaza, riesgo) y se estudian las metodologías, herramientas y especificaciones que se ocupan del análisis de riesgos y del desarrollo de sistemas de gestión de seguridad de la información.			

Competencias	
Código	
A2	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
A3	Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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.
B1	Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación
B2	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones.
C5	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia
C7	Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros
C13	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
D5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Conocer los conceptos fundamentales relacionados con la Gestión de la Seguridad de la Información: vulnerabilidad, amenaza, riesgo, contramedida, política de seguridad, plan de seguridad, auditoría	A2 A3 D4 D5

Conocer las diferentes metodologías de Gestión de Seguridad de la Información, comúnmente aceptadas	B1 B2 C5 D5
Conocer las herramientas propias para llevar a cabo tareas relacionadas con el análisis de riesgos y la auditoría de seguridad, así como saber cuáles son las más adecuadas a cada entorno	B1 B2 C7 C13 D5

Contenidos

Tema	
Fundamentos	Conceptos básicos: Confidencialidad, Integridad, Disponibilidad, amenaza, riesgo, etc. Marco legal de la ciberseguridad Normalización: estándares y especificaciones Centros de operaciones de seguridad
Análisis de riesgos, gestión y certificación	ISO 27005 e ISO 31000 Metodologías y herramientas de análisis de riesgos Estrategia Nacional de Seguridad
Sistemas de Gestión de Seguridad de la Información	ISO27000, 27001 y 27002 Esquema Nacional de Evaluación y Certificación de las Tecnologías de la Información Clasificación de información Formación y concienciación
Impacto de negocio	Roles de ciberseguridad Secuencia típica de un ataque Resilencia Gestión de la continuidad del negocio Plan de contingencia
Auditoría de seguridad	Objetivos de control Marcos y estándares para la auditoría Auditoría de seguridad de los datos personales Delegado de protección de datos

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Lección magistral	19.5	39	58.5
Prácticas de laboratorio	18	57	75
Examen de preguntas objetivas	1.5	3	4.5
Estudio de casos	3	9	12

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

Metodologías

	Descripción
Lección magistral	Presentación por parte del profesorado del temario de la materia. Con esta metodología se trabajan las competencias: CE5, CE7, CE13, CT4 y CT5.
Prácticas de laboratorio	En el laboratorio se desarrollarán prácticas guiadas y se plantearán casos de estudio prácticos. Con esta metodología se trabajarán las competencias CB2, CB3, CG1, CG2, CE5, CE7, CE13 y CT5.

Atención personalizada

Metodologías	Descripción
Lección magistral	El profesorado de la asignatura proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial o en línea (durante la propia sesión magistral, o durante lo horario establecido para las tutorías). El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Prácticas de laboratorio	El profesorado de la materia proporcionará atención individual y personalizada al alumnado durante el curso, solucionando sus dudas y preguntas. Así mismo, el profesorado orientará y guiará al alumnado durante la realización de las tareas que tienen asignadas en las prácticas de laboratorio. Las dudas se atenderán de forma presencial (durante las prácticas, o durante el horario establecido para tutorias). El horario de tutorias se establecerá al principio del curso y se publicará en la página web de la asignatura.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje			
Examen de preguntas objetivas	Examen de conocimientos teóricos y de desarrollo práctico	70		B1 B2	C5 C7 C13	D4 D5
Estudio de casos	Se desarrollarán ejercicios de casos prácticos sobre el análisis de riesgos y la realización de planes de seguridad	30	A2 A3		C5 C7 C13	D5

Otros comentarios sobre la Evaluación

Los estudiantes pueden decidir ser evaluados según un modelo de evaluación continua o bien de evaluación única. Todos los alumnos que entreguen el primer estudio de casos están optando por la evaluación continua. Una vez los estudiantes opten por el modelo de evaluación continua su calificación no podrá ser nunca "No presentado".

La calificación será el resultado de aplicar la media ponderada entre os resultados: (i) examen escrito (70%) , y (ii) estudio de casos (30%).

Examen escrito: tendrá lugar en las fechas publicadas en el calendario oficial.

Parte práctica:

1- Modelo de evaluación continua. Un informe de 2 casos prácticos que se entregarán en las semanas indicadas en el documento que se facilitará a los alumnos el primer día de clase. Esta actividad se desarrollará en grupo y todos los alumnos del mismo grupo recibirán la misma calificación.

2- Modelo de evaluación única. Entrega del informe de los dos casos prácticos en la misma fecha del examen escrito publicado en el calendario oficial.

En la evaluación en segunda oportunidad los estudiantes serán evaluados utilizando la modalidad de evaluación única.

Si se detecta plagio en cualquiera de las pruebas de evaluación, la calificación final de la asignatura será de "suspenso (0)", hecho que se comunicará a la dirección de la escuela para adoptar las medidas oportunas.

Fuentes de información

Bibliografía Básica

Campbell, Tony, **Practical Information Security Management: A Complete Guide to Planning and Implementation**, Apress, 2016

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Especificaciones. (ISO 22301:2012).**, AENOR, 2015

UNE-EN ISO, **Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Directrices. (ISO 22313:2012).**, AENOR, 2015

UNE-EN ISO, **Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)**, AENOR, 2017

UNE-EN ISO, **Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).**, AENOR, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (ISO/IEC 27000:2018)**, ISO/IEC, 2018

ISO/IEC, **Information technology -- Security techniques -- Information security management systems -- Guidance (ISO/IEC 27003:2017)**, ISO/IEC, 2017

ISO/IEC, **Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation (ISO/IEC 27004:2016)**, ISO/IEC, 2016

ISO/IEC, **Information technology -- Security techniques -- Information security risk management (ISO/IEC 27005:2011)**, ISO/IEC, 2011

Bibliografía Complementaria

Gómez Fernández, Luis y Fernández Rivero, Pedro Pablo, **Como implantar un SGSI según UNE-ISI/IEC 27001:2014 y su aplicación en el ENS**, AENOR, 2015

Fernández Sánchez, Carlos Manuel y Piatiini Velthuis, Mario, **Modelo para el gobierno de las TIC basado en las normas ISO**, AENOR, 2012

ISO, **Risk management -- Principles and guidelines (ISO/IEC 31000:2009)**, ISO, 2009

Alan Calder Steve Watkins, **IT Governance: An International Guide to Data Security and ISO27001/ISO27002**, 5, Kogan Page, 2012

Alan Calder, **Nine Steps to Success - North American edition: An ISO 27001:2013 Implementation Overview**, 1, IT Governance Publishing, 2017

Edward Humphreys, **Implementing the ISO / IEC 27001 ISMS Standard**, 2, Artech House, 2016

Recomendaciones