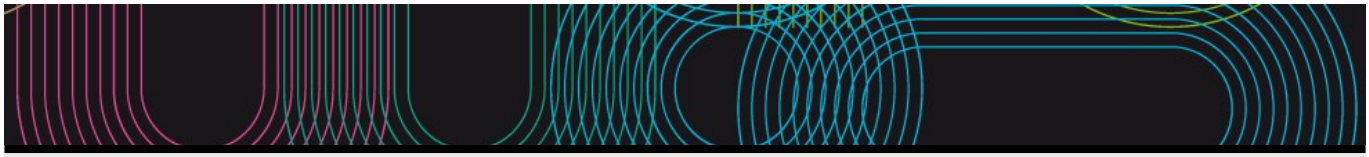

DATOS IDENTIFICATIVOS				
Xestión da seguridade da información				
Materia	Xestión da seguridade da información			
Código	V05M175V01101			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OB	1	1c
Lingua de impartición	Castelán Galego			
Departamento				
Coordinador/a	Caeiro Rodríguez, Manuel			
Profesorado	Caeiro Rodríguez, Manuel Fernández Vilas, Ana López Rivas, Antonio Daniel			
Correo-e	mcaeiro@det.uvigo.es			
Web	http://moovi.uvigo.es			
Descrición xeral	Nesta materia introdúcense os conceptos fundamentais relacionados coa xestión da seguridade da información (e.g. vulnerabilidade, ameaza, risco) e estúdanse as metodoloxías, ferramentas e especificacións que se ocupan da análise de riscos e do desenvolvemento de sistemas de xestión de seguridade da información.			

Competencias	
Código	
A2	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 más amplos (ou multidisciplinares) relacionados coa súa área de estudo
A3	Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar 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.
B1	Ter capacidade de análisis e síntesis. Ter capacidade para proxectar, modelar, calcular e diseñar solucións de seguridade da información, as redes e/ou os sistemas de comunicacións en todos os ámbitos de aplicación
B2	Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións.
C5	Deseñar, implantar e manter un sistema de xestión da seguridade da información utilizando metodoloxías de referencia
C7	Ter capacidade para realizar a auditoría de seguridade de sistemas e instalacións, o análisis de riscos derivados de debilidades de ciberseguridade e desenvolver o proceso de certificación de sistemas seguros
C13	Ter capacidade de análisis, detección e eliminación de vulnerabilidades, e do malware susceptible de utilizalas, en sistemas e redes
D4	Valorar a importancia da seguridade da información no avance socioeconómico da sociedade
D5	Ter capacidade para comunicarse oralmente e por escrito en inglés.

Resultados de aprendizaxe	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Coñecer os conceptos fundamentais relacionados coa Xestión da Seguridade da Información: vulnerabilidade, ameaza, risco, contramedida, política de seguridade, plan de seguridade, auditoría	A2 A3 D4 D5

Coñecer as diferentes metodoloxías de Xestión de Seguridade da Información, comúnmente aceptadas	B1 B2 C5 D5
Coñecer as ferramentas propias para levar a cabo tarefas relacionadas coa análise de riscos e a auditoría de seguridade, así como saber cales son as máis adecuadas a cada contorna	B1 B2 C7 C13 D5

Contidos	
Tema	
Fundamentos	Conceptos básicos: Confidencialidade, Integridade, Dispoñibilidade, ameaza, risco, etc. Marco legal da ciberseguridade Normalización: estándares e especificacións Centros de operacións de seguridade
Análise de riscos, xestión e certificación	ISO 27005 e ISO 31000 Metodoloxías e ferramentas de análises de riscos Estratexia Nacional de Seguridade
Sistemas de Xestión de Seguridade da Información	ISO27000, 27001 y 27002 Esquema Nacional de Avaliación e Certificación das Tecnoloxías da Información Clasificación de información Formación e concienciación
Impacto de negocio	Roles de ciberseguridade Secuencia típica dun ataque Resilencia Xestión da continuidade do negocio Plan de continxencia
Auditoría de seguridade	Obxectivos de control Marcos e estándares para a auditoría Auditoría de seguridade dos datos persoais Delegado de protección de datos

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Lección maxistral	19	29	48
Traballo tutelado	0.5	10	10.5
Prácticas de laboratorio	18	57	75
Exame de preguntas obxectivas	1.5	3	4.5
Estudo de casos	3	9	12

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

Metodoloxía docente	
	Descrición
Lección maxistral	Presentación por parte do profesorado do temario da materia. Con esta metodoloxía trabállanse as competencias: CE5, CE7, CE13, CT4 e CT5.
Traballo tutelado	Cada alumno de forma individual realizará un traballo sobre un dos temas da materia a presentar no grupo A. Con esta metodoloxía traballaranse as competencias CG1, CG2, CT4 e CT5.
Prácticas de laboratorio	No laboratorio desenvolveranse prácticas guiadas e suscitaranse casos de estudo prácticos. Con esta metodoloxía traballaranse as competencias CB2, CB3, CG1, CG2, CE5, CE7, CE13 e CT5.

Atención personalizada	
Metodoloxías	**Descrición**
Lección maxistral	O profesorado da materia proporcionará atención individual e personalizada ao alumnado durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial ou en liña (durante a propia sesión maxistral, ou durante o horario establecido para as titorías). O horario de titorías establecerase ao principio do curso e publicarase na páxina web da materia.

Prácticas de laboratorio	O profesorado da materia proporcionará atención individual e personalizada ao alumnado durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que teñen asignadas nas prácticas de laboratorio. As dúbidas atenderanse de forma presencial (durante as prácticas, ou durante o horario establecido para titorias). O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.
Traballo tutelado	O profesorado da materia proporcionará atención individual e personalizada ao alumnado durante o curso, solucionando as súas dúbidas e preguntas. Así mesmo, o profesorado orientará e guiará ao alumnado durante a realización das tarefas que teñen asignadas nas prácticas de laboratorio. As dúbidas atenderanse de forma presencial (durante as prácticas, ou durante o horario establecido para titorias). O horario de titorias establecerase ao principio do curso e publicarase na páxina web da materia.

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe		
Traballo tutelado	Cada alumno de forma individual realizará un traballo sobre un dos temas da materia a presentar no grupo A	10	B1 B2		D4 D5
Exame de preguntas obxectivas	Exame de coñecementos teóricos e de desenvolvemento práctico	50	B1 B2	C5 C7 C13	D4 D5
Estudo de casos	Desenvolveranse exercicios de casos prácticos sobre a análise de riscos e a realización de plans de seguridade	40	A2 A3	C5 C7 C13	D5

Outros comentarios sobre a Avaliación

Os estudantes poden decidir ser avaliados segundo un modelo de avaliación continua ou ben de avaliación única. Tódolos alumnos que entreguen o primeiro dos estudos de casos están optando pola avaliación continua. Unha vez os estudantes opten polo modelo de avaliación continua a súa cualificación non poderá ser nunca "Non presentado".

No modelo de avaliación continua a cualificación será o resultado de aplicar a media ponderada entre os resultados: (i) exame escrito (50%), (ii) estudo de casos (40%) e (iii) traballo tutelado (10%).

No modelo de avaliación única a cualificación será o resultado de aplicar a media ponderada entre os resultados: (i) exame escrito (50%), (ii) estudio de casos (50%).

Exame escrito:

Terá lugar nas datas publicadas no calendario oficial. Incluirá preguntas sobre os contidos e os casos prácticos.

Parte práctica:

1- Modelo de avaliación continua. Sendos informes de 2 casos prácticos e 2 avaliacións de informes de compañeiros que se entregarán nas semanas indicadas no documento que se facilitará aos alumnos o primeiro día de clase. Un informe será sobre análise de riscos e o outro sobre o desenvolvemento dun plan de seguridade (SGSI). Cada informe tenrá un peso na nota final do 15% e cada avaliación do 5%. Os informes desenvolveranse en grupo e todos os alumnos do mesmo grupo recibirán ea mesma cualificación. As avaliacións realizaranse de forma individual. Tamén é necesario realizar un traballo tutelado sobre un tema da asignatura a presentar no grupo A.

2- Modelo de avaliación única. Entrega individual de 2 informes dos dous casos prácticos na mesma data do exame escrito publicado no calendario oficial. Neste caso non se realizará a avaliación de informes de compañeiros e cada informe tenrá un peso na nota final do 25%.

Na avaliación en segunda oportunidade os estudantes serán avaliados utilizando a modalidade de avaliación única.

Si se detectase plaxio en calquera das probas de avaliación, a cualificación final da materia será de "suspenso (0)", feito que se comunicará á dirección da escola para adoptar as medidas oportunas.

Bibliografía. Fontes 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

Recomendacións