



DATOS IDENTIFICATIVOS

Xestión da seguridade e análise de riscos

Materia	Xestión da seguridade e análise de riscos			
Código	P52M182V01107			
Titulación	Master Universitario en Dirección TIC para a defensa			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	4	OB	1	1c
Lingua de impartición	Castelán			
Departamento				
Coordinador/a	Fernández Gavilanes, Milagros			
Profesorado	Fernández Gavilanes, Milagros López Román, Iago			
Correo-e	mfgavilanes@tud.uvigo.es			
Web	http://campus.defensa.gob.es https://moovi.uvigo.gal			
Descrición xeral	A materia de Xestión da Seguridade e Análise de Riscos pretende ofrecer aos alumnos unha visión xeral dos Sistemas de Xestión da Seguridade da Información (SXS), coa descrición dos fundamentos dos estándares existentes para a certificación dun SXS, e prestando especial atención ás metodoloxías de análises e xestión de riscos, así como aos plans de resposta a incidentes de seguridade.			

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.
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.
D6	CT6 - Manexar apropiadamente recursos de información.

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
RA1. Entender o concepto de Xestión de Riscos e valorar a súa importancia nos Sistemas TIC.	A6 A7 A8 A9 A10 B1 B2 B6 B7 C9 D6
RA2. Comprender as características o proceso de certificación dun SXSI.	A9 A10 B1 B7 C9 D6
RA3. Estudar as metodoloxías e ferramentas dispoñibles para analizar e xestionar os riscos.	A7 A10 B1 B3 B6 B7 C9 D6
RA4. Coñecer a política e xestión da seguridade da información no MINISDEF e as recomendacións emitidas polo CCN.	A10 B7 C9 D6
RA5. Valorar o alcance e a metodoloxía que deben seguir as auditorías de seguridade de sistemas TIC.	A7 A8 A9 A10 B2 B6 B7 C9 D6
RA6. Entender como se pode levar a cabo unha correcta xestión de incidentes de seguridade.	A7 A8 A10 B2 B6 B7 C9 D6

Contidos

Tema	
Tema 1: Introducción á Xestión da Seguridade da Información	- A importancia estratéxica da información e os activos dixitais - O proceso de xestión da seguridade da información. - Definición de Políticas, Plans e Procedementos de Seguridade. - Os profesionais da Seguridade da Información: Competencias, formación e certificacións.
Tema 2: Análise e Xestión de Riscos	- O proceso de identificación, análise e avaliación de riscos. - Revisión das principais vulnerabilidades e tipos de ataques a sistemas informáticos. - Tratamento dos riscos. - Metodoloxía MAGERIT. - O modelo proposto pola ISO 31000.

Tema 3: Sistema de Xestión de Seguridade da Información	<ul style="list-style-type: none"> - Características dun SXXI. - Certificacións e estándares de seguridade: ISO 27001 e ENS. - Política e xestión da seguridade da información no MINISDEF. - Normativa STIC do CCN.
Tema 4: Auditorías de seguridade e resposta a incidentes	<ul style="list-style-type: none"> - O proceso de auditoría da seguridade da información. - Xestión de incidentes de seguridade.
Tema 5: A importancia do factor humano na seguridade da información	<ul style="list-style-type: none"> - Aspectos a considerar relacionados co factor humano e a seguridade. - Técnicas de Enxeñaría Social. - Ataques de Phishing. - Definición de políticas de uso seguro e aceptable dos recursos informáticos.

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Resolución de problemas de forma autónoma	0	5	5
Estudo previo	0	55	55
Lección maxistral	16	8	24
Resolución de problemas	2	2	4
Foros de discusión	0	5	5
Autoavaliación	0	3	3
Presentación	3	0	3
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.
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	Exponse dous métodos de atención personalizada: (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	Exponse dous métodos de atención personalizada: (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

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 A10	C9 D6
Autoavaliación	Mecanismo no que, por medio dunha serie de preguntas ou actividades, posibilitase 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.	20		B1 C9 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.	35	A7 A8 A9 A10	B1 B2 C9 B3 D6 B6 B7
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.	35	A10	B1 C9 D6

Outros comentarios sobre a Avaliación

Para superar a materia será necesario alcanzar unha cualificación do 50% ou superior no conxunto das avaliacións da materia.

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 en modalidade a distancia nas datas establecidas para ese efecto pola Comisión Académica de Máster. O proceso de avaliación en convocatoria extraordinaria será o mesmo que en convocatoria ordinaria. A presentación e a proba escrita realizaranse utilizando medios telemáticos. O alumno terá a opción de gardar as cualificacións obtidas na convocatoria ordinaria durante o mesmo curso académico.

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 cualificación de suspenso (0.0) na convocatoria. (Sen prexuízo das posibles medidas que poida tomar a universidade fronte a estes casos.

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

Bibliografía. Fontes de información

Bibliografía Básica

Bibliografía Complementaria

Fernández, C. Manuel., Piattini, M., y Peso, E., **Auditoría Informática: Un enfoque práctico**, 2, Ra-Ma, 2000

Merino Bada, C. y Cañizares Sales, R., **Implantación de un sistema de gestión de seguridad de la información según ISO 27001**, 1, Fundación Confemetal, 2011

Talabis, M. y Martin, J., **Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis**, 1, Syngress, 2012

Tipton, H. F. and Micki K., **Information Security Management Handbook**, 5, Auerbach Publications, 2004

Recomendacións

Materias que se recomenda cursar simultaneamente

Sistemas de información/P52M182V01105