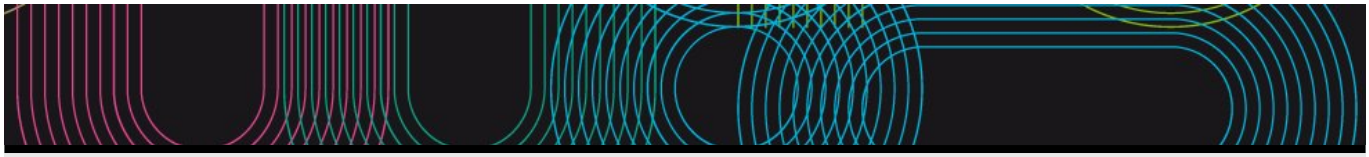

DATOS IDENTIFICATIVOS				
Gestión de la seguridad y análisis de riesgos				
Asignatura	Gestión de la seguridad y análisis de riesgos			
Código	P52M182V01107			
Titulacion	Master Universitario en Dirección TIC para la defensa			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	4	OB	1	1c
Lengua Impartición	Castellano			
Departamento				
Coordinador/a	Fernández Gavilanes, Milagros			
Profesorado	Fernández Gavilanes, Milagros López Román, Iago			
Correo-e	mfgavilanes@cud.uvigo.es			
Web	http://campus.defensa.gob.es | https://moovi.uvigo.gal			
Descripción general	La asignatura de Gestión de la Seguridad y Análisis de Riesgos pretende ofrecer a los alumnos una visión general de los Sistemas de Gestión de la Seguridad de la Información (SGSI), con la descripción de los fundamentos de los estándares existentes para la certificación de un SGSI, y prestando especial atención a las metodologías de análisis y gestión de riesgos, así como a los planes de respuesta a incidentes de seguridad.			

Competencias	
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.
B2	CG2 - Integrar y aplicar los conocimientos adquiridos, y poseer capacidad de resolución de problemas en entornos nuevos o definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar relacionados con su ámbito 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.

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
RA1. Entender el concepto de Gestión de Riesgos y valorar su importancia en los Sistemas TIC.	A6 A7 A8 A9 A10 B1 B2 B6 B7 C9 D6
RA2. Comprender las características el proceso de certificación de un SGSI.	A9 A10 B1 B7 C9 D6
RA3. Estudiar las metodologías y herramientas disponibles para analizar y gestionar los riesgos.	A7 A10 B1 B3 B6 B7 C9 D6
RA4. Conocer la política y gestión de la seguridad de la información en el MINISDEF y las recomendaciones emitidas por el CCN.	A10 B7 C9 D6
RA5. Valorar el alcance y la metodología que deben seguir las auditorías de seguridad de sistemas TIC.	A7 A8 A9 A10 B2 B6 B7 C9 D6
RA6. Entender cómo se puede llevar a cabo una correcta gestión de incidentes de seguridad.	A7 A8 A10 B2 B6 B7 C9 D6

Contenidos	
Tema	
Tema 1: Introducción a la Gestión de la Seguridad de la Información	- La importancia estratégica de la información y los activos digitales - El proceso de gestión de la seguridad de la información. - Definición de Políticas, Planes y Procedimientos de Seguridad. - Los profesionales de la Seguridad de la Información: Competencias, formación y certificaciones.
Tema 2: Análisis y Gestión de Riesgos	- El proceso de identificación, análisis y evaluación de riesgos. - Revisión de las principales vulnerabilidades y tipos de ataques a sistemas informáticos. - Tratamiento de los riesgos. - Metodología MAGERIT. - El modelo propuesto por la ISO 31000.

Tema 3: Sistema de Gestión de Seguridad de la Información	- Características de un SGSI. - Certificaciones y estándares de seguridad: ISO 27001 y ENS. - Política y gestión de la seguridad de la información en el MINISDEF. - Normativa STIC del CCN.
Tema 4: Auditorías de seguridad y respuesta a incidentes	- El proceso de auditoría de la seguridad de la información. - Gestión de incidentes de seguridad.
Tema 5: La importancia del factor humano en la seguridad de la información	- Aspectos a considerar relacionados con el factor humano y la seguridad. - Técnicas de Ingeniería Social. - Ataques de Phishing. - Definición de políticas de uso seguro y aceptable de los recursos informáticos.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Resolución de problemas de forma autónoma	0	5	5
Estudio previo	0	55	55
Lección magistral	16	8	24
Resolución de problemas	2	2	4
Foros de discusión	0	5	5
Autoevaluación	0	3	3
Presentación	3	0	3
Examen de preguntas de desarrollo	1	0	1

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

Metodologías

	Descripción
Resolución de problemas de forma autónoma	Actividad en la que el alumnado analiza y resuelve problemas y/o ejercicios relacionados con la materia de forma autónoma.
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.
Resolución de problemas	Actividad en la que se formulan problemas y/o ejercicios relacionados con la materia. El alumno/a debe desarrollar las soluciones adecuadas y correctas mediante la ejercitación de rutinas, aplicación de fórmulas o algoritmos, la aplicación de procedimientos de transformación de la información disponible y la interpretación de los resultados.
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 plantean dos métodos de atención personalizada: (1) Atención en la fase a distancia: 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. (2) Atención en la fase presencial: si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante esta fase se emplearán también mecanismos de tutoría presencial.
Resolución de problemas	Se plantean dos métodos de atención personalizada: (1) Atención en la fase a distancia: 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. (2) Atención en la fase presencial: si bien sigue siendo posible el uso de mecanismos telemáticos de atención al alumno, durante esta fase se emplearán también mecanismos de tutoría presencial.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje

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. Permite evaluar las habilidades, los conocimientos y, en menor medida, las actitudes del alumno/a. Se evaluará la participación en los foros.	10	A6 A7 A10		C9	D6
Autoevaluación	Mecanismo en el que, por medio de una serie de preguntas o actividades, se posibilita que el alumno/a evalúe de manera autónoma su grado de adquisición de conocimientos y habilidades sobre la materia, permitiendo una autorregulación del proceso de aprendizaje personal.	20		B1	C9	D6
Presentación	Exposición por parte del alumnado, de manera individual o en grupo, de un tema relacionado con los contenidos de la materia o de los resultados de un trabajo, ejercicio, proyecto, etc. A través de la presentación se pueden evaluar conocimientos, habilidades y actitudes.	35	A7 A8 A9 A10	B1 B2 B3 B6 B7	C9	D6
Examen de preguntas de desarrollo	Prueba de evaluación que incluye preguntas abiertas y/o ejercicios, sobre un tema. Los alumnos/as deben desarrollar, relacionar, organizar y presentar los conocimientos que tengan sobre la materia en una respuesta argumentada. Se puede utilizar para evaluar conocimientos y habilidades.	35	A10	B1	C9	D6

Otros comentarios sobre la Evaluación

Para superar la asignatura será necesario alcanzar una calificación del 50% o superior en el conjunto de las evaluaciones de la asignatura.

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 modalidad a distancia en las fechas establecidas a tal efecto por la Comisión Académica de Máster. El proceso de evaluación en convocatoria extraordinaria será mediante la realización de un examen final.
El fraude o intento de fraude por parte del alumno en el proceso de evaluación (copia o plagio o su facilitación a terceros) será penalizado otorgándole directamente una calificación de suspenso (0.0) en la convocatoria. (Sin perjuicio de las posibles medidas que pueda tomar la universidad frente a estos casos.
En el caso de que exista alguna diferencia entre las guías en gallego/español relacionada con la evaluación prevalecerá siempre lo indicado en la guía docente en español.

Fuentes 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

Recomendaciones

Asignaturas que se recomienda cursar simultáneamente

Sistemas de información/P52M182V01105