



Guía Docente				
Datos Identificativos				2018/19
Asignatura (*)	Xestión de Incidentes	Código	614530015	
Titulación	Máster Universitario en Ciberseguridade			
Descritores				
Ciclo	Período	Curso	Tipo	Créditos
Mestrado Oficial	2º cuatrimestre	Primeiro	Optativa	3
Idioma	CastelánGalego			
Modalidade docente	Presencial			
Prerrequisitos				
Departamento	Computación			
Coordinación	Dafonte Vazquez, Jose Carlos	Correo electrónico	carlos.dafonte@udc.es	
Profesorado	Dafonte Vazquez, Jose Carlos Gomez Garcia, Angel	Correo electrónico	carlos.dafonte@udc.es angel.gomez@udc.es	
Web	www.munics.es			
Descrición xeral	A xestión de incidentes de ciberseguridade céntrase no manexo da proactividade para previr e atenuar posibles consecuencias. Acadarase o coñecemento necesario sobre as ferramentas que poidan facilitar a xestión dos incidentes e as recuperacións, a xustificación dos plans propostos para a recuperación e resiliencia, a identificación e clasificación dos posibles incidentes e a definición das canles para a súa xestión e resolución.			

Competencias do título	
Código	Competencias do título
A3	CE3 - Coñecer a normativa técnica e legal de aplicación en materia de ciberseguridade, as súas implicacións no deseño de sistemas, no uso de ferramentas de seguridade e na protección da información
A9	CE9 - Ter capacidade para elaborar plans e proxectos de traballo no ámbito da ciberseguridade, claros, concisos e razoados
A14	CE14 - Ter capacidade para desenvolver un plan de continuidade de negocio seguindo normas e estándares de referencia
A15	CE15 - Ter capacidade de identificar o valor, tanto económico como doutra índole, da información da institución, os seus procesos críticos e o impacto que produciría a interrupción destes; e, tamén, as necesidades internas e externas que permitirán estar preparados ante ataques de seguridade
A17	CE17 - Ter capacidade de planificar no tempo os periodos de detección de incidentes ou desastres, e a súa recuperación
B2	CB2 - 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
B3	CB3 - 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
B5	CB5 - 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
B6	CG1 - Ter capacidade de análise 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
B10	CG5 - Ter capacidade para aplicar os coñecementos teóricos na práctica, no marco de infraestruturas, equipamentos e aplicacións concretos, e suxeitos a requisitos de funcionamento específicos
C4	CT4 - Valorar a importancia da seguridade da información no avance socioeconómico da sociedade

Resultados da aprendizaxe	
Resultados de aprendizaxe	Competencias do título



Manexar a proactividade para prever e atenuar posibles incidentes de seguridade	AP9 AP14 AP17	BP2 BP3 BP5 BP6 BP10	CP4
Obter o coñecemento necesario sobre ferramentas que poidan facilitar a xestión dos incidentes e as recuperacións	AP3 AP14 AP17	BP2 BP3 BP5 BP6 BP10	
Xustificar os plans propostos para recuperación e resiliencia	AP3 AP9 AP14 AP15	BP2 BP3 BP5 BP6 BP10	CP4
Identificar e clasificar os posibles incidentes e definir as canles para a súa xestión e resolución	AP3 AP9 AP17	BP2 BP3 BP5 BP6 BP10	CP4

Contidos	
Temas	Subtemas
1. Fundamentos: resiliencia e o valor da información	1.1. Introducción 1.2. Fundamentos
2. Detección de incidentes e xestión de resposta	2.1. Detección e notificación de incidentes 2.2. Xestión de resposta, contención e mitigación do impacto
3. Estándares: plans de continuidade e de recuperación	3.1. Estándares ISO/IEC 3.2. Directrices para a xestión de incidentes
4. Recuperación de desfeitas	4.1. Mecanismos 4.2. Fases de recuperación 4.3. Protección de infraestruturas críticas
5. Lexislación	5.1. Lexislación específica: Esquema Nacional de Seguridade, Estrategia de Ciberseguridade Nacional

Planificación				
Metodoloxías / probas	Competencias	Horas presenciais	Horas non presenciais / traballo autónomo	Horas totais
Prácticas de laboratorio	A9 A14 A17 B2 B3 B10	11	27.5	38.5
Sesión maxistral	A3 A14 A15 A17 B5 B6 C4	8	16	24
Traballos tutelados	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	1	9	10
Proba obxectiva	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	2.5	0	2.5
Atención personalizada		0		0

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



Metodoloxías

Metodoloxías	Descrición
Prácticas de laboratorio	Sesións prácticas en computador asociadas a escenarios de incidencias e manexo de ferramentas para ciberincidentes. O obxectivo é poñer en práctica os coñecementos das sesións maxistrais fomentando o aprendizaxe autónomo.
Sesión maxistral	Docencia expositiva. Presentacións dos coñecementos teóricos dos temas da asignatura promovendo a interacción cos estudantes.
Traballos tutelados	Traballo a desenvolver polo alumno sobre algunha das temáticas da asignatura a proposta do propio estudante ou do profesor. Este traballo terá seguimento por parte do profesorado e o estudante fará unha breve defensa presencial do mesmo.
Proba obxectiva	Proba escrita para valorar os coñecementos adquiridos. Aínda que se centrará no material da docencia expositiva, poderá incorporar algunhas cuestións relacionadas coas sesións prácticas.

Atención personalizada

Metodoloxías	Descrición
Prácticas de laboratorio Traballos tutelados	A atención personalizada está enfocada a apoiar ó alumno na comprensión das diferentes técnicas mediante o apoio nas tutorías e a resolución de dúbidas que podan xurdir nas clases maxistrais. Tamén se lle prestará axuda nas dúbidas que poidan xurdir durante a realización das prácticas e a aprendizaxe mediante traballos tutelados para un mellor aproveitamento e comprensión dos coñecementos acadados na clase.

Avaliación

Metodoloxías	Competencias	Descrición	Cualificación
Prácticas de laboratorio	A9 A14 A17 B2 B3 B10	Sesións prácticas en computador asociadas a escenarios de incidencias e manexo de ferramentas para ciberincidentes. O obxectivo é poñer en práctica os coñecementos das sesións maxistrais fomentando o aprendizaxe autónomo. A avaliación será continua perante as sesións. NOTA: Será posible utilizar algunha das sesións presenciais para realizar algún taller dunha entidade colaboradora.	30
Traballos tutelados	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	Traballo a desenvolver polo alumno sobre algunha das temáticas da asignatura a proposta do propio estudante ou do profesor. Este traballo terá seguimento por parte do profesorado e o estudante fará unha breve defensa presencial do mesmo.	20
Proba obxectiva	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	Proba escrita para valorar os coñecementos adquiridos. Aínda que se centrará no material da docencia expositiva, poderá incorporar algunhas cuestións relacionadas coas sesións prácticas.	50

Observacións avaliación

Para superar a materia, será preciso obter un mínimo de 5 sobre 10 tanto na prueba obxectiva como nos traballos prácticos. En caso contrario, a nota máxima que se poderá obter será de 4.5. ESTUDANTES CON MATRÍCULA A TEMPO PARCIAL OU CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA: Deberán poñerse en contacto cos profesores da asignatura para posibilitar a realización das tarefas fóra da organización habitual de materia.
--

Fontes de información



Bibliografía básica	- ISO/IEC 27035:2016 - Information technology - Security techniques - Information security incident management. http://www.iso27001security.com/html/27035.html - Gestión de incidentes de seguridad informática, Álvaro Gómez Vieites, 978-84-92650-77-4, RA-MA Editorial, 2014- Gestión de incidentes de seguridad informática (MF0488_3), Ester Chicano Tejada, 978-84-16351-70-1, IC Editorial, 2014- Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad, Luis Gómez Fernández y Pedro Pablo Fernández Rivero, 978-84-81439-63-2 AENOR, 2018- Sistema de Información para gestionar un SGSI basado en ISO 27001:2013: Cómo tener trazabilidad de un Sistema de Gestión de Seguridad de la información a través de una herramienta Informática, Lorena Mahecha Guzmán y Gabriel Coello F., 978-620-2-25000-9, EAE, 2017- Implementing the ISO/IEC 27001 ISMS Standard 2016 (Information Security), Edward Humphreys, 978-1-60807-930-8, Artech House Publishers, 2016- Infosec Management Fundamentals, Henry Dalziel, 978-0-12-804187-1, Syngress, 2015- Information Security Incident Management: A Methodology, Neil Hare-Brown, 978-0-580-50720-5, BSI Standards, 2007
Bibliografía complementaria	

Recomendacións

Materias que se recomenda ter cursado previamente

Materias que se recomenda cursar simultaneamente

Materias que continúan o temario

Observacións

Recoméndase ó estudante, para un aproveitamento óptimo da materia, un seguimento activo das clases así como participar nas distintas actividades e o uso da atención personalizada para a resolución das dúbidas ou cuestións que lle poidan xurdir.

(*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías