Guia docente					
Datos Identificativos					2020/21
Asignatura (*)	Gestión de Incidentes			Código	614530015
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Periodo	Curso		Tipo	Créditos
Máster Oficial	2º cuatrimestre	Primero		Optativa	3
Idioma	CastellanoGallego				
Modalidad docente	Presencial				
Prerrequisitos					
Departamento	Ciencias da Computación e Tecnoloxías da InformaciónComputación				
Coordinador/a	López Rivas, Antonio Daniel		Correo electrónico	daniel.lopez@udc.es	
Profesorado	Dafonte Vazquez, Jose Carlos López Rivas, Antonio Daniel		Correo electrónico	carlos.dafonte@udc.es daniel.lopez@udc.es	
Web	faitic.uvigo.es				
Descripción general	La gestión de incidentes de ciberseguridad se centra en manejar la proactividad para prevenir y atenuar posibles consecuencias. Se obtendrá el conocimiento necesario sobre herramientas que pueden facilitar la gestión de los incidentes y las recuperaciones, la justificación de los planes propuestos para recuperación y resiliencia, la identificación y clasificación de los posibles incidentes y la definición de los cauces para su gestión y resolución.				

Plan de contingencia	Plan de contingencia A: confinamiento total o parcial de estudiantes y/o profesores. 1. Modificación en los contenidos: no hay 2. Metodologías *Metodologías docentes que se modifican - Sesión magistral, impartida a través de videoconferencia. - Prácticas a través de las TIC, se imparte mediante el uso de herramientas propias de los estudiantes y/o acceso remoto al equipamiento del aula. - Prueba objetiva, a través de Faitic, Moodle o otra herramienta que proporcionen UVigo y/o UDC. 3. Mecanismos de atención personalizada al alumnado - Moodle: siempre. Todos los recursos docentes (diapositivas, enunciado de la práctica, anuncios, software, etc.) están disponibles a través de Moodle. - Teams: semanalmente. Las tutorías se atenderán por Teams en los horarios oficiales de cada profesor. - Correo electrónico: siempre. Para responder a cualquier cuestión. 4. Modificaciones en la evaluación: ninguna * Obeservaciones de la evaluación: en el caso de no poder realizarse presencialmente, se llevaran a cabo: - Prueba objetiva: a través de Faitic y Campus Remoto o Teams. 5. Modificaciones de la bibliografía o webgrafía: ninguna. Plan de contingencia B: número de estudiantes excede el aforo del aula. 1. Modificación en los contenidos: no hay 2. Metodologías *Metodologías docentes que se modifican - Sesión magistral, se establecerán dos grupos que asistirán presencialmente en semanas alternas. Se buscará una solución de videoconferencia (Campus remoto o Teams) para acceder a las sesiones remotamente. - Prácticas a través de las TIC, se establecerán dos grupos que asistirán presencialmente semanas alternas. Se buscará una solución de acceso remoto o simuladores para el grupo que no pueda asistir presencialmente. Se imparte mediante el uso de herramientas propias de los estudiantes y/o acceso remoto al equipamiento del aula. - Prueba objetiva, se habilitará un aula con aforo suficiente. 3. Mecanismos de atención personalizada al alumnado - Moodle: siempre. Todos los recursos docentes (diapositivas, enunciado de la práctica, anuncios, software, etc.) están disponibles a través de Moodle. - Teams: semanalmente. Las tutorías se atenderán por Teams en los horarios oficiales de cada profesor. - Correo electrónico: siempre. Para responder a cualquier cuestión. 4. Modificaciones en la evaluación: ninguna * Obeservaciones de la evaluación: en el caso de no poder realizarse presencialmente, se llevaran a cabo: - Prueba objetiva: a través de Faitic y Campus Remoto o Teams. 5. Modificaciones de la bibliografía o webgrafía: ninguna.

Competencias del título	
Código	Competencias del título
A3	CE3 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información

A9	CE9 - Tener capacidad para elaborar de planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
A14	CE14 - Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia
A15	CE15 - Tener capacidad de identificar el valor, tanto económico como de otra índole, de la información de la institución, sus procesos críticos y el impacto que produciría la interrupción de estos; y, también, las necesidades internas y externas que permitirán estar preparados ante ataques de seguridad
A17	CE17 - Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación
B2	CB2 - 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
B3	CB3 - 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
B5	CB5 - 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
B6	CG1 - 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
B10	CG5 - Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos
C4	CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias del título		
Manejar la proactividad para prevenir y atenuar posibles incidentes de seguridad	AP9 AP14 AP17	BP2 BP3 BP5 BP6 BP10	CP4
Obtener el conocimiento necesario sobre herramientas que pueden facilitar la gestión de los incidentes y las recuperaciones	AP3 AP14 AP17	BP2 BP3 BP5 BP6 BP10	
Justificar los planes propuestos para recuperación y resiliencia	AP3 AP9 AP14 AP15	BP2 BP3 BP5 BP6 BP10	CP4
Identificar y clasificar los posibles incidentes y definir los cauces para su gestión y resolución	AP3 AP9 AP17	BP2 BP3 BP5 BP6 BP10	CP4

Contenidos	
Tema	Subtema
1. Fundamentos: resiliencia y el valor de la información	1.1. Introducción 1.2. Fundamentos
2. Detección de incidentes y gestión de respuesta	2.1. Detección y notificación de incidentes 2.2. Gestión de respuesta, contención y mitigación del impacto

3. Estándares: planes de continuidad y de recuperación	3.1. Estándares ISO/IEC 3.2. Directrices para la gestión de incidentes
4. Recuperación de desastres	4.1. Mecanismos 4.2. Fases de recuperación 4.3. Protección de infraestructuras críticas
5. Legislación	5.1. Legislación específica: Esquema Nacional de Seguridad, Estrategia de Ciberseguridad Nacional

Planificación				
Metodologías / pruebas	Competéncias	Horas presenciales	Horas no presenciales / trabajo autónomo	Horas totales
Prácticas de laboratorio	A9 A14 A17 B2 B3 B10	10	25	35
Sesión magistral	A3 A14 A15 A17 B5 B6 C4	10	20	30
Trabajos tutelados	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	1	9	10
Prueba objetiva	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	1.5	0	1.5
Atención personalizada		0		0
(*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos				

Metodologías	
Metodologías	Descripción
Prácticas de laboratorio	Sesiones prácticas en ordenador asociadas a escenarios de incidencias y manejo de herramientas para ciberincidentes. El objetivo es poner en práctica los conocimientos de las sesiones magistrales fomentando el aprendizaje autónomo.
Sesión magistral	Docencia expositiva. Presentaciones de los conocimientos teóricos de los temas de la asignatura promoviendo la interacción con los estudiantes. NOTA: será posible utilizar alguna de estas sesiones para realizar algún taller de empresa o persona colaboradora de reconocida competencia.
Trabajos tutelados	Trabajo a desarrollar por el alumno sobre alguna de las temáticas de la asignatura a propuesta del estudiante o del profesor. Este trabajo tendrá un seguimiento por parte del profesorado y el estudiante realizará una breve defensa presencial del mismo.
Prueba objetiva	Prueba escrita para valorar los conocimientos adquiridos. Aunque se centrará en el material de la docencia expositiva, podrá incorporar algunas cuestiones relacionadas con las sesiones prácticas.

Atención personalizada	
Metodologías	Descripción
Prácticas de laboratorio Trabajos tutelados	La atención personalizada está enfocada a apoyar al alumno en la comprensión de las diferentes técnicas mediante el apoyo en las tutorías y la resolución de dudas que puedan surgir en las clases magistrales. También se le prestará ayuda en las dudas que puedan surgir durante la realización de las prácticas o el aprendizaje mediante los trabajos tutelados para un mejor aprovechamiento y comprensión de los conocimientos adquiridos en clase.

Evaluación			
Metodologías	Competéncias	Descripción	**Calificación**

Prácticas de laboratorio	A9 A14 A17 B2 B3 B10	Sesiones prácticas en ordenador asociadas a escenarios de incidentes y manejo de herramientas para ciberincidentes. El objetivo es poner en práctica los conocimientos de las sesiones magistrales fomentando el aprendizaje autonomo. La evaluación será continua a través de las sesiones. NOTA: será posible utilizar alguna de las sesiones presenciales para realizar algún taller de una entidad colaboradora.	30
Trabajos tutelados	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	Trabajo a desarrollar por el alumno sobre alguna de las temáticas de la asignatura a propuesta del estudiante o del profesor. Este trabajo tendrá un seguimiento por parte del profesorado y el estudiante realizará una breve defensa presencial del mismo.	20
Prueba objetiva	A3 A9 A14 A15 A17 B2 B3 B5 B6 B10 C4	Prueba escrita para valorar los conocimientos adquiridos. Aunque se centrará en el material de la docencia expositiva, podrá incorporar algunas cuestiones relacionadas con las sesiones prácticas.	50

Observaciones evaluación
Para superar la materia, será preciso obtener un mínimo de 5 sobre 10 tanto en la prueba objetiva como en los trabajos prácticos. En caso contrario, la nota máxima que se podrá alcanzar será de 4.5. La nota obtenida en la evaluación continua de prácticas de laboratorio y trabajos tutelados será conservado durante todo el curso académico.FORMA DE TRABAJO Tanto las prácticas de laboratorio como los trabajos tutelados serán realizados en grupos, los tamaños de los grupos será impuestos por el profesorado mientras que los integrantes de los mismos serán de libre elección. FECHAS DE ENTREGA: i) Prácticas de laboratorio: las memorias de las prácticas de laboratorio serán entregadas en la plataforma virtual de docencia antes de finalizar el período de clases y con tiempo suficiente para ser evaluadas por los profesores antes del comienzo del período de examenes. El número de entregas será propuesto a través de la plataforma virtual de docencia. ii) Trabajos tutelados: deberán ser entregado con anterioridad a la última sesión práctica, la cual será utilizada para hacer las exposiciones de los mismos. La fecha final de entrega será propuesta a través de la plataforma virtual de docencia. ESTUDIANTES QUE NO PARTICIPARON EN LA EVALUACIÓN CONTÍNUA DE PRÁCTICAS Y TRABAJOS TUTELADOS: i) Cuando el estudiante se presente en la convocatoria de primera oportunidad, su nota será de 0 en ambas metodologías. ii) Cuando el estudiante se presente en la convocatoria de segunda oportunidad o convocatoria extraordinaria, sin participar en el proceso de evaluación continua, a través de estas metodologías, podrá realizar de forma individual las prácticas con el material disponible, en la plataforma virtual de docencia mediante la solicitud de tutorías con los profesores de la asignatura. También de forma individual, el estudiante concretará con el profesoar la fecha del examen de prácticas, que en este caso, será imprescindible. ESTUDIANTES QUE NO PARTICIPARON EN LA PRUEBA OBJETIVA EN LA PRIMERA OPORTUNIDAD: Participaran o no en el proceso de evaluación continua de prácticas y trabajo tutelado, su calificación será de "No Presentado". PLAGIO: En el caso de detectar plagio en cualquier prueba o material entregado, la calificación final será de SUSPENSO (0) y el hecho será comunicado a la dirección del Centro para los efectos oportunos.

Fuentes de información	
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
Complementária	

Recomendaciones
Asignaturas que se recomienda haber cursado previamente
Asignaturas que se recomienda cursar simultáneamente
Asignaturas que continúan el temario
Otros comentarios
Se recomienda al estudiante, para un aprovechamiento óptimo de la materia, un seguimiento activo de las clases así como participar en las distintas actividades y el uso de la atención personalizada para la resolución de las dudas o cuestiones que le puedan surgir.

(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías