

DATOS IDENTIFICATIVOS				
Prácticas en empresa				
Asignatura	Prácticas en empresa			
Código	V05M175V01106			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	15	OB	2	1c
Lengua Impartición	Castellano			
Departamento	Tecnología electrónica			
Coordinador/a	Marcos Acevedo, Jorge			
Profesorado	Marcos Acevedo, Jorge			
Correo-e	acevedo@uvigo.es			
Web	http://www.munics.es/			
Descripción general	La misión del máster es formar profesionales de alta cualificación en todos los procesos técnicos, organizativos, operativos y forenses relativos a la seguridad digital. El profesorado pertenece a las áreas de Ingeniería Telemática, Teoría de la Señal y Comunicaciones, Ciencias de la Computación e Inteligencia Artificial, Ingeniería de Sistemas y Derecho Penal de las dos universidades, y se complementa con la contribución de destacados profesionales de empresas del sector en Galicia y el compromiso de éstas en apoyar las prácticas de los estudiantes.			

Competencias	
Código	
A1	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación.
A2	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
A3	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.
A4	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
A5	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	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
B2	Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones.
B3	Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas de comunicaciones
B4	Compromiso ético. Capacidad para diseñar e implantar soluciones técnicas y de gestión con criterios éticos de responsabilidad y deontología profesional en el ámbito de la seguridad de la información, las redes y/o los sistemas de comunicaciones
B5	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
B6	Destreza para investigar. Capacidad para innovar y contribuir al avance de los principios, las técnicas y los procesos referidos a su ámbito profesional, diseñando nuevos algoritmos, dispositivos, técnicas o modelos útiles para la protección de los activos digitales públicos, privados o comerciales
C1	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras
C2	Conocer en profundidad las técnicas de ciberataque y ciberdefensa

C3	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
C4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
C5	Diseñar, implantar y mantener un sistema de gestión de la seguridad de la información utilizando metodologías de referencia
C6	Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad
C7	Tener capacidad para realizar la auditoría de seguridad de sistemas e instalaciones, el análisis de riesgos derivados de debilidades de ciberseguridad y desarrollar el proceso de certificación de sistemas seguros
C8	Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad
C9	Tener capacidad para elaborar planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados
C10	Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras.
C11	Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones.
C12	Conocer el papel de la ciberseguridad en el diseño de las nuevas industrias, así como las particularidades, restricciones y limitaciones que se han de acometer para obtener una infraestructura industrial segura.
C13	Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes
C14	Tener capacidad para desarrollar un plan de continuidad de negocio siguiendo normas y estándares de referencia.
C15	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.
C16	Tener capacidad para vislumbrar y enfocar el esfuerzo de negocio en temáticas relacionadas con la ciberseguridad, y con una monetización viable.
C17	Tener capacidad de planificar en el tiempo los periodos de detección de incidentes o desastres, y su recuperación
C18	Interpretar de una forma adecuada las fuentes de información en el ámbito del derecho penal informático (leyes, jurisprudencia y doctrina) de ámbito nacional e internacional.
C19	Saber identificar los perfiles de personal necesarios para una institución en función de sus características y su sector
C20	Conocimiento de las empresas orientadas específicamente al sector de seguridad de nuestro entorno.
D1	Tener capacidad para comprender el significado y aplicación de la perspectiva de género en los distintos ámbitos de conocimiento y en la práctica profesional con el objetivo de alcanzar una sociedad más justa e igualitaria.
D2	Tener capacidad para comunicarse oralmente y por escrito en lengua gallega
D3	Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos
D4	Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad
D5	Tener capacidad para comunicarse oralmente y por escrito en inglés.

Resultados de aprendizaje

Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Experiencia en el desempeño de la profesión y de sus funciones más habituales en un entorno real de empresa.	A1 A2 A3 A4 A5 B1 B2 B3 B4 B5 B6 C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 C20 D1 D2 D3 D4 D5

Contenidos

Tema	
Contenido general	A definir por el tutor en la empresa y el tutor académico.
Integración en la empresa y en su entorno de trabajo	Durante su estancia el alumno se integrará en la organización de la empresa y se deberá coordinar con el resto de integrantes del equipo de trabajo al que sea asignado.
Desarrollo de su actividad profesional	El alumno realizará las tareas encomendadas, de acuerdo con sus conocimientos y competencias.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Prácticum, Practicas externas y clínicas	370	5	375

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

Metodologías

	Descripción
Prácticum, Practicas externas y clínicas	Estancia en una empresa desarrollando funciones propias de un titulado de Master en Ciberseguridad para que pueda poner en práctica los conocimientos y competencias adquiridas, para completar su formación académica.

Atención personalizada

Metodologías	Descripción
Prácticum, Practicas externas y clínicas	El alumno tendrá un tutor dentro de la empresa que le guiará y supervisará en las tareas específicas que tendrá que desarrollar dentro de la misma; y un tutor académico -profesor de la E.E.T. de la Universidad de Vigo- que definirá junto con el tutor de la empresa, el marco general de la actividad del alumno, comprobando que se ajusta al perfil/mención estudiado por el estudiante.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje			
Prácticum, Practicas externas y clínicas	Prácticas externas La evaluación se realizará en función de: 1) La memoria de actividades 2) La evaluación del tutor en la empresa	100	A1 A2 A3 A4 A5	B1 B2 B3 B4 B5 B6	C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 C11 C12 C13 C14 C15 C16 C17 C18 C19 C20	D1 D2 D3 D4 D5

Otros comentarios sobre la Evaluación

MEMORIA DE ACTIVIDADES: El alumno/a deberá entregar una memoria explicativa de las actividades realizadas durante las prácticas, especificando su duración, las unidades o departamentos de la empresa en que se realizaron, la formación recibida (cursos, programas informáticos, etc.), el nivel de integración dentro de la empresa y las relaciones con el personal.

La memoria debe incluir también un apartado de conclusiones, que contendrá una reflexión sobre la adecuación de las enseñanzas recibidas durante la carrera para el desempeño de la práctica (aspectos positivos y negativos más significativos relacionados con el desarrollo de las prácticas). Se valorará, además, la inclusión de información sobre la experiencia profesional y personal obtenida con las prácticas (valoración personal del aprendizaje conseguido a lo largo de las prácticas y sugerencias o aportaciones propias sobre la estructura y funcionamiento de la empresa visitada).

La valoración de la memoria será el 60% de la nota final.

EVALUACIÓN DEL TUTOR EN LA EMPRESA: El tutor de la empresa entregará un informe valorando aspectos relacionados con las prácticas realizadas por el alumno: puntualidad, asistencia, responsabilidad, capacidad de trabajo en equipo e integración en la empresa, calidad del trabajo realizado, etc.

La valoración del tutor en la empresa será el 40% de la nota final.

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

Recomendaciones

Plan de Contingencias

Descripción

=== ADAPTACIÓN DE LAS METODOLOGÍAS ===
* Metodologías docentes que se mantienen
Ninguna porque la asignatura consiste en la permanencia en una empresa desarrollando actividades adaptadas a la titulación

* Metodologías docentes que se modifican
Todas. La asignatura cosiste en la estancia en la empresa del alumno durante un tiempo. En el caso de que la docencia sea

exclusivamente no presencial, la práctica en la empresa solo se podrá realizar si se hace en remoto.

* Modificaciones (si proceden) de los contenidos a impartir
No hay cambios

* Bibliografía adicional para facilitar el auto-aprendizaje
No hay

* Otras modificaciones
No hay más modificaciones

=== ADAPTACIÓN DE LA EVALUACIÓN ===
Sin cambios