Proyecto Formativo Módulo Prácticas Externas: Grado en Ingeniería de la Ciberseguridad

Organización

La asignatura de Prácticas Externas es de carácter obligatorio y se desarrollará preferentemente durante el cuarto curso de Grado. La duración de las prácticas será la que determine el plan de estudios.

La asignatura contará con un tutor académico, responsable de supervisar la calidad de las prácticas y su adecuación, hacer el seguimiento durante la realización de las mismas y evaluar la asignatura a su finalización, basándose para ello en el informe de evaluación final del tutor de empresa y en la memoria final elaborada por el estudiante.

Competencias generales:

- Capacidad para resolver problemas con iniciativa, buena toma de decisiones, autonomía y creatividad.
- Capacidad para saber comunicar y transmitir, tanto de forma oral como escrita, los conocimientos, habilidades y destrezas.
- Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar documentos que tengan por objeto definir, planificar, especificar, resumir proyectos y planes en el ámbito de la ciberseguridad.
- Capacidad para dirigir y liderar las actividades objeto de los proyectos del ámbito de la informática y la ciberseguridad comprendiendo los criterios de calidad que rigen dichas actividades investigadora y profesional.
- Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.
- Capacidad para conocer, comprender y aplicar la legislación y código ético necesario para la labor profesional en el sector de la ciberseguridad.
- Capacidad para evaluar y asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos.
- Capacidad para definir, evaluar y seleccionar contramedidas para la protección de los activos tecnológicos, entendiendo las peculiaridades de los distintos contextos en los que deben desplegarse.
- Conocimiento y aplicación de elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como de legislación, regulación y normalización en el sector de la ciberseguridad.
- Capacidad de trabajo en grupos multidisciplinares propios del ámbito de la ciberseguridad, siendo capaz de comunicarse, dirigir y comprender las necesidades de otros miembros del equipo con perfiles distintos.
- Conocimiento para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos.
- Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad en el ámbito de la ciberseguridad.

- Capacidad para concebir, desarrollar, implantar y mantener sistemas, servicios y aplicaciones informáticas empleando los métodos de la ingeniería como instrumento para el aseguramiento de su calidad.
- Conocimiento y comprensión de un área de estudio que parte de la base de la educación secundaria general y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
- Capacidad para aplicar conocimientos a su trabajo o vocación de una forma profesional. Capacidad para elaborar y defender argumentos y resolver problemas dentro de su aérea de estudio.
- Capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- Capacidad para transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
  Capacidad para aplicar las habilidades de aprendizaje adquiridas necesarias para emprender estudios posteriores con un alto grado de autonomía.

Competencias específicas:

- Comprender los conceptos básicos de álgebra lineal, cálculo diferencial e integral, métodos estadísticos y métodos numéricos que permiten resolver los problemas matemáticos que puedan plantearse en el ámbito de la ciberseguridad.
- Conocer los fundamentos de matemática discreta, lógica, algorítmica y complejidad computacional y saber aplicarlos en la resolución de problemas propios de la ingeniería.
- Conocer el concepto, marco institucional y jurídico, organización y gestión de la empresa, y en especial de aquellas que operan en el sector de la ciberseguridad.
- Conocer y comprender la estructura, organización, funcionamiento e interconexión de los sistemas informáticos, los fundamentos de su programación y su aplicación para la resolución de problemas propios de la ciberseguridad.
- Diseñar e implementar aplicaciones y sistemas orientados a la extracción automática de información y conocimiento a partir de grandes volúmenes de datos con unos niveles adecuados de seguridad.
- Conocer y aplicar los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.
- Comprender, diseñar y utilizar de forma eficiente los tipos y estructuras de datos más adecuados para la resolución de un problema.
- Analizar, diseñar, desarrollar, mantener y desplegar aplicaciones de forma segura y eficiente, eligiendo el paradigma, la metodología y los lenguajes de programación más adecuados para cada contexto.
- Conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como de los componentes básicos que los conforman, siendo capaces de analizar su influencia en la seguridad de los sistemas informáticos.
- Conocer, comprender y evaluar las características, funcionalidades y estructura de los sistemas operativos, siendo capaces de analizar su influencia en la seguridad de los sistemas informáticos.

- Diseñar, desarrollar y desplegar aplicaciones considerando las características, funcionalidades y estructura de Internet y los riesgos que éstas suponen para la ciberseguridad.
- Conocer y aplicar las características, funcionalidades y estructura de los sistemas de información (incluidas las bases de datos y los basados en servicios web), que permitan un adecuado diseño y uso de aplicaciones basadas en ellos que sean seguras.
- Comprender y analizar las implicaciones que para la seguridad tiene desarrollar, desplegar y utilizar aplicaciones y servicios basados en tecnologías de red, incluyendo: Internet, web, comercio electrónico, multimedia, servicios interactivos, redes sociales, computación móvil, Internet de las cosas.
- Comprender y ser capaz de poner en práctica los principios, metodologías y ciclos de vida de la ingeniería de software, especialmente aquellos modelos utilizados preferentemente para el desarrollo de software seguro.
- Analizar, diseñar y construir sistemas inteligentes y autónomos para la cibserseguridad que perciban su entorno y actúen racionalmente de acuerdo con la tarea asignada.
- Conocer el concepto de ciberseguridad y sus pilares fundamentales e implicaciones en un contexto globalizado, tecnológico y conectado como el actual.
- Conocer, comprender y aplicar las arquitecturas y modelos de ciberseguridad.
- Ser capaz de gestionar el factor humano en ciberseguridad mediante la definición de políticas y procedimientos adecuados para cada contexto.
- Comprender los algoritmos criptográficos de clave pública y de clave privada más importantes y conocer sus aplicaciones en ciberseguridad.
- Analizar las etapas o pasos que los atacantes siguen para construir sus ataques de manera que se puedan comprender los patrones de ataque más graves e importantes y llevarlos a cabo en entornos de seguridad ofensiva.
- Analizar y cuantificar el riesgo que corre un determinado activo, evaluar sus vulnerabilidades e identificar los potenciales impactos de un ciberataque, calibrando su criticidad.
- Conocer la legislación nacional e internacional que se aplica a la ciberseguridad y a sus profesionales, así como comprender el concepto de ciberdelito, su modelo de negocio y sus implicaciones.
- Diseñar, desplegar, configurar y gestionar soluciones que protejan el perímetro de una red, segmentarla y prevenir/detectar intrusiones en ella.
- Diseñar, desplegar, configurar y gestionar soluciones que protejan los datos almacenados y en tránsito (las comunicaciones).
- Diseñar, desplegar, configurar y gestionar mecanismos adecuados para la gestión de identidades digitales (identificación, autenticación, autorización y auditoría o IAAA)
- Conocer los distintos tipos de malware en función de su vector de infección, mecanismos de propagación, replicación y protección, de sus objetivos, etc.
- Analizar malware, extraer conclusiones acerca de su funcionamiento y ser capaz de diseñar, desplegar, configurar y gestionar soluciones que protejan contra ese malware.
- Diseñar, desplegar, configurar y gestionar soluciones de seguridad física de las instalaciones.
- Diseñar, desplegar, evaluar y mejorar planes de respuesta ante incidentes y de continuidad del negocio.
- Garantizar la disponibilidad, tolerancia a fallos y/o resiliencia hasta los niveles adecuados para cada contexto
- Recoger y analizar evidencias digitales para extraer conclusiones post-incidente y realizar análisis forenses.

- Definir e implantar planes directores de seguridad siendo capaz de priorizar las iniciativas y proyectos recogidos en estos planes.
- Establecer controles de seguridad que garanticen los niveles adecuados de madurez y seguridad en cada contexto.
- Escoger el tipo de auditoría más adecuado para cada contexto, ser capaz de elegir o desarrollar las herramientas más adecuadas para llevarla a cabo y analizar los resultados obteniendo conclusiones relevantes.
- Comprender el concepto de infraestructura crítica, analizar los riesgos específicos que pueden sufrir y ser capaz de desplegar las contramedidas adecuadas para gestionarlos adecuadamente y teniendo en cuenta la legislación vigente.
- Comprensión y dominio de los conceptos básicos de campos y ondas y electromagnetismo, teoría de circuitos eléctricos, circuitos electrónicos, principio físico de los semiconductores y familias lógicas, dispositivos electrónicos y fotónicos, y su aplicación para la resolución de problemas propios de la ingeniería.
- Comprender y analizar los retos y las repercusiones que las diferentes ciber amenazas representan para la Seguridad Nacional

Salidas profesionales

- Arquitecto de seguridad.
- Analista de seguridad.
- Administrador de seguridad.
- Desarrollador de aplicaciones seguras.
- Consultor o auditor.
- Pen-tester o hacker ético.
- Investigador.
- Miembro de equipos de detección y respuesta ante incidentes.
- Director o responsable de seguridad.

Convenios firmados / Entidades colaboradoras

- GMV SOLUCIONES GLOBALES INTERNET, S.A
- INNOTEC SYSTEM, S.L.U.
- ACCENTURE, S.L.
- TECNILOGICA ECOSISTEMAS, S. A.
- GRUPO SIA, SISTEMAS INFORMÁTICOS ABIERTOS, S.A.
- NTT DATA SPAIN, S.L.
- TELEFÓNICA CYBERSECURITY Y CLOUD TECH, S.L. (FUE)
- BANKINTER GLOBAL SERVICES, S.A.
- S2 GRUPO DE INNOVACION EN PROCESOS ORGANIZATIVOS, S.L.U.
- PRICEWATERHOUSECOOPERS ASESORES DE NEGOCIOS, S.L.
- MAPFRE TECH, S.A.
- TOYOTA ESPAÑA S.L.U.
- BOTECH FRAUD PREVENTION & INTELLIGENCE, S.L.
- SISTEMAS AVANZADOS DE TECNOLOGIA (SATEC), S.A.
- AVANADE SPAIN, S.L.U.
- SERVICIO INFORMÁTICO Y MANTENIMIENTO TECNOLÓGICO, S.L.
- BNP PARIBAS SUCURSAL EN ESPAÑA, S.L.