Guía Docente: Prácticas de Iniciación Profesional

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Año verificación	2017
Materia/Módulo	Prácticum
Carácter	Optativo
Modalidad	Virtual
Período de impartición	Tercer Trimestre
Curso	Primero
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No precisa

DATOS DEL PROFESORADO			
Profesor Responsable	Rafael Mata Milla	**Correo electrónico**	rafael.mata.milla@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Doctor acreditado	No		
Perfil Profesional 2.0	LinkedIn		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Contexto y sentido de la asignatura	La asignatura «Prácticas de Iniciación Profesional» se impartirá de forma virtual a través del aula virtual adquiriendo sus competencias y habilidades a través de situaciones similares a las que se producen en contextos laborales y que están diseñadas para que el alumno siga un proceso de aprendizaje basado en el «aprender haciendo» (learn by doing). Es una asignatura optativa respecto a las Prácticas externas presenciales o en modo teletrabajo realizadas en un centro colaborador de prácticas externas.

RESULTADOS DE APRENDIZAJE	
Conocimientos o contenidos	• CON01: Conocer las tendencias actuales en técnicas de ciberataque. • CON02: Comprender, aplicar y evaluar técnicas de hacking ético. • CON03: Conocer requisitos y procedimientos avanzados de certificación de sistemas seguros. • CON05: Conocer, aplicar y evaluar técnicas avanzadas de autenticación biométrica de acceso a sistemas. • CON06: Conocer los conceptos básicos de los principales procesos y respuestas ante incidentes y su aplicación a casos reales. • CON07: Comprender, aplicar y evaluar la gestión de la seguridad de sistemas altamente securizados por su naturaleza o criticidad.
Habilidades o destrezas	• HAB01: Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • HAB02: Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • HAB03: Analizar e identificar las vulnerabilidades de un sistema informático, y ser capaz de desarrollar y aplicar técnicas y métodos de protección de la información. • HAB05: Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas.
Competencias (básicas y generales)	• 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. • 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. • 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. • 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. • 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. • CG7: Ser capaz de integrarse en equipos de trabajo o investigación multidisciplinares de manera eficaz y colaborativa

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	La asignatura «Prácticas de Iniciación Profesional» se impartirá de forma virtual a través del aula virtual adquiriendo sus competencias y habilidades a través de situaciones similares a las que se producen en contextos laborales y que están diseñadas para que el alumno siga un proceso de aprendizaje basado en el «aprender haciendo» (learn by doing).
Contenidos	Esta asignatura tendrá un enfoque práctico y se planteará como uno o varios proyectos de trabajo o de investigación donde se deberán alcanzar unos resultados esperados, siguiendo el proceso de aprendizaje de aprender-haciendo. Por este motivo, la asignatura no cuenta con unos contenidos teóricos fijos sino que serán contenidos de apoyo al proyecto concreto que se plantee en cada convocatoria de la asignatura.

METODOLOGÍA	
Métodos y actividades formativas del proceso de enseñ anza-aprendizaje	Se desarrollarán casos prácticos dentro de uno o varios proyectos, con orientación por parte del docente, guiando al alumno a lo largo de todo el proceso y aportando los fundamentos teóricos necesarios para afrontarlos. El trabajo desarrollado por el alumno a lo largo de la asignatura se estructurará en los siguientes tipos de actividades: **Proyectos prácticos:** se plantearán proyectos de aplicación profesional práctica a partir de los contenidos propuestos. La explicación del proceso de aprendizaje se completará con orientaciones al estudio que ayudarán al alumnado en la comprensión y la consecución de actividades. De este modo el alumnado tendrá a su disposición actividades que podrá encontrarse durante su práctica profesional. **Videotutorías**: sesiones en directo, que pueden visualizarse en diferido, donde se expone la resolución de las dudas presentadas al profesor previamente. **Lectura crítica, análisis e investigación**: se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación.

EVALUACIÓN	
Sistema evaluativo	El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. La asignatura presenta un sistema de evaluación continua a través del cual se valorará la adquisición de competencias y se logrará un mayor seguimiento de la evolución y el progreso del alumnado. A lo largo del desarrollo de la asignatura se presentarán una serie de actividades de aplicación práctica, de carácter evaluable, mediante las cuales se conformará la calificación final.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	[1] W. Stallings, «Network security essentials». Pearson, 2017. (Disponible en: https: //dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2792) Es una publicación completa sobre seguridad en redes. Ofrece una amplia información sobre seguridad aplicada en sistemas, redes, auditorias, etc. [2] Y. Diogenes and E. Ozkaya, «Cybersecurity, attack and defense strategies». Packt Publishing, 2019. (Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2697) Libro que se centra en las estrategias de ataque y defensa para mejorar la seguridad de un sistema, con numerosos ejemplos y figuras que facilitan la comprensión de los conceptos.
Bibliografía complementaria	[3] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 2022. Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=3097 [4] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls. 2022. Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=3098 [5] J. Vacca, «Cyber security and IT infrastructure protection», 1st ed. Syngress. Elsevier, 2014. Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1925
Otros recursos	DomainTools. (2021). Whois Lookup, Domain Availability & IP Search. Retrieved from https://whois.domaintools.com/ Calvo Ortega, G. (2020). Seguridad zero – Un sitio donde encontrar soluciones tecnológicas y de seguridad. Retrieved June 4, 2021, from https://seguridadzero.com/