Guía Docente: Ciberseguridad Social e Industrial

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Tendencias tecnológicas y Ciberseguridad
Carácter	Obligatorio
Período de impartición	Anual
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se prevén requisitos previos, por tanto los requisitos serán los propios del título.

DATOS DEL PROFESORADO			
Profesor Responsable	Félix Antonio Barrio Juárez	**Correo electrónico**	felixantonio.barrio@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	https://es.linkedin.com/in/felixbarrio		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Ciberseguridad Social e Industrial
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura, que constituye una de los grandes áreas conceptuales del Master en Ciberseguridad por su carácter anual, describirá los conceptos y problemática que afrontan los expertos en ciberseguridad como base para implementar sistemas de gestión de la seguridad que faciliten la prevención, mitigación, reacción y recuperación frente a los riesgos. Se hará un recorrido por las arquitecturas recomendadas para asegurar un nivel óptimo de securización, así como las medidas a articular en entornos organizacionales. Será igualmente importante para adquirir una solvencia analítica y la capacidad para responder a las necesidades de las organizaciones en materia de ciberseguridad, que el alumno conozca los distintos tipos de incidentes y ataques, las motivaciones y vectores utilizados por los atacantes.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• 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. • 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. • CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones • CG2: Ser capaz de permanecer eficaz dentro de un medio cambiante, así como a la hora de enfrentarse con nuevas tareas, retos y personas • CG6: Conocer y aplicar métodos de protección en sistemas tecnológicos industriales y sociales avanzados. • CG7: Ser capaz de integrarse en equipos de trabajo o investigación multidisciplinares de manera eficaz y colaborativa. • CE02: Conocer las tendencias actuales en técnicas de ciberataque • CE06: Comprender, aplicar y evaluar la gestión de la seguridad de sistemas altamente securizados por su naturaleza o criticidad. • CE11: Conocer, aplicar y evaluar métodos y técnicas para la seguridad de sistemas tecnológicos sociales (IoT) e industriales (IIoT).
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Conocer las principales formas de ataque a infraestructuras sociales (IoT) e industriales avanzadas. • Desarrollar métodos de seguridad en sistemas tecnológicos sociales (IoT) e industriales. • Conocimientos adecuados de gestión de seguridad en sistemas e infraestructuras críticos.

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	
	• Internet de las cosas (I):
	  ◦ Análisis de ataques.
	  ◦ Del Cloud Computing al IoT
	  ◦ Seguridad y redes sociales.
	• Internet de las cosas (II):
	  ◦ Seguridad en Smart Cities.
	  ◦ Drones y ciberseguridad.
	  ◦ Normativa aplicable.
	• Industria 4.0 (1):
	  ◦ Riesgos de seguridad 4.0.
	  ◦ Certificación de sistemas seguros.
	• Industria 4.0 (2):
	  ◦ Infraestructuras críticas.
	  ◦ Sistema global de seguridad industrial.
	• Métodos inteligentes de gestión de seguridad:
	  ◦ Análisis y detección inteligente de vulnerabilidades.
	  ◦ Gestión de ciberataques

Contenidos	**UD1: Introducción a la ciberseguridad. Conceptos de seguridad y amenazas** • Ciberseguridad. Conceptos básicos • Principales amenazas y motivaciones • Tipos de software malicioso y su evolución • El rol del profesional de la seguridad de la información y los sistemas de gestión de la ciberseguridad **UD2: Vulnerabilidades y gestión del riesgo** • Tipos de vulnerabilidades y clasificación • Controles preventivos, correctivos, detectivos, disuasivos. • Buenas prácticas de seguridad (ISO 27002, CobIT, SoGP – ISF, PCI) • Medición de efectividad de controles. **UD3: Agentes de la amenaza** • Mapas de amenazas • Detección de amenazas • Inteligencia y aprendizaje **UD4: Ciberincidentes** • Tipos de incidentes de seguridad y su distribución social e industrial • Respuesta a incidentes • Mitigación de impacto cuando sucedan los eventos inesperados **UD5: Métodos de ataque** • Tipos principales y tendencias • Investigación y desarrollo frente a los nuevos métodos de ataque **UD6: Medidas de protección y arquitectura de seguridad** • Regulación, legislación y normalización técnica • Definición, implementación y gestión de la arquitectura de seguridad para

	garantizar que los servicios de la organización cumplan con los requerimientos de seguridad

METODOLOGÍA	
Actividades formativas	Para el desarrollo de la asignatura se llevarán a cabo las siguientes actividades: **Foros de debate:** actividad en la que se discutirá y argumentará acerca de diferentes temas relacionados con la asignatura **Estudio de caso:** actividad en la que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando una situación real o simulada que le servirá para guiar el proceso de descubrimiento inducido. **Trabajo colaborativo:** en esta tarea se deberá reflexionar sobre alguno de los temas planteados y entablar un diálogo y debate con el resto de estudiantes para presentar un trabajo conjunto. **Cuestionarios:** cuestionario evaluable que servirán para poner a prueba los conocimientos adquiridos. **Actividades de contenidos:** Al igual que el cuestionario, pone a prueba los conocimientos adquiridos mediante la resolución de ejercicios prácticos.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* 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)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua** Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior.

	En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	Taleb, N. N., & Filella, R. (2008). El cisne negro: el impacto de lo altamente improbable. Paidós. Salas, A. (2015). Los hombres que susurran a las máquinas: hackers, espías e intrusos en tu ordenador. Espasa.
Bibliografía complementaria	Cano, J. (2009). Computación forense. Descubriendo los rastros informáticos. Editorial: AlfaOmega, México. Villalón, Antonio; Holguín, José Miguel; Belda, Nelo; Vila, José (2011). Protección de Infraestructuras Críticas 2011. Valencia: S2 Grupo. Poulsen, Kevin (2003). Slammer worm crashed Ohio nuke plant net. Recuperado de http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/ Chien, Eric (2010). Stuxnet: A Breakthrough. Recuperado de http://www.symantec.com/connect/blogs/stuxnet-breakthrough Falliere, Nicolas, Murchu, Liam O., y Chien, Eric (2011). W32.Stuxnet Dossier. Symantec. Recuperado de http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf Allen, Julia H. Jody R. Westby. “Governing for Enterprise security (GES). Implementation Guide”. Carnegie Mellon University, USA. ISO (2013). ISO/IEC 27002, Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneve: ISO. ISO (2015). ISO/IEC 20000-1:2011. Information technology -- Service management -- Part 1: Service management system requirements. Geneve: ISO IT Governance Institute, *Control Objectives for Information and related Technology* (CobiT).

	Trendmicro (2016). Utility Provider in Michigan Hit by Ransomware Attack. Recuperado de http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digitalthreats/electricity-utility-in-michigan-downed-by-ransomware-attack Firvida, Daniel (2016). Familias de malware en la industria. Instituto Nacional de Ciberseguridad, 2016. Recuperado de https://www.incibe.es/blog/BlogSeguridad/ultimos_articulos/?postAction=getBlogHome&blogID=1000077536&p=0 Paganini, Pierluigi (2014). Cyber attack on German steel factory caused severe damage. Recuperado de http://securityaffairs.co/wordpress/31368/cyber-crime/cyber-attackgerman-steel-factory.html Organization for Economic Co-operation and Development (OECD), *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security,* France, 2002.
Otros recursos	Estándares ISO: http://www.iso.org/iso/home/standards.htm. La familia de normas ISO 2700X resulta un imprescindible para el responsable de ciberseguridad. Estándares IEEE: http://standards.ieee.org/index.html. Estándares como IEEE 1686:2013 para ciberseguridad de IoT resultan un instrumento de conocimiento obligado. Blog de la Oficina de Seguridad del Internauta: https://www.osi.es/es/actualidad/blog. El blog se nutre de interesantes artículos profesionales. NICE Program: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework. Este modelo de los USA orienta sobre los perfiles de ciberseguridad así como las funciones asignadas a cada rol. Shodan. Search Engine for Vulnerabilities. https://www.shodan.io/. Un imprescindible portal web para detección de vulnerabilidades en la red. Talleres CyberCamp. https://www.youtube.com/results?search_query=talleres+cybercamp. Relación de las mejores ponencias y talleres en ciberseguridad de este evento anual celebrado en España desde 2015.