Guía Docente: Ciberseguridad en Servicios y Aplicaciones Web

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	Segundo Trimestre
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	Antonio Pérez Carrasco	**Correo electrónico**	antonio.perez.carrasco@ui1.es
Área	Arquitectura y Tecnología de Computadores	**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Linkedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Biometría Aplicada • Ciberseguridad en Servicios y Aplicaciones Web • Ciberseguridad Móvil • Ciberseguridad Social e Industrial
Contexto y sentido de la asignatura en la titulación y perfil profesional	La asignatura se centra en el mundo de las aplicaciones web, eje fundamental del uso masivo de internet hoy día, en el que las páginas web estáticas de antaño dejaron paso a servicios dinámicos tales como redes sociales, servicios de *streaming*, telebanca, tiendas, alojamiento *online* y otros tipos de servicios que permiten hacer de la web el mayor banco de aplicaciones y servicios que puede imaginarse. Esta asignatura ayuda a complementar el resto de asignaturas del máster, que se centran en la seguridad en redes informáticas, aplicaciones móviles, biometría, llenando el hueco fundamental que representa el mundo web. Esta asignatura permite obtener una panorámica sobre los principales problemas de seguridad que asoman en internet desde el punto de vista de los usuarios y de los proveedores de las aplicaciones. Se sientan las bases de las buenas prácticas y de la tecnología disponibles, mientras se repasan los principales problemas existentes en las distintas áreas de las aplicaciones web. Dado que todos los servicios digitales que se prestan tienen una interfaz web (incluso cuando van enmascarados a través de aplicaciones móviles), la asignatura se torna fundamental para cualquier persona que quiera dedicarse al sector de la seguridad, ya se trate de revisar el estado de la web corporativa de una entidad, diseñar o mantener una aplicación web o bien ofrecer cualquier tipo de soporte en entornos de cualquier tamaño donde la tecnología web se emplee.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• ?????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. • 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. • 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. • CG3: Diseñar y elaborar concisa, clara y razonadamente planes y proyectos de trabajo en el ámbito de la ciberseguridad. • CG5: Ser capaz de proponer soluciones imaginativas y originales así como ser capaz de promover la innovación e identificación de alternativas contrapuestas a los métodos y enfoques tradicionales en el ámbito de la ciberseguridad. • 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. • CE07: Comprender, aplicar y evaluar las técnicas de seguridad en el desarrollo y uso de aplicaciones web y en los servicios basados en ellas. • CE10: Conocer los conceptos básicos de los principales procesos y respuestas ante incidentes y su aplicación a casos reales.
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Implantar de manera segura las aplicaciones web de la empresa. • Configurar de manera segura la plataforma necesaria para el soporte de aplicaciones y servicios web. • Conocimientos adecuados de las diferentes tecnologías empleadas para desarrollar servicios seguros en Internet.

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	• Ataques específicos en Internet:
	  ◦ Ataques contra la sesión.
	  ◦ Ataques de fuerza bruta.
	  ◦ *Phising*.
	  ◦ XSS.
	  ◦ Ataques SQLi.
	  ◦ Ataques DDoS.
	• Configuración de servidores en Internet:
	  ◦ Principio de mínima información.
	  ◦ El servidor de correo.
	  ◦ El servidor DNS.
	  ◦ El servidor web.
	  ◦ Los servidores de ficheros.
	  ◦ Servidores de terminal.
	  ◦ Servidores DBMS.
	• Configuración segura de servicios:
	  ◦ Cifrado.
	  ◦ Sistemas de clave pública.

	◦ Revisión de logs. • Configuración del servidor DBMS: ◦ Accesos. ◦ Administración y permisos. • Configuración del servidor web: ◦ Tecnologías de aplicaciones web. ◦ Asegurar la aplicación. ◦ Módulos de seguridad.
Contenidos	Unidad 1: Introducción a la seguridad web • La Evolución de la Web • Los componentes de las Aplicaciones Web • Los Riesgos de las Aplicaciones Web • Herramientas de Protección Unidad 2: Seguridad en autenticación y gestión de sesión • Los problemas de la actualidad • Métodos de ataque a las contraseñas • Métodos de aumento de protección • Gestión de la identidad de los usuarios • Otras formas de autenticación Unidad 3: Seguridad en el servidor • Los principales problemas detectados en servidores • Herramientas para hacer seguro el servidor y monitorizarlo • Control de acceso • Organización de las políticas de seguridad Unidad 4: Configuración de servidores • Principios a seguir • Configuración del servidor web • Configuración del servidor de correo electrónico • Configuración del servidor DNS • Configuración de servidores de DBMS Unidad 5: Ataques a aplicaciones web • XSS • Ataques SQLi • Ataques DDoS • Ataques a base de datos Unidad 6: Configuración segura de servicios • Cifrado • Sistemas de clave pública • Firewalls • Punto de vista de atacantes: herramientas y metodología

METODOLOGÍA	
Actividades formativas	• Contenidos teóricos: Texto Canónico donde se explican los nuevos conceptos de cada unidad didáctica, apoyado por el uso de material gráfico y enlaces a información multimedia que ayuden a la mejor comprensión de dichos conceptos. • Foros de Debate: El alumnado debatirá para aportar ideas sobre temas de la asignatura, relacionados con aspectos tecnológicos y de la vida cotidiana. Se plantearán tres foros de debate a lo largo de la asignatura. • Trabajo de Investigación: Se planteará un tema sobre el cual el alumno podrá realizar una ampliación del mismo persiguiendo conocer un aspecto concreto en profundidad. Se plantearán dos trabajos de investigación. • Actividad práctica: Se propone una actividad relacionada con la programación o con la aplicación directa de los contenidos teóricos en un contexto concreto. • Trabajo Colaborativo: Se planteará un ejercicio práctico relacionado con los contenidos de la asignatura, y que deberá resolverse siguiendo alguna técnica de trabajo colaborativo, abarcará varias unidades para darle un carácter amplio y de aplicación real. • Cuestionarios: Al final de las unidades didácticas 2, 4 y 6 se planteará un cuestionario relacionado con los contenidos de las unidades didácticas que permitirá medir el grado de adquisición de conocimientos y competencias. • 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. **Prueba de Evaluación de Competencias (PEC)** En el caso de optar por la opción 2 de evaluación (PEC+ examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC). Esta prueba se define como una actividad integradora a través de la cual el estudiante deberá demostrar la adquisición de competencias propuestas en la asignatura, vinculadas principalmente al «saber hacer». Para ello hará entrega de un conjunto de evidencias en respuesta a los retos propuestos en esta prueba. La entrega se realizará antes de finalizar la asignatura.

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)*. 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.

* Los estudiantes que realicen el máster por formación bonificada (FUNDAE) deberán acogerse a la opción 1 del sistema de evaluación, evaluación continua (EC)+ examen final (EX).

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.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el resultado total, se establece una relación de proporcionalidad en una escala de 10.

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	[1] Stuttard, D, Pinto, M. The Web Application Hacker's Book, Finding and Exploiting Security Flaws (2nd edition). Wiley Publishing. 2011. Es uno de los manuales de referencia en el mundo de la seguridad web. [2] Mueller, J. P. Security for Web Developers, O'Reilly.2016. Recorre los aspectos básicos acerca de la seguridad a la hora de programar una aplicación web.
BibliografÍa complementaria	[3] Scambray, J., Liu, V., Sima, C. Hacking Exposed Web Applications 3, Web Applications Security Secrets and Solutions. EE.UU., Mc Graw Hill, 2011. [4] Bertino, E., Martino, L. Paci, L., Squicciarini, A. Security for Web Services and Service-Oriented Architectures. Reino Unido, Springer, 2010. [5] Young Rhee, M. Internet Security, Cryptographic Principles, Algorithms and Protocols. Reino Unido, Wiley Publishing, 2003. [6] J. LeBlanc, T. Messerschmidt. Identity and Data Security for Web Development, Best Practices. EE.UU., O'Reilly, 2016.
Otros recursos	• https://www.darkreading.com/ DarkReading: Portal dedicado a la información sobre seguridad, que aporta noticias, análisis, reportajes sobre áreas como la seguridad móvil, web o redes, entre otras. • https://cybersecurityventures.com/cybersecurity-market-report/ Cybersecurity Ventures: Página que ofrece un punto de vista social y económico del mundo de la ciberseguridad, ofreciendo informes sobre tendencias, riesgos y soluciones. • https://searchsecurity.techtarget.com/ Tech Target: Portal tecnológico dedicado a recopilar información sobre las últimas noticias sobre tecnología, comercio y ciberseguridad. • https://www.zdnet.com/ ZD Net: portal dedicado a ofrecer noticias y reportajes sobre el mundo de la tecnología y, entre otros aspectos, la seguridad. • http://www.infopackets.com/ InfoPackets: Portal web sobre informática que pone el foco de atención en información sobre seguridad y buenas prácticas. • https://www.eff.org/ Electronic Frontier Foundation: FUndación sin ánimo de lucro orientada a investigar y concienciar sobre la privacidad y la seguridad en el entorno digital. • https://authy.com/ Authy: Web que propone el uso de métodos 2FA para autenticarse en internet con el fin de mejorar la seguridad de la identidad digital. • https://12factor.net/ The Twelve-Factor: Web que se dedica a repasar los doce factores que conducen al éxito en la publicación de una aplicación web. • https://www.blackhat.com/ BlackHat: Comunidad que crea foros de dicusión sobre temas de seguridad y actualidad.