Guía Docente: Ciberseguridad en Sistemas Locales y Redes

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Ciberseguridad y sistemas
Carácter	Obligatorio
Período de impartición	Primer 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	Amalia Beatriz Orúe López	**Correo electrónico**	amaliabeatriz.orue@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Google Academic		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Ciberseguridad en Sistemas Locales y Redes
Contexto y sentido de la asignatura en la titulación y perfil profesional	La interconexión de sistemas y redes existentes en la sociedad actual, nos facilita el intercambio de información, de bienes y servicios de una manera casi transparente. En este mundo «ultra-conectado» la seguridad en redes y sistemas locales es el pilar básico para interactuar en la sociedad de una manera confiable. Para tener capacidad efectiva de desarrollar medidas de seguridad que protejan nuestros activos digitales, es imprescindible conocer la red por donde transita la información sensible así como los sistemas locales donde ésta se encuentra almacenada. En esta asignatura se pretende establecer una base de conocimientos acerca de las amenazas a los sistemas locales y redes, así como las medidas de protección ante posibles ataques o accesos no autorizados, siendo conscientes que las redes de acceso deben ser la primera línea de defensa. Para cursar esta asignatura son necesarios algunos conocimientos previos sobre redes locales y protocolos TCP/IP para entender de manera adecuada las técnicas de seguridad que serán estudiadas.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	Generales y básicas • 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. • CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones. • 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. • 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. Específicas • CE01: Analizar y detectar técnicas de ocultación de ataques a sistemas y redes en casos reales. • 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. • Elaboración de una operativa de seguridad acorde con la política de seguridad y la legislación. • Conocer y evaluar los problemas de seguridad existentes en una red local, así como los posibles puntos de vulnerabilidad. • Conocer tendencias en ciberataques y saber detectar técnicas de ocultación de ataque a sistemas y redes • Ser capaz de recuperar información acerca de una red (equipos vivos, elementos, paquetes de red, etc.).

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	• Administración de servidores:
	  ◦ Instalación segura del servidor GNU/Linux.
	  ◦ Instalación segura del servidor Windows Server.
	• Seguridad pasiva y activa:
	  ◦ Políticas de copias de seguridad.
	  ◦ Sistemas de recuperación local y en red.
	  ◦ Certificados y sistemas de clave pública y privada.
	  ◦ IPSEC.
	• Configuración de servicios:
	  ◦ Cortafuegos.
	  ◦ Protección de los puertos.
	• Ataques contra redes
	  ◦ Protección contra ataques
	  ◦ Accesos seguros a servidores.
	  ◦ Acceso seguro entre redes: VPN.
	• Instalación y configuración de sistemas de seguridad perimetral:

	◦ Configuración de cortafuegos. ◦ Configuración de servidores proxy.
Contenidos	Unidad didáctica 1: Conceptos básicos de Ciberseguridad • Políticas y gestión de la seguridad informática. • Seguridad aplicada a Redes y sistemas locales. • Tipos de amenazas en sistemas locales y redes. • Conceptos y fases de un ataque informático y medidas de respuesta. Unidad didáctica 2: Seguridad en la electrónica de red • Criptografía. • Conceptos de tunneling (GNS3). • VLAN y segmentacion de redes. • Seguridad en servicios VoIP. Unidad didáctica 3: Sistemas de Protección Perimetral • Cortafuegos y Arquitecturas. • Filtrado y reglas de filtrado de paquetes. • Dispositivos de Protección Perimetral. • Sistemas de detección de intrusos en red. Unidad didáctica 4: Seguridad en redes inalámbricas • Protocolos de seguridad WIFI y Bluetooth. • Vulnerabilidades en redes WIFI y Bluetooth. • Medidas de seguridad en redes WIFI. • Medidas de seguridad en redes Bluetooth. Unidad didáctica 5: Seguridad en sistemas locales y remotos I • Servicios y vulnerabilidades en un sistema local. • Arquitectura GNU/Linux vs Windows. • Seguridad pasiva y activa. • Monitorización y Hardening de hosts. Unidad didáctica 6: Seguridad en sistemas locales y remotos II • Arquitecturas de sistemas locales y remotos. • Servicios remotos y «la nube». • Seguridad en sistemas remotos, contenedores y «la nube». • Seguridad proporcionada por los contenedores.

METODOLOGÍA	
Actividades formativas	Para el desarrollo de la asignatura se llevarán a cabo entre otras, las siguientes actividades: • **Estudios de caso**: Los estudios de caso se plantearán bien como un ejercicio introductorio, sobre el que se deberá investigar en la web para resolverlo, o bien como un ejercicio de aplicación, sobre algún tema del que ya se haya iniciado su tratamiento en la unidad, donde el alumno deberá utilizar en su resolución, los recursos necesarios aplicando los conceptos y aspectos desarrollados en la unidad didáctica. • **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. Además, se propondrán actividades autoevaluables a lo largo del desarrollo del contenido teórico, las cuales permitirán al alumno comprobar su grado de comprensión del mismo. • **Foros de Debate**: Actividad en la que se debatirá y argumentará sobre diversos temas de la asignatura, promoviendo el desarrollo del pensamiento crítico. • **Trabajo Colaborativo**: Se podrán plantear ejercicios prácticos relacionados con los contenidos de la asignatura, y que deberán resolverse siguiendo técnicas de trabajo colaborativo. • **Cuestionarios:** cuestionario evaluable que servirán para poner a prueba los conocimientos adquiridos.

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	**Bibliografía básica** Jhon R. Vacca (2017). **Computer and Information Security Handbook**. (3ª ed.). United States of America. ELSEVIER. Es una publicación actualizada y completa sobre seguridad informática. Ofrece una amplia informacion sobre seguridad aplicada en sistemas, redes, auditorias, etc. Andrew Lockhar (2006). **Network security Hacks**. Tips & Tools for Protecting Your Privacy. (2ª ed.) O'Reilly. Libro de referencia para administradores de Windows y técnicas para garantizar la seguridad en redes informaticas. Ofrece respuestas y ejemplos concisos de cifrado aplicado, detección de intrusiones y respuesta a incidentes.
BibliografÍa complementaria	Wil Allsopp. **Advanced Penetration Testing: Hacking the World's Most Secure Networks**. John Wiley & Sons; 1 edition (14 April 2017) Chris McNab. **Network Security Assessment: Know Your Network**. O'Reilly Media; 3 edition (25 Feb. 2016 Stuart McClure, Joel Scambray, George Kurtz. **Hacking Exposed 7: Network Security Secrets and Solutions.** McGraw-Hill Education; 7 edition (16 Mar. 2012) Joshua Wright, Johnny Cache. **Hacking Exposed Wireless, Third Edition: Wireless Security Secrets & Solutions**. McGraw-Hill Education; 3 edition (16 Mar. 2015) Michael Davis, Sean Bodmer, Aaron Lemasters, Christopher Elisan. **Hacking Exposed Malware & Rootkits: Security Secrets and Solutions.** McGraw-Hill Education; 2 edition (16 Jan. 2017) Ben Clark. **Rtfm: Red Team Field Manual** CreateSpace Independent Publishing Platform; 1.0 edition (11 Feb. 2014) Ajay Singh Chauhan. **Practical Network Scanning: Capture network vulnerabilities**

	using standard tools such as Nmap and Nessus. Packt Publishing (24 May 2018) Clifford Stoll. **El huevo del cuco**. Planeta (20 de noviembre de 1990) Julio Gómez López, Eugenio Villar Fernández, Alfredo Alcayde García. **Seguridad en Sistemas Operativos Windows y Linux**. RA-MA S.A. Editorial y Publicaciones; Edición: 2 (29 de julio de 2011) David Santo Orcero. **Pentesting con Kali: Aprende a dominar la herramienta Kali de pentesting, hacking y auditorías activas de seguridad**. CreateSpace Independent Publishing Platform (15 de junio de 2017)
Otros recursos	Para oficial para descargar GNS3 y ver tutoriales: https://www.gns3.com/. Video que muestra cómo instalar un router IOS en GNS3: https://www.youtube.com/watch?v=hdMXGz5rozk Obtencion de informacion via web de dispositivos en red: https://whois.domaintools.com/ Página Oficial para descargar Wireshark y ver tutoriales: https://www.wireshark.org/ Analisis de capturas de paquetes con Wireshark Página oficial para descargar Snort y ver tutoriales: https://www.snort.org/ Página oficial de NMAP para descargar y ver tutoriales: https://nmap.org/ Búsqueda de puertos abiertos con NMAP. Página oficial de Nessus para descargar y ver tutoriales: https://www.tenable.com/products/nessus/nessus-professional Web sobre contenedores y virtualización por Guillermo Calvo: https://seguridadzero.com/