Guía Docente: Ciberseguridad en la Red y Sistemas

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Grado en Ciencias de la Seguridad
Plan de estudios	2016
Materia	Informática
Carácter	Obligatorio
Período de impartición	Tercer Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No existen requisitos previos para esta asignatura.

DATOS DEL PROFESORADO			
Profesor Responsable	Diego Ramírez Jiménez	**Correo electrónico**	diego.ramirez@ui1.es
Área		**Facultad**	Facultad de Criminología
Perfil Profesional 2.0	Mi Linkedin		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Aplicación de las TIC a la Práctica Profesional • Ciberseguridad en la red y sistemas • Tecnologías Aplicadas a la Gestión de la Seguridad
Contexto y sentido de la asignatura en la titulación y perfil profesional	Las nuevas tecnologías y la evolución de la informática han ayudado a que nos encontremos en un mundo interconectado donde el acceso a la información y el desempeño diario de las actividades se realiza en su totalidad o en parte de ella mediante el uso de dispositivos informáticos. La protección ya no solo se debe aplicar en el mundo físico sino en el virtual donde los riesgos y las amenazas cada vez son mayores y tienen más repercusión, para ello, el concepto de ciberseguridad es algo que tiene que estar presente en cualquier empresa y como parte de su normativa de seguridad y plan de protección. En esta asignatura, se abordará el concepto de seguridad desde diferentes puntos de vista. En primer lugar desde el plano auditor y de cumplimiento normativo donde veremos las técnicas de evaluación del nivel de seguridad de una empresa, aprenderemos a realizar un análisis de riesgos informático y a detectar dónde y cómo hay que implantar medidas de protección, basandonos en metodologías y normativas como el Esquema Nacional de Seguridad o la norma ISO/IEC 27001. El segundo punto de vista es el de la seguridad técnica, abordando conceptos de hacking para conocer en mayor profundidad nuestra infraestructura informática y de esta forma saber protegerla bajo la premisa de ponerse en la piel de un atacante para conocer sus técnicas y saber defenderlas. Abordaremos también el estado actual de ciberataques y sus consecuencias en casos reales. Estudiaremos cómo detectar, analizar y recuperarnos de incidentes de ciberseguridad mediante técnicas de análisis forense así como las principales medidas y recomendaciones para mantener los sistemas y la red empresarial protegida de ciberataques. Esta asignatura está ubicada en el grado de Ciencias de la Seguridad como asignatura optativa para complementar los conocimientos de seguridad desde el punto de vista informático.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CB04: Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. • CB05: Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. • CG01: Conocer, saber organizar y planificar los recursos individuales y colectivos disponibles para el ejercicio, en sus distintas modalidades, de la profesión. • CG02: Capacidad para asesorar a terceros en cuestiones concretas y específicas que solo la especialización en una materia puede otorgar. • CG03: Capacidad de gestión de la información, de redacción de informes y/o artículos de investigación con una actitud creativa e innovadora y mediante el empleo de una correcta técnica de investigación. • CG04: Resolución de problemas en materias relativas a la seguridad. • CG05: Motivación por la calidad. • CU04: Utilizar las tecnologías de la información y la comunicación (TIC) para poner en marcha procesos de trabajo ajustados a las necesidades de la sociedad actual. • CU05: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión. • CU06: Aprender a trabajar individualmente de forma activa. • CU07: Valorar lo que suponen las nuevas formas de trabajo actuales, como es el teletrabajo y el trabajo en red, y saber trabajar de forma colaborativa en ellas. • CU08: Entender las prácticas y el trabajo colaborativo como una forma de aplicar la teoría y como una manera de indagar sobre la práctica de valores teóricos.
Resultados de aprendizaje de la asignatura	• Busca y localiza información digital relevante para aplicarla a su ámbito de conocimiento. • Aplica herramientas y recursos para buscar información. • Presenta y difunde información a través de medios digitales con una calidad profesional. • Aplica correctamente estrategias de comunicación y de difusión de información en la red. • Domina los conceptos, las funciones y aplicaciones básicas, dispositivos e interrelación entre programas. • Aplica estrategias de comunicación e interacción en entornos virtuales correctamente. • Usa y aplica críticamente y de forma segura las TIC. • Sabe qué es una amenaza informática, qué intenta dañar o por qué se produce. • Diferencia entre los distintos tipos de amenazas informáticas y sabe cómo minimizar sus daños. • Conoce qué tecnologías están destinadas a la seguridad y su gestión. • Conoce el funcionamiento, los avances técnicos y las limitaciones de la seguridad privada.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Adquirir los conocimientos necesarios para saber identificar cualquier tipo de agresión a la seguridad virtual de un sistema, así como poder minimizar los daños producidos por esta. Distinguir qué tipos de ataques hay y qué se pretende con dicha amenaza.
Contenidos	**Unidad Didáctica 1. Auditoría Informática y cumplimiento normativo** - Evaluación de la seguridad - Metodología - Normas ISO/IEC 27001 y 27002 - Esquema Nacional de Seguridad - Análisis de riesgos **Unidad Didáctica 2. Hacking ético** - Concepto de hacker y fundamentos del hacking ético - Blue team y red team - Auditoría técnica: análisis pasivo y activo - Auditoría técnica: explotación de vulnerabilidades **Unidad Didáctica 3. Ciberataques** - Clasificación - Ataques contra la integridad - Ataques contra la disponibilidad - Ataques contra la privacidad - Amenazas persistentes avanzadas - Ataques en entornos industriales e infraestructuras críticas **Unidad Didáctica 4. Seguridad en servidores y aplicaciones web** - Protección de servidores - Seguridad en páginas web - Seguridad en la nube **Unidad Didáctica 5. Análisis forense** - Adquisición de evidencias y cadena de custodia - Localización de la información - Recuperación de datos borrados - Análisis de ataques y malware **Unidad Didáctica 6. Seguridad de red y perimetral** - Monitorización de red, IDS/IPS - Cortafuegos - Control de acceso a la red y VPN - Seguridad en redes inalámbricas

METODOLOGÍA	
Actividades formativas	En cada una de las 6 Unidades didácticas, el alumnado deberá llevar a cabo actividades que le conduzcan a la asimilación de los conceptos y a su puesta en práctica. Entre otros, se propondrán las siguientes actividades: • **Estudio de Caso:** Se plantearán estudios de caso reales sobre algún tema de la unidad. Se trata de ejercicios introductorios sobre el que se deberá investigar en la web para resolverlos y donde el alumno deberá utilizar los recursos necesarios aplicando los conceptos y aspectos desarrollados en las unidades didácticas. Han de servir además como motivación y conducción del pensamiento reflexivo personal. • **Foros de Debate:** Los alumnos debatirán para aportar ideas sobre temas de la asignatura. • **Trabajo Colaborativo:** Se planteará un ejercicio práctico relacionado con los contenidos de la asignatura, y que deberá resolverse siguiendo alguna técnica de trabajo colaborativo grupal. • **Trabajo Individual:** Ejercicio práctico que el alumno tendrá que resolver individualmente, no solo indicando su propuesta o solución sino como la llevaría a cabo. • **Cuestionarios:** preguntas evaluables 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.

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	R. Messier, CEH v11 Certified Ethical Hacker. Study Guide. Sybex Inc. ISBN: 978-1119800286, 2021. Gallotti, C. (2022). *Information security - 2022 Edition. Risk management. Management systems. The ISO/IEC 27001:2022 standard. The ISO/IEC 27002:2022 controls*. ISBN: 979-1220388474 El primer libro corresponde a la guía de referencia y de preparación para obtener el certificado en Hacking Ético o CEH del EC-Council, libro que recoge de forma extensa los términos, técnicas y medidas de seguridad a evaluar desde el punto de vista de un auditor técnico de ciberseguridad o hacker ético para exponer los contenidos relacionados con la parte técnica de la ciberseguridad de esta asignatura. El segundo libro recoge la guía para implementar y auditar un sistema de gestión de seguridad de la información, fundamental para comprender los requisitos de ciberseguridad a nivel de protección de la información basándose en normativa como es la ISO 27001.
Bibliografía complementaria	Agé, M., Ebel, F., Rault, R., Vicogne, F., Crocfer, R., Puche, D., Dumas, D., Schalkwijk, L., Bancal, D., Acissi, H. J., Lasson, S., Fortunato, G. (2018). *Seguridad informática. Hacking Ético* (4ª edición). ISBN: 978-2409012976 2 Lazaro Dominguez, F. (2015). *Introducción a la Informática Forense*. ISBN:

978-8499642093

Molina, F. (2015). La evolución de las técnicas de 'hacking' ético. *Red Seguridad: Revista Especializada. Seguridad Informática, Protección De Datos Y Comunicaciones 68*.

Centro Criptológico Nacional. (2017). *Guía de Seguridad de las TIC CCN-STIC 808: Verificación del cumplimiento del ENS*.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.

McClure S., Scambray J., & Kurtz, G. (1999). Hacking Exposed. Network Security Secrets and Solutions. McGraw Hill, ISBN: 0072121270

Kim, P. (2018). *The Hacker Playbook 3: Practical Guide To Penetration Testing*. ISBN: 978-1980901754

Ramos A. y Barbero C. (2014). *Seguridad perimetral, monitorización y ataques en redes*. ISBN: 978-84-9964-297-0

Stuttard, D. y Pinto M. (2011). *The Web Application Hacker's Handbook.* [Recurso Electrónico] [e-book]. Sussex John Wiley & Sons.

Mitnick K. (2006). *El arte de la intrusión : la verdadera historia de las hazañas de hackers, instrusos e impostores*.

Otros recursos

ENS - Esquema Nacional de Seguridad. Recuperado de https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001 Consultado en junio 2021.

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XpA8UjfVKUn Consultado en junio 2021.

OWASP. Web Application Penetration Testing. Recuperado de https://www.owasp.org/index.php/Web_Application_Penetration_Testing Consultado en septiembre 2018.

Awesome Hacking. A collection of awesome lists for hackers, pentesters & security researchers. Recuperado de https://github.com/Hack-with-Github/Awesome-Hacking. Consultado en junio 2021.

Kali Linux, distribución para hacking y test de penetración (web principal). Recuperado de https://www.kali.org/. Consultado en junio 2021.

VirusTotal, servicio de análisis de archivos y URLs sospechosas para la detección de malware. Recuperado de https://www.virustotal.com/es/. Consultado en junio 2021.

Bleeping Computer, Foro de informática con un destacado subforo en ciberseguridad centrado en las últimas novedades en malware. Recuperado de https://www.bleepingcomputer.com/forums/f/79/security/. Consultado en junio 2021.

Wireshark User's GuideVersion 3.3.0. Recuperado de https://www.wireshark.org/download/docs/user-guide.pdf. Consultado en junio 2021.

Óscar López, Haver Amaya, Ricardo León. Informática Forense : Generalidades, aspectos técnicos y herramientas. Recuperado de http://www.urru.org/papers/Rrfraude/InformaticaForense_OL_HA_RL.pdf. Consultado en junio 2021.

	INCIBE - Avisos de seguridad. Recuperado de https://www.incibe.es/protege-tu-empresa/avisos-seguridad. Consultado en junio 2021.