Guía Docente: Fundamentos de Seguridad de la Información

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Materia	Ingeniería de Computadores
Carácter	Obligatorio
Período de impartición	Segundo Trimestre
Curso	Tercero
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Ninguno

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	• Arquitectura de Computadores • Fundamentos de Seguridad de la Información
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura recoge muchos de los interrogantes abiertos en cuanto a las amenazas existentes en las redes de computadores, aspectos relacionados con otras asignaturas del grado como son redes de computadores y redes avanzadas de computadores. De hecho, los fundamentos de la seguridad juegan un rol fundamental en los sistemas informáticos que existen actualmente en el mercado tecnológico. Esta seguridad se ha extendido, ya no sólo para asegurar la información de grandes corporaciones, también resulta vital para garantizar la integridad de sistemas de tamaño medio, incluso pequeño. Por ello, se precisa una difusión de conceptos básicos y técnicas específicas para garantizar la seguridad, formando a los estudiantes con todas las terminologías y técnicas existentes. Esta materia se engloba dentro de la Mención de Criptología y Seguridad de la Información.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CE01: Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, de acuerdo con los conocimientos adquiridos, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas. • CE03: Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas. • CR01: Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente. • CR04: Capacidad para elaborar el pliego de condiciones técnicas de una instalación informática que cumpla los estándares y normativas vigentes. • CU09: Considerar los valores propios de la Formación Profesional Superior en términos de igualdad formativa y educativa con la universitaria. • CT01: Capacidad de análisis y síntesis: encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos • CT04: Capacidad para la resolución de problemas • CU15: Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. • CU16: Saber transmitir un informe técnico de la especialidad.
Resultados de aprendizaje de la asignatura	• Adopta pautas y prácticas de tratamiento seguro de la información, reconociendo las vulnerabilidades de un sistema informático y la necesidad de asegurarlo*. • Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema. • Implanta técnicas seguras de acceso remoto a un sistema informático, interpretando y aplicando el plan de seguridad. • Implanta cortafuegos para asegurar un sistema informático, analizando sus prestaciones y controlando el tráfico hacia la red interna. • Implanta servidores «proxy», aplicando criterios de configuración que garanticen el funcionamiento seguro del servicio. • Implanta soluciones de alta disponibilidad empleando técnicas de virtualización y configurando los entornos de prueba. • Reconoce la legislación y normativa sobre seguridad y protección de datos valorando su importancia. • Caracteriza diferentes modelos de seguridad relacionados con el control de acceso en el sistema operativo. • Identifica diferentes arquitecturas de seguridad de los sistemas operativos actuales. • Entiende la importancia de definir una política de seguridad dentro del sistema y expresarla en un lenguaje de seguridad. • Escribe módulos de política de seguridad para un sistema. • Conoce los procesos y herramientas necesarias para identificar los problemas de seguridad que puede provocar un programa. • Conoce la importancia del análisis forense en el contexto actual, y las técnicas básicas utilizadas para recolectar, analizar y presentar evidencias. • Identifica los pasos necesarios para la construcción de software seguro. • Identifica los usos de la ingeniería inversa desde el punto de vista de la seguridad del sistema con objeto de poder detener posible ataques.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Conforme a la Orden EDU/392/2009, de 20 de enero, por la que se establece el currículo del ciclo formativo de Grado Superior correspondiente al título de Técnico Superior en Administración de Sistemas Informáticos en Red, los ejes temáticos de esta asignatura coincidirán con los del módulo profesional '0378. Seguridad y Alta disponibilidad', y serán los siguientes: • Adopción de pautas de seguridad informática. • Implantación de mecanismos de seguridad activa. • Implantación de técnicas de acceso remoto. Seguridad perimetral. • Instalación y configuración de cortafuegos. • Instalación y Configuración de servidores «proxy». • Implantación de soluciones de alta disponibilidad. • Legislación y normas sobre seguridad.
Contenidos	**Unidad didáctica 1: Conceptos básicos** • La seguridad de la información. • Conceptos fundamentales de la seguridad. • Clasificación de seguridad. • Arquitecturas de los sistemas operativos **Unidad didáctica 2: Criptografía y seguridad en sistemas** • Criptografía simétrica: cifrado en flujo y en bloques. • Criptografía asimétrica • Infraestructura de clave pública (PKI). • Certificados digitales **Unidad didáctica 3: Amenazas tecnológicas y seguridad en accesos** • Los atacantes. • Tipos de ataques • Fases de un ataque. • Acceso seguro a sistemas **Unidad didáctica 4: Mecanismos de seguridad pasiva** • La seguridad pasiva. • Copias de seguridad. • Seguridad Perimetral. • Sistemas de alimentación ininterrumpida. **Unidad didáctica 5: Mecanismos de seguridad activa** • La seguridad activa. • Seguridad de las Contraseñas • Listas de control de acceso. • El servidor proxy. • Cortafuegos. **Unidad didáctica 6: Normativa y Legislación** • Sistema de Gestión de la Seguridad de la Información. • Normativas: ISO 27000. ISO 27001. ISO 27002.

	• Otras normas ISO 2700X relevantes. • Legislación: L59/2003. RGPD 2016. LO 3/2018 (LOPDGDD)

METODOLOGÍA	
Actividades formativas	Para el desarrollo de la asignatura se llevarán a cabo entre otras, las siguientes actividades: • **Estudio de Caso real de aplicación práctica:** Se plantearán estudios de caso real en varias unidades didácticas sobre algún tema de la unidad. Se trata de ejercicios introductorios sobre los 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. • **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, en cada unidad didáctica se incluyen actividades autoevaluables (no computables para la calificación final) para ayudar al alumnado en el proceso de asimilación de contenidos de cada una de las diferentes unidades didácticas. Así mismo, se plantearán cuestionarios de autoevaluación que sí computarán para la nota final; en ellos, los alumnos y alumnas valorarán la comprensión de los contenidos de las unidades didácticas a través de un cuestionario final en cada una de ellas • **Foros de Debate:** Los alumnos debatirán para aportar ideas sobre temas de la asignatura, relacionados con aspectos de la vida cotidiana. • **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. • **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	Jhon R. Vacca (2017). **Computer and Information Security Handbook**. (3ª ed.). United States of America. ELSEVIER. Esta publicación proporciona la referencia más actual y completa sobre seguridad informática. Este volumen ofrece una amplia informacion sobre todo tipo de seguridad aplicada en sistemas, redes, auditorias, etc. Stallings, W. (2010). **Fundamentos de seguridad en redes** (2º ed.). Madrid: Pearsons. Libro fundamental para la iniciación en el mundo de la seguridad en las redes de computadores. Permite al alumno adquirir un marco global de la asignatura y profundizar a través de ejemplos. El índice está estructurado de forma que la identificación de las unidades didácticas no resulta compleja dentro del contenido del libro.
Bibliografía complementaria	Agé, M., Ebel, F., & Rault, R. (2016). **Seguridad informática - Hacking Ético**. ENI. Apaza Cora, M. G. (2009). **Informática Forense en Entornos de Windows**. *Revista de Información, Tecnología y Sociedad*, 45. Cano, J. J. (2007). **Inseguridad Informática y Computación Anti-forense: Dos Conceptos Emergentes en Seguridad de la Información**. *Information Systems Control Journal*, 4, 54. Chicano, E. (2012). **Gestión de incidentes de seguridad informática**. Antequera: ICE. Wil Allsopp. (2017). **Advanced Penetration Testing: Hacking the World's Most Secure**

Networks. John Wiley & Sons; 1 edition.

Chris McNab. (2017). **Network Security Assessment: Know Your Network**. O'Reilly Media; 3 edition.

Stuart McClure, Joel Scambray, George Kurtz. (2012). **Hacking Exposed 7: Network Security Secrets and Solutions.** McGraw-Hill Education; 7 edition.

Ben Clark. **Rtfm: Red Team Field Manual** (2014). CreateSpace Independent Publishing Platform; 1.0 edition.

Ajay Singh Chauhan. (2018). **Practical Network Scanning: Capture network vulnerabilities using standard tools such as Nmap and Nessus**. Packt Publishing

Clifford Stoll. (1990). **El huevo del cuco**. Planeta.

Julio Gómez López, Eugenio Villar Fernández, Alfredo Alcayde García. (2011). **Seguridad en Sistemas Operativos Windows y Linux**. RA-MA S.A. Editorial y Publicaciones; Edición: 2.

Fundación Telefónica. (2016). **Ciberseguridad, la protección de la información en un mundo digital**. Madrid: Ariel.

Gómez, A. & González, M. (2011). **Auditoria de seguridad informática. Certificados de profesionalidad. Seguridad informática**. Paracuellos de Jarama: Agapea.

Marrero Travieso, Y. (2003). **La Criptografía como elemento de la seguridad informática**. *ACIMED*, *11*(6).

Plata Cheje, R. W. (2009). **Des/Encriptacion en la Informatica Forense**. *Revista de Información, Tecnología y Sociedad*, 35.

Rascagneres, P. (2016). **Seguridad informática y Malwares**. ENI.

Roa, J. M. (2013). **Seguridad informática**. Madrid: McGraw-Hill.

Ugas, L. (2010). **Seguridad en organizaciones con tecnologías de información**. *Télématique*, *1*(1), 1-8.

Otros recursos

- ARP Poisoning. Man in the Middle Attack
- Entrevista a Chema Alonso que refleja la sencillez que supone hackear un sistema informático.
- ISO 27001 Sistemas de Gestión de Seguridad de la Información. Part I. https://www.youtube.com/watch?v=2yQv_sBYr6I
- ISO 27001 Sistemas de Gestión de Seguridad de la Información. Part II. https://www.youtube.com/watch?v=Qw695g4I8-8
- SGSI Sistema de Gestión de Seguridad de la Información. https://www.youtube.com/watch?v=wIe01QIFA8Q
- Privacidad y Anonimato en la Red: Uso básico Tor Browser. https://www.youtube.com/watch?v=YHSg0xrFtQo
- ¿Qué es un Firewall o Cortafuegos?
- Proteger la información en la era del computador cuántico. https://www.youtube.com/watch?v=U4ngc73uF6s
-
- Webinar Planeando e Implementando ISO 27001: https://www.youtube.com/watch?v=JgG9Xj2V2as
- Webinar. Aspectos clave sobre SGSI en la nueva ISO 27001:2013: https://www.youtube.com/watch?v=EqTgSPNm7dY

	• Webinar: "Estandares ISO 27001": https://www.youtube.com/watch?v=bvxpJKkhJF0 • Nuevo fallo de seguridad deja expuestos datos de clientes de Target: https://www.cnet.com/es/noticias/target-sufre-de-nuevo-otra-vulnerabilidad-en-su-seguridad/ • Un fallo de seguridad pone al descubierto datos confidenciales de clientes de Vodafone: https://www.facua.org/es/noticia.php?Id=3731 • Las diez peores violaciones de seguridad en 2014: http://muyseguridad.net/2014/12/31/violaciones-de-seguridad-en-2014/ • Tecnología vs privacidad. https://www.youtube.com/watch?v=-xsey5xgF6E • Ryuk, ¿Qué hay detrás del Ciberataque al SEPE? Ryuk, ¿Qué hay detrás del Ciberataque al SEPE? - Una al Día (hispasec.com)