Guía Docente: Fundamentos de Seguridad de la Información

DATOS GENERALES	
Facultad	Facultad de Criminología
Titulación	Grado en Criminología
Plan de estudios	2012
Especialidad/Mención	Mención en Ciberseguridad
Materia	Informática
Carácter	Optativo
Período de impartición	Tercer Trimestre
Curso	Tercero
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	Lucía Bort Lorenzo	**Correo electrónico**	lucia.bort@ui1.es
Área		**Facultad**	Facultad de Criminología
Perfil Profesional 2.0	Doctora Cum Laude en el programa de doctorado de Ciencias Jurídicas y Económicas de la UCJC, especializada en Criminalística. Graduada en Criminología por la Universidad de Valencia, con especialidad en Seguridad Privada (habilitación Detective Privado). Máster Oficial Universitario en Criminalística, escena del crimen e investigación criminal en la UCJC. Máster Oficial Universitario en Ciberseguridad por la UAX. Directora y fundadora de INTK Business Security. www.linkedin.com/in/lucía-bort-lorenzo-6266a4162		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Aplicación de las TIC a la Práctica Profesional • Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Dirección de Proyectos de Seguridad Corporativos • 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 sobre nuevas tecnologías. Por ello es muy recomendable que el alumno tenga unos conocimientos previos sobre redes de ordenadores y sistemas operativos. 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.

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CU-05: Realizar investigaciones basándose en métodos científicos que promuevan un avance en la profesión. • CU-06: Aprender a trabajar individualmente de forma activa. • CG-01: Capacidad de análisis, síntesis y organización. • CG-02: Comunicación oral y escrita en la lengua nativa. • CG-03: Conocimientos de una lengua extranjera y/o de informática, relativos al ámbito de estudio. • CG-04: Capacidad de gestión de la información. • CG-06: Razonamiento crítico y aprendizaje autónomo. • CB-01: Poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio. • CG-05: Resolución de problemas. • CG-07: Motivación por la calidad. • CU-04: Utilizar las Tecnologías de la Información y la Comunicación (TICs) para poner en marcha procesos de trabajo ajustados a las necesidades de la sociedad actual. • CU-07: 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. • CU-08: Entender las prácticas y el trabajo colaborativo como una forma de aplicar la teoría y como una manera de indagar sobre la práctica valores teóricos. • CB-03: Reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética. • CB-05: Desarrollar aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía. • CB-04: Transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado. • CE-16: Organizar y/o programar a su nivel el trabajo de la unidad/gabinete, adaptando procedimientos, produciendo información o instrucciones, previendo, asignando o distribuyendo tareas, recursos y materiales.

	• CMB-02 Capacidad para plantear, desarrollar y dirigir el proceso de auditoría de un sistema en red, de forma manual y a través del uso de herramientas automáticas, generando un informe que resume los resultados. • CMB-03 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. • CMB-04 Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas. • CMB-07: Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional. • CMB-08: Conocer y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos. • CMB-09: Conocer de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios. • CMB-06: Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión.
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. • Es capaz de plantear, redactar, organizar y desarrollar proyectos de seguridad y auditoria informática. • Conocer las características, funcionalidades y estructura de los sistemas operativos, implementar aplicaciones así como diseñar soluciones a los problemas. • Conocer y tener la capacidad de analizar y valorar el impacto social y medioambiental de las soluciones técnicas, así como resolver los problemas con iniciativa, autonomía y creatividad. • Ser capaz de identificar, valorar y relacionar los activos de una organización con las amenazas a las que están expuestos. • Ser capaz de desarrollar y desplegar proyectos globales y políticas de seguridad corporativas, teniendo según el alcance establecido. • Conocer y saber utilizar las principales herramientas que permite obtener vulnerabilidades en los sistemas. • Conocer y saber utilizar las principales herramientas de análisis de red. • Conocer los principios generales sobre los cortafuegos, sus diferentes componentes, tipos diferentes y capacidad para poder crear reglas propias.

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** 1.1. La seguridad de la información. 1.2. Seguridad informática. 1.3. Seguridad de las TIC 1.4. Seguridad de los equipos informáticos **Unidad didáctica 2: Criptografía y seguridad en sistemas** 2.1. Principios de diseño y clasificación de los criptosistemas 2.2. Criptosistemas simétricos o de clave secreta 2.3. Criptosistemas asimétricos o de clave pública 2.4. Criptosistemas híbridos **Unidad didáctica 3: Amenazas tecnológicas y seguridad en accesos** 3.1. Conceptos básicos y terminología 3.2. Fases de un ataque informático 3.3. Ataques más comunes 3.4. Accesos seguros a sistemas **Unidad didáctica 4: Mecanismos de seguridad pasiva** 4.1. Seguridad pasiva 4.2. Tipos de almacenamientos 4.3. Seguridad del entorno 4.4. Seguridad perimetral (física) 4.5. Sistemas de alimentación ininterrumpida **Unidad didáctica 5: Mecanismos de seguridad activa** 5.1. Uso de contraseñas 5.2. Listas de control de acceso 5.3. Uso de software de seguridad: antivirus 5.4. Cortafuegos (firewalls) 5.5. Sistemas de detección y prevención de intrusos (IDS/IPS) 5.6. Empleo de la criptografía: protocolos AAA y Kerberos **Unidad didáctica 6: Normativa y Legislación** 6.1. Normas ISO

	6.2. Sistema de gestión de la seguridad de la información 6.3. Legislación

METODOLOGÍA	
Actividades formativas	Para el desarrollo de la asignatura se llevarán a cabo entre otras, las siguientes actividades: • **Estudio de Caso:** se plantearán estudios de caso en los 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. • **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. • **Cuestionarios**: cuestionarios de autoevaluación que sí computarán para la nota final; en ellos, se valorará la comprensión de los contenidos de las unidades didácticas. • **Foros de Debate:** los alumnos debatirán para aportar ideas sobre temas de la asignatura, relacionados con aspectos de la vida cotidiana. • **Prueba de Evaluación de Competencias (PEC):** Además, en el caso de optar por esta opción 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.

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	Jhon R. Vacca (2017). *Computer and Information Security Handbook*. Elsevier. Esta publicación proporciona una referencia 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*. 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. y Rault, R. (2015). *Seguridad informática - Hacking Ético*. ENI. Agé, M., Ebel, F. y 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*. ICE.

Gómez López, J., Villar Fernández, E. y Alcayde García, A. (2011). **S**eguridad en Sistemas Operativos Windows y Linux. RA-MA S.A.

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

Gómez, A. & González, M. (2011). *Auditoria de seguridad informática. Certificados de profesionalidad. Seguridad informática*. 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*. 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)
-