

GUÍA DOCENTE

1. DESCRIPCIÓN DE LA ASIGNATURA

Grado:	Ingeniería Informática en Sistemas de Información
Doble Grado:	
Asignatura:	Seguridad
Módulo:	M6: Tecnología Específica de Sistemas de Información
Departamento:	Deporte e Informática
Año académico:	2016-2017
Semestre:	Primer semestre
Créditos totales:	6
Curso:	3º
Carácter:	Obligatoria
Lengua de impartición:	Español

Modelo de docencia:	C1	
a. Enseñanzas Básicas (EB):		50%
b. Enseñanzas de Prácticas y Desarrollo (EPD):		50%
c. Actividades Dirigidas (AD):		

2. RESPONSABLE DE LA ASIGNATURA

Responsable de la asignatura	
Nombre:	Eloy Rafael Sanz Tapia



GUÍA DOCENTE

Centro:	Escuela Politécnica Superior
Departamento:	Deporte e Informática
Área:	Lenguajes y Sistemas Informáticos
Categoría:	Profesor Asociado TP
Horario de tutorías:	Jueves 18:00-21:00
Número de despacho:	23.1.50
E-mail:	esanz@upo.es
Teléfono:	

GUÍA DOCENTE

3. UBICACIÓN EN EL PLAN FORMATIVO

3.1. Descripción de los objetivos

Como objetivos generales en términos de resultados de aprendizaje, son los directamente derivados de la principal competencia a desarrollar: EB4 (adquirir conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería). Además, se espera que el estudiante potencie su pensamiento crítico, razonamiento abstracto, y capacidad para organizar las ideas y comunicarlas.

Como objetivos concretos, se pretende que el alumno conozca los conceptos asociados a la seguridad de la información, la forma de analizar los riesgos de un sistema de información, los controles disponibles para gestionar esos riesgos y los aspectos organizativos y procedimentales para gestionar la seguridad de la información, así como la normativa, estándares y legislación aplicables en este ámbito.

3.2. Aportaciones al plan formativo

Enmarcada en el Módulo de Tecnología Específica de Sistemas de Información - Materia Sistemas de Información, la asignatura Seguridad presenta los conceptos de la seguridad de la información y da al alumnado herramientas para analizar de manera crítica los riesgos derivados del almacenamiento, tratamiento y comunicación de la información, así como los conocimientos para gestionar y reducir esos riesgos.

En esta asignatura deberían sentarse las bases que permitan garantizar la seguridad en las actividades tratadas en otras asignaturas (diseño, desarrollo y explotación de sistemas de información, creación y operación de redes de comunicaciones, configuración y operación de sistemas operativos...).

3.3. Recomendaciones o conocimientos previos requeridos

Es muy recomendable que el alumno haya superado las asignaturas Sistemas Operativos (SO) y Redes de Computadores (RC).

4. COMPETENCIAS

4.1 Competencias de la Titulación que se desarrollan en la asignatura

4.1.1 Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía usabilidad y seguridad de los sistemas,

GUÍA DOCENTE

servicios y aplicaciones informáticas (Competencia G03).

4.1.2 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 (Competencia EC01).

4.1.3 Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados. (Competencia EC08)

4.2. Competencias del Módulo que se desarrollan en la asignatura

4.2.1 Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente. (Competencia ET02).

4.3. Competencias particulares de la asignatura

4.3.1 Conocimientos fundamentales sobre seguridad de la información.

4.3.2 Capacidad de analizar y gestionar los riesgos sobre los sistemas de información y la continuidad del negocio.

4.3.3 Conocimientos sobre los controles de seguridad, su funcionamiento y aplicación.

4.3.4 Conocimientos sobre los aspectos organizativos y procedimentales para gestionar la seguridad de la información.

4.3.5 Conocimientos sobre la normativa, estándares y legislación aplicables en este ámbito.

GUÍA DOCENTE

5. CONTENIDOS DE LA ASIGNATURA (TEMARIO)

Tema 1: Introducción y conceptos básicos

1. Necesidad de la seguridad de la información
2. Aspectos de la seguridad

Tema 2: El ciclo de la seguridad

1. Análisis y gestión de riesgos
2. Controles y procesos de seguridad
3. Métricas, evaluación y mejora continua
4. Sistemas de gestión de seguridad de la información

Tema 3: Aspectos organizativos de la seguridad

1. Políticas y aspectos organizativos
2. Gestión de activos
3. Seguridad ligada a los recursos humanos

Tema 4: Seguridad física

1. Áreas seguras
2. Seguridad del hardware
3. Equipos móviles
4. Gestión de medios

Tema 5: Seguridad en sistemas

1. Configuración segura de sistemas
2. Protección frente a código malicioso
3. Gestión de actualizaciones, monitorización y registros
4. Sistemas de detección de intrusiones en host

Tema 6: Seguridad en redes

1. Aspectos de la seguridad en redes
2. Cortafuegos
3. Sistemas de detección de intrusiones en red
3. Seguridad en redes inalámbricas

Tema 7: Criptografía

1. Criptografía de clave privada
2. Criptografía de clave pública
3. Funciones hash
4. Firma electrónica, certificados digitales e infraestructura de clave pública
5. Esteganografía

GUÍA DOCENTE

Tema 8: Desarrollo seguro

1. Principios de seguridad en desarrollo
2. Principales vulnerabilidades

Tema 9: Control de acceso

1. Autenticación, autorización, auditoría
2. Buenas prácticas para la gestión del acceso
3. Sistemas de gestión de identidades

Tema 10: Gestión de incidentes de seguridad

1. Conceptos
2. Procedimientos
3. Análisis forense

Tema 11: Continuidad

1. Conceptos
2. Copias de seguridad
3. Redundancia
4. Sistemas de alta disponibilidad
5. Centros de respaldo

Tema 12: Cumplimiento

1. Introducción
2. Protección de datos de carácter personal
3. Propiedad intelectual
4. Otra normativa aplicable

6. METODOLOGÍA Y RECURSOS

Por un lado las Enseñanzas Básicas (EB), comúnmente llamadas clases teóricas, están dirigidas a todo el grupo y se imparten en forma de lección magistral, con los objetivos esenciales de transmitir conocimientos, ofrecer un enfoque crítico de la asignatura que lleve a los alumnos a reflexionar y descubrir las relaciones entre los diversos conceptos, y el formar una mentalidad crítica en la forma de afrontar los problemas y la existencia de un método. Aunque la lección magistral se trata principalmente de la exposición continua del profesor, los alumnos pueden tomar notas y tienen la oportunidad de preguntar. La resolución de problemas se llevará a cabo tanto en clases de teoría como en las de prácticas de laboratorios, pudiéndose trabajar tanto en pequeños grupos de trabajo como individualmente.

Por otro lado, en las prácticas de laboratorio o Enseñanzas Prácticas de Desarrollo (EPD) se exponen las ideas fundamentales desarrolladas de una manera básica, se introduce al alumno en la resolución de problemas mediante unos experimentos



GUÍA DOCENTE

guiados, y se enumeran una serie de ejercicios y problemas que el alumno debe resolver. Aunque se potenciará principalmente el trabajo individual y autónomo, esta actividad permite también el trabajo en pequeños grupos de dos o tres alumnos.

Todas estas actividades formativas estarán además complementadas con soporte a través de herramientas Web como la herramienta de Campus Virtual.

GUÍA DOCENTE

7. EVALUACIÓN

CONVOCATORIA DE CURSO:

La evaluación de la asignatura se acogerá al modelo de evaluación continua y sólo será aplicable para la convocatoria de curso. Aquellos alumnos que no superen la asignatura en dicha convocatoria, se podrán evaluar en la convocatoria de recuperación como se describe más adelante.

La evaluación se basará principalmente en los conocimientos adquiridos tanto en clase de teoría como en el aula de informática y se realizará según las siguientes indicaciones:

En las Enseñanzas Básicas se evaluará la participación en clase, exposición y defensa de trabajos propuestos durante el desarrollo de la teoría y una prueba escrita al final del semestre.

Las Enseñanzas Prácticas y de Desarrollo se evaluarán mediante pruebas en aulas de informática y/o una prueba escrita sobre aspectos tratados en las clases prácticas.

La nota oscilará entre 0 y 10 puntos, y vendrá dada por los porcentajes descritos a continuación:

- Enseñanzas básicas: 50%
- Enseñanzas prácticas y de desarrollo: 50%

El examen escrito se realizará en las fechas oficialmente reservadas para tal efecto y consistirá en la respuesta a preguntas (tipo test y de desarrollo) y la resolución de cuestiones y problemas sobre los contenidos de la asignatura.

Para poder realizar la media de la nota final, el alumno deberá obtener al menos 3 puntos sobre el cómputo de 10 en la parte de enseñanzas básicas y al menos 3 sobre el cómputo de 10 en el examen .

Para la realización de cualquier prueba evaluable no se permitirá el uso o consulta de documentación, salvo indicación expresa del profesor en convocatoria oficial.

CONVOCATORIA DE RECUPERACIÓN

Los estudiantes que no superen alguna de las dos partes de la asignatura (Enseñanzas Básicas y Enseñanzas de Prácticas y Desarrollo) en la convocatoria de curso anteriormente descrita, entendiéndose por superar obtener al menos un 5 sobre 10 en

GUÍA DOCENTE

dicha parte, dispondrán de una convocatoria de recuperación de curso en el mes de junio/julio para evaluarse de la parte no superada.

Para esta convocatoria, la asignatura se evaluará mediante dos pruebas escritas correspondientes a las EB y a las EPD, respectivamente, con un porcentaje de 50% cada prueba y que englobarán todos los contenidos de la asignatura.

8. BIBLIOGRAFÍA GENERAL

Fundamentos de seguridad en redes: aplicaciones y estándares . William Stallings. Prentice Hall, 2005
[https://athenea.upo.es/record=b1357200~S1*spj]

Cryptography and Network Security: principles and practice, 4th edition. William Stallings. Prentice Hall, 2006
[http://athenea.upo.es/record=b1357167~S1*spj]

Seguridad práctica en UNIX e Internet. Simson Garfinkel y Gene Spafford. McGraw-Hill, 1999

Computer security : principles and practice. William Stallings, Lawrie Brown. Pearson Education International

UNE-ISO/IEC 27001:2014 : Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Requisitos. AENOR, 2007

UNE-ISO/IEC 27002:2015 : Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. AENOR, 2015