Universidad Isabel I

Guía Docente de la Asignatura: Fundamentos de Seguridad de la Información

Responsable	Dr. D. David Freire-Obregón					
Facultad	Ciencias y Tecnología					
Titulación	Grado en Ingeniería Informática					
Materia	Ingeniería de Computadores					
Plan	2012					
Carácter	Obligatoria					
Periodo de impartición	Trimestral					
Curso/es	Tercero					
Nivel/Ciclo	Grado					
Créditos ECTS	**Teóricos**	6	**Prácticos**	0	**Total**	6
Lengua en la que se imparte	Castellano					
Datos de Contacto:	Correo electrónico: david.freire@ui1.es					

<table>
<tr><td>Asignaturas de la Materia</td><td>
<table>
<tr><th>Asignaturas</th><th>Carácter</th><th>Curso</th><th>Créditos</th><th>Horas</th></tr>
<tr><td>Arquitectura de computadores.</td><td>OB</td><td>2º</td><td>6</td><td>150</td></tr>
<tr><td>Fundamentos de seguridad de la información.</td><td>OB</td><td>3º</td><td>6</td><td>150</td></tr>
</table>
</td></tr>
<tr><td>Contextualización curricular de la asignatura</td><td>Esta asignatura recoge muchos de los interrogantes abiertos en cuanto a las amenazas existentes en las redes de computadores, aspectos relaciones 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 a lo 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 relativas para garantizar la seguridad, formando a los estudiantes con todas las terminologías y técnicas existentes.

Los objetivos de esta asignatura se recogen en las siguientes destrezas en las que se formará al estudiante:
Entender y relacionar los conceptos básicos relacionados con la seguridad informática.
Conocer la normativa internacional y la legislación relativa a los fundamentos de la seguridad así como la implantación de sistemas de gestión de seguridad de la información.
Saber reconocer y anticiparse a las amenazas tecnológicas a través de mecanismos de seguridad activa y pasiva.
Conocer los conceptos básicos de los algoritmos de cifrado más populares así como la diferencia entre criptografía simétrica y asimétrica.</td></tr>
<tr><td>Prerrequisitos para cursar la asignatura</td><td>Ninguno.</td></tr>
</table>

De Rama	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. CR08: Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados. CR09: Capacidad de conocer, comprender y evaluar la estructura y arquitectura de los computadores, así como los componentes básicos que los conforman. CR14: Conocimiento y aplicación de los principios fundamentales y técnicas básicas de la programación paralela, concurrente, distribuida y de tiempo real.	**Específicas**	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. CE04: Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas.
Propias de la Universidad	CU09: Considerar los valores propios de la Formación Profesional Superior en términos de igualdad formativa y educativa con la universitaria. 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.	**Transversales**	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.

Competencias de la Asignatura	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. CU15: Utilizar una adecuada estructura lógica y un lenguaje apropiado para el público no especialista y escribir con corrección. 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.

Actividades Formativas de la Materia

Trabajo dirigido	ECTS	HORAS	Trabajo autónomo del alumno	ECTS	HORAS
Comunidad de aprendizaje (Aula Virtual)			Actividades de trabajo autónomo individual (Estudio de la Lección).	4	100
Actividades de descubrimiento inducido (Estudio del Caso).	2,88	72	Actividades de aplicación práctica (individuales).	1,44	36
Actividades de Interacción y colaboración (Foros-Debates de apoyo al caso y a la lección).	0,96	24	Lectura crítica, análisis e investigación.	1,8	45
Actividades de aplicación práctica (grupal online).	0	0	Actividades de evaluación.	0,2	5
Presentaciones de trabajos y ejercicios.	0	0	*Prácticas externas.*	0	0
Seminarios.	0	0	*Prácticas de iniciación profesional.*	0	0
Interacción alumno-tutor (Aula Virtual).			Trabajo Fin de Grado.	0	0
Tutorías.	0,16	4			
Presentaciones de trabajos y ejercicios propuestos.	0,32	8			
Actividades de evaluación.	0,24	6			
Total	**4,56**	**114**	**Total**	**7,4**	**186**

Actividad	Descripción
Trabajo dirigido.	
Comunidad de aprendizaje (Aula Virtual).	
Actividades de descubrimiento inducido (Estudio del Caso).	Actividades en las que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando, en el Aula Virtual y de manera colaborativa, una situación real o simulada que le permitirá realizar un primer acercamiento a los diferentes temas de estudio.
Actividades de Interacción y colaboración (Foros-Debates de apoyo al caso y a la lección).	Actividades en las que se discutirá y argumentará acerca de diferentes temas relacionados con las asignaturas de cada materia y que servirán para guiar el proceso de descubrimiento inducido.
Actividades de aplicación práctica (grupal online).	Incluye la resolución de problemas, elaboración de proyectos y actividades similares que permitan aplicar los aspectos conceptuales, procedimentales y actitudinales trabajados en otras partes de las asignaturas.

Presentaciones de trabajos y ejercicios.	Incluye la elaboración conjunta en el Aula Virtual y, en su caso, defensa virtual de los trabajos y ejercicios solicitados conforme a los procedimientos de defensa que se establezcan en las guías docentes.
Seminarios.	Incluye la asistencia presencial o virtual a sesiones en pequeño grupo dedicadas a temáticas específicas de cada asignatura.
Interacción alumno-tutor (Aula Virtual).	
Tutorías.	Permiten la interacción directa entre docente y alumno para la resolución de dudas y el asesoramiento individualizado sobre distintos aspectos de las asignaturas.
Presentaciones de trabajos y ejercicios propuestos.	Incluye la elaboración individual, presentación y, en su caso, defensa virtual de los trabajos y ejercicios solicitados conforme a los procedimientos de defensa que se establezcan en las guías docentes.
Actividades de evaluación.	*Véase información al respecto en el apartado siguiente.*
Trabajo Autónomo del alumno.	
Actividades de trabajo autónomo individual (Estudio de la Lección).	Trabajo individual de los materiales utilizados en las asignaturas, aunque apoyado por la resolución de dudas y construcción de conocimiento a través de un foro habilitado para estos fines. Esta actividad será la base para el desarrollo de debates, resolución de problemas, etc.
Actividades de aplicación práctica (individuales).	Incluye el trabajo individual en la resolución de problemas, elaboración de proyectos y actividades similares que permitan aplicar los aspectos conceptuales, procedimentales y actitudinales trabajados en otras partes de la asignatura.
Lectura crítica, análisis e investigación.	Se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación. Se incluyen a modo de ejemplo, recensiones de libros o crítica de artículos y proyectos de investigación.
Actividades de evaluación.	*Véase información al respecto en el apartado siguiente.*

Actividades Formativas de la Asignatura	**Actividad**	**Descripción**
	Trabajo dirigido.	
	Comunidad de aprendizaje (Aula Virtual).	
	Actividades de descubrimiento inducido (Estudio del Caso).	Actividades en las que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando, en el Aula Virtual y de manera colaborativa, una situación real o simulada que le permitirá realizar un primer acercamiento a los diferentes temas de estudio.
	Actividades de Interacción y colaboración (Foros-Debates de apoyo al caso y a la lección).	Actividades en las que se discutirá y argumentará acerca de diferentes temas relacionados con las asignaturas de cada materia y que servirán para guiar el proceso de descubrimiento inducido.
	Actividades de aplicación práctica (grupal online).	Incluye la resolución de problemas, elaboración de proyectos y actividades similares que permitan aplicar los aspectos conceptuales, procedimentales y actitudinales trabajados en otras partes de las asignaturas.
	Presentaciones de trabajos y ejercicios.	Incluye la elaboración conjunta en el Aula Virtual y, en su caso, defensa virtual de los trabajos y ejercicios solicitados conforme a los procedimientos de defensa que se establezcan en las guías docentes.
	Interacción alumno-tutor (Aula Virtual).	
	Presentaciones de trabajos y ejercicios propuestos.	Incluye la elaboración individual, presentación y, en su caso, defensa virtual de los trabajos y ejercicios solicitados conforme a los procedimientos de defensa que se establezcan en las guías docentes.
	Trabajo Autónomo del alumno.	
	Actividades de trabajo autónomo individual (Estudio de la Lección).	Trabajo individual de los materiales utilizados en las asignaturas, aunque apoyado por la resolución de dudas y construcción de conocimiento a través de un foro habilitado para estos fines. Esta actividad será la base para el desarrollo de debates, resolución de problemas, etc.
	Actividades de aplicación práctica (individuales).	Incluye el trabajo individual en la resolución de problemas, elaboración de proyectos y actividades similares que permitan aplicar los aspectos conceptuales, procedimentales y actitudinales trabajados en otras partes de la asignatura.

	Lectura crítica, análisis e investigación.	Se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación. Se incluyen a modo de ejemplo, recensiones de libros o crítica de artículos y proyectos de investigación.
	Actividades de evaluación.	
Proceso de Aprendizaje	Exposición esquematizada de cómo organizaría el profesor el proceso de enseñanza-aprendizaje de la asignatura: • **Estudio de caso real de aplicación práctica**: Se presenta un estudio de caso real que sirve al alumno para ir desarrollando las distintas competencias a medida que va adquiriendo los conocimientos de la materia. • **Contenidos teóricos**: Dentro de los contenidos de cada unidad. • **Foros de Dudas**: Los alumnos y alumnas podrán exponer posibles dudas para que el equipo docente pueda solventarlas. • **Foros de Debate**: A través de un trabajo colaborativo asíncrono, los alumnos y alumnas deberán debatir cuestiones planteadas en las distintas unidades, intentando aportar un valor añadido a las propuestas del resto de compañeros. • **Lectura crítica, análisis e investigación**: Se propondrá el estudio de diversas técnicas criptográficas a fin de que el alumno argumente las bondades o debilidades de cada una de las técnicas desarrolladas. • **Actividades de interacción y colaboración**: Se plantearán trabajos que se podrán realizar en grupo de forma colaborativa.	
Orientaciones al estudio	Se trata de una asignatura donde es importante la reflexión. Es fundamental conocer las herramientas de las que disponemos, pero no debemos confundir la cantidad a la hora de hacer ejercicios con la calidad de cada ejercicio. Para un buen diseño de la seguridad de un sistema informático, la lectura detenida y el proceso de reflexión son esenciales. Entender bien los conceptos ayudará a un mejor diseño. Para ello puede preguntar directamente al profesor a través de los foros de dudas, así como compartir consejos con el resto de los compañeros. Una vez comprendamos el problema en el mundo real y conozcamos las herramientas de las que disponemos, la implantación no supondrá un problema mayor.	
Resultados de Aprendizaje de la Materia	Al completar con éxito esta materia, el alumno:[1] • Explica las diferentes clasificaciones de arquitecturas paralelas. • Distingue entre procesamiento paralelo y procesamiento distribuido, y los asocia con las arquitecturas que se utilizan para implementarlos. • Relaciona el paralelismo implícito en una aplicación con las arquitecturas que lo aprovechan. • Describe lo que hace un compilador y el programador para aprovechar una arquitectura ILP, así como distingue entre las prestaciones del procesador, las del compilador y las del programa que ejecute el computador.	

1 Todos los resultados de aprendizaje del módulo profesional '0378. Seguridad y Alta disponibilidad', más otros propios definidos por la Universidad Internacional Isabel I de Castilla, han sido incluidos en la asignatura 'Fundamentos de seguridad de la información'. Estos resultados están marcados con el símbolo '*' y han sido obtenidos del Anexo I del Real Decreto 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas.

	• Describe la estructura y organización de arquitecturas multihebra, multinúcleo y multiprocesador. • Explica lo que hace un compilador para aprovechar una arquitectura multinúcleo y multiprocesador. • Expresa un algoritmo de forma apropiada para que se pueda ejecutar en multinúcleos y multiprocesadores, así como escribe código que aproveche dicha arquitectura. • Explica la necesidad de mantener coherencia entre caches y entre cache y memoria principal, y afronta el análisis y diseño de protocolos de mantenimiento de coherencia • 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.
Resultados de Aprendizaje de la Asignatura	• 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*.

Plan de Evaluación	En el sistema de evaluación de la Universidad Internacional Isabel I de Castilla, en coherencia con la consecución gradual de competencias y resultados de aprendizaje que se ha descrito en la metodología, se dará preferencia a la evaluación continua complementada con una evaluación final presencial en cada unidad trimestral. Estas evaluaciones finales presenciales permiten obtener garantías respecto a la identidad del estudiante a la que se refiere la Guía de Apoyo para la elaboración de la Memoria de verificación de títulos oficiales universitarios (Grado y máster[2]) y a la veracidad del trabajo realizado durante el proceso de aprendizaje online, puesto que una parte importante de estas pruebas finales consiste en pruebas de verificación de la evaluación continua. Ésta será, por tanto, la vía preferente y recomendada por la Universidad para la obtención de los mejores resultados por parte del estudiante. Sin embargo, es voluntad de esta Universidad ofrecer también una respuesta adecuada para aquellas personas que, por razones personales o profesionales, no pueden hacer un seguimiento de las asignaturas mediante el sistema de evaluación continua. No podemos olvidar que el perfil característico del estudiante de las universidades no presenciales se corresponde con personas de más de 25 años, en muchos casos con otros estudios universitarios y con responsabilidades profesionales y personales que deben compatibilizar con sus estudios online. Teniendo en cuenta ambas perspectivas, el sistema de evaluación de la Universidad Internacional Isabel I de Castilla queda configurado de la siguiente manera: • **Opción 1.** Evaluación continua más evaluación final. Los estudiantes que opten por esta vía podrán obtener hasta el 60% de la nota final a través de las actividades que se planteen en la evaluación continua. El 40% restante se podrá obtener en la prueba de evaluación final que se realizará de manera presencial. Esta prueba tendrá una parte dedicada a la verificación del trabajo realizado por el estudiante durante la evaluación continua (que se corresponde con el 60% de la nota final) y otra parte en la que realizarán diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura. La no superación de la parte de verificación implica que la calificación de la evaluación continua no se tendrá en cuenta y, por tanto, el 100% de la nota dependerá del resultado obtenido en la prueba final de evaluación de competencias. • **Opción 2.** Evaluación final. Para los estudiantes que opten por esta vía, el 100% de la nota de la asignatura depende del resultado obtenido en esta prueba de evaluación final. Tanto en el proceso de información previa como en la formalización de la matrícula, el tutor informará de la existencia de esta posibilidad y valorará conjuntamente con cada persona su experiencia previa en la temática de la asignatura y otros factores que puedan influir en el resultado final. Todos los estudiantes, independientemente de la opción seleccionada, tendrán derecho a una convocatoria extraordinaria de la prueba final de evaluación de competencias que se realizará después de finalizadas las pruebas de evaluación final ordinaria del conjunto de tres trimestres. Para los estudiantes de evaluación continua que no hayan superado la verificación y que también hayan suspendido la prueba de evaluación de competencias ordinaria, el 100% de la nota final dependerá del resultado obtenido en esta convocatoria extraordinaria o "Prueba de conjunto".

[2] Versión 0.1 - 22/03/2011 (Disponible en: http://www.aneca.es/content/download/10717/120032/file/verifica_guia_11°324.pdf)

Opciones	Seguimiento de la Evaluación Continua (EC)	Ponderación valor%
Opción 1.	Si	60%
Opción 2.	No	0%

→

Opciones	Examen final de *verificación* de la EC	Examen final de validación de competencias	Total
Opción 1.	Superado.	40%	100%
	No superado.	100%	100%
Opción 2.	No.	100%	100%

Tabla. Sistema de evaluación.

Nota: Si no se supera la *verificación* se pasa de la Opción 1 de evaluación a la Opción 2.

Los alumnos que no superen alguno/s de los exámenes finales trimestrales de validación de competencias pasarán a la evaluación extraordinaria que se celebrará un mes después de cada conjunto de tres trimestres y que se denominará "Prueba de conjunto".

Finalmente, las Prácticas externas y el Trabajo Fin de Grado (TFG) tendrán su propio sistema de evaluación, que se especificará en las Guías docentes correspondientes. El TFG, en todo caso, deberá ser defendido por el estudiante ante una Comisión de Evaluación.

El sistema de evaluación final será común para todas las asignaturas de la materia y se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. Las pruebas de evaluación, on-line o presenciales, se clasifican de la siguiente forma (Montanero et al., 2006[3]):

1. Pruebas para evaluar competencias relacionadas con la comprensión, análisis, expresión de información (1, 2, 3, 4, 12).
2. Pruebas para evaluar competencias relacionadas con la aplicación de técnicas, procedimientos o protocolos de actuación y resolución de problemas (5, 6, 7, 13).
3. Pruebas para evaluar competencias relacionadas con la capacidad de investigar, pensar o actuar con creatividad y comunicarse verbalmente (8, 9, 12).
4. Pruebas para evaluar otras competencias profesionales, sociales y personales de carácter transversal (6, 9, 10, 11, 12).

[3] Montanero, M.; Mateos, V. L.; Gómez, V.; Alejo, R.: Orientaciones para la elaboración del Plan Docente de una Asignatura. Guía extensa. Badajoz, Universidad de Extremadura, Servicio de Publicaciones. 2006

Estrategias Evaluativas	Componentes de las competencias		
	Saber Competencias técnicas	**Saber Hacer Competencias metodológicas**	**Saber ser-estar Competencias sociales y personales**
Pruebas objetivas (tipo test).	x		
Pruebas semiobjetivas (preguntas cortas).	x		
Pruebas de desarrollo.	x		
Entrevista oral (en determinadas áreas).	x		x
Solución de problemas.	x	x	
Análisis de casos o supuestos prácticos.	x	x	x
Registros de observación sistemática.	x		
Proyectos y trabajos.	x	x	x
Entrevista (tutoría ECTS).	x	x	x
Pruebas de ejecución.	x	x	x
Solución de problemas.	x	x	x
Prueba de evaluación presencial.	x	x	x
Otros.			

Tabla. Estrategias o procedimientos de evaluación.

Los procedimientos de evaluación, al igual que ocurre con las actividades, se integran en el Sistema de Garantía Interna de Calidad (SGIC) de esta Universidad, de manera que la información recogida en cada trimestre se tendrá en cuenta en posteriores implementaciones de las asignaturas. La información acerca de la evaluación formará parte del compromiso público de la Universidad Internacional Isabel I de Castilla con sus estudiantes, de manera que las Guías docentes proporcionarán la información precisa sobre cómo se va a realizar el seguimiento de su trabajo y en qué va a consistir el sistema de evaluación de cada asignatura.

El sistema de calificaciones previsto para esta titulación se ajusta al 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, que en su artículo 5, respecto al Sistema de calificaciones establece lo siguiente:

	• La obtención de los créditos correspondientes a una materia comportará haber superado los exámenes o pruebas de evaluación correspondientes. • El nivel de aprendizaje conseguido por los estudiantes se expresará con calificaciones numéricas, que se reflejarán en su expediente académico junto con el porcentaje de distribución de estas calificaciones, sobre el total de alumnos que hayan cursado los estudios de la titulación en cada curso académico. • La media del expediente académico de cada alumno será el resultado de la aplicación de la siguiente fórmula: suma de los créditos obtenidos por el alumno multiplicados cada uno de ellos por el valor de las calificaciones que correspondan, y dividida por el número de créditos totales obtenidos por el alumno. • Los resultados obtenidos por el alumno en cada una de las materias del plan de estudios se calificarán en función de la siguiente escala numérica de 0 a 10, con expresión de un decimal, a la que podrá añadirse su correspondiente calificación cualitativa: 0-4,9: Suspenso (SS). 5,0-6,9: Aprobado (AP).7,0 -8,9: Notable (NT).9,0 -10: Sobresaliente (SB). • Los créditos obtenidos por reconocimiento de créditos correspondientes a actividades formativas no integradas en el plan de estudios no serán calificados numéricamente ni computarán a efectos de cómputo de la media del expediente académico. • La mención de Matrícula de Honor podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9.0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola Matrícula de Honor.
Sistema de Calificación	Ponderación de la Evaluación Continua dentro del Proceso: 60% • Estudio de Caso Real de aplicación práctica: 10% • Contenidos teóricos/Texto Canónico: 25% • Foros de Debate:10% • Trabajo Colaborativo: 15% Ponderación de la Evaluación Final dentro del Proceso: 40% • Prueba de Contenidos + Prueba de Validación del Alumno/a

Introducción	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.

Breve Descripción de los Contenidos	• UD 1: Conceptos Básicos
	  ○ La información.
	  ○ Los principios de la seguridad.
	  ○ Firmar vs. Cifrar.
	  ○ Clasificación de seguridad.
	• UD2: Normativa y Legislación
	  ○ Normativa.
	  ▪ ISO 27000.
	  ▪ ISO 27001.
	  ▪ ISO 27002.
	  ▪ Otras normas ISO 2700X relevantes.
	  ▪ Sistema de Gestión de la Seguridad de la Información.
	  ○ Legislación.
	  ▪ LO15/1999
	  ▪ L59/2003
	  ▪ RD1720/2007
	  ▪ RD3/2010
	• UD3: Amenazas Tecnológicas
	  ○ Los atacantes.
	  ○ Ataques.
	  ▪ Ataques pasivos.
	  ▪ Ataques activos.
	  ○ Estrategia para un ataque.
	  ○ Redes sociales.
	• UD4: Mecanismos de Seguridad Pasiva
	  ○ Conceptos clave.
	  ○ Copias de seguridad.
	  ○ Seguridad del entorno.
	  ○ Seguridad Perimetral.

	○ Sistemas de alimentación ininterrumpida. • UD5: Mecanismos de Seguridad Activa ○ La Seguridad Activa. ○ Contraseñas y listas de control de acceso. ○ El servidor proxy. ○ Cortafuegos (Firewall). ○ Alta disponibilidad. • UD6: Criptografía ○ Conceptos básicos. ○ Criptoanálisis. ○ Criptografía simétrica. ○ Criptografía asimétrica. ○ Infraestructura de clave pública (PKI). ○ Tipos de cifrado. ▪ Cifrado en flujo. ▪ Cifrado en bloques

Bibliografía Básica	• Fundamentos de seguridad en redes. W. Stallings. [2ª edición]. Pearsons, 2010. ISBN 9788420540023 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. • Seguridad en las comunicaciones y en la información. G. Díaz-Orureta. [1ª edición]. Universidad Nacional de Educación a Distancia (Madrid), 2004. ISBN 8436249755 Libro muy completo. Al igual que la anterior recomendación tiene un índice bien estructurado para la identificación de contenidos. Especialmente relevante si se desea hacer un profundización más exhaustiva sobre alguno de las unidaes didácticas expuestas.
Bibliografía Complementaria	• Enciclopedia de la Seguridad Informática. 2ª Edición Tapa blanda de Álvaro Gómez Vieites (Autor). RA-MA. • Seguridad Informática: Ethical Hacking Conocer Mejor Defensa. 2ª Edición. Ediciones Eni. • Seguridad Informática. Ethical Hacking. Conocer El Ataque Para Una Mejor Defensa - 2ª Edición. ISBN 978-2746079281. • Auditoria de seguridad informáticaUn libro de Gómez Vieites, Álvaro; González Pérez, María Ángeles. ISBN 978849265074 • Seguridad Informática. McGraw-Hill. Interamericana de España, 2013. ISBN 9788448183967 • Gestión de incidentes de seguridad informática: seguridad informática. Chicano Tejada, Ester. ISBN 9788416207152 • Seguridad Informática: Ethical Hacking Conocer Mejor Defensa. 2ª Edición. Ediciones Eni. • Seguridad Informática. McGraw-Hill. Interamericana de España, 2013. ISBN 9788448183967
Otros Recursos	• Ataque de hombre en medio. https://www.youtube.com/watch?v=WF83CsYgMHM • Entrevista que refleja la sencillez que supone hackear un sistema informático. https://www.youtube.com/watch?v=uvMT-V_4kb8 • Interesante seminario de Chema Alonso acerca del robo de identidad. Muy recomendado. https://www.youtube.com/watch?v=84bO7CUn_xU

	• Interesante charla acerca de consultoría informática. https://www.youtube.com/watch?v=WFwsho6Ae5Y • Explicación básica sobre el concepto de seguridad informática. https://www.youtube.com/watch?v=lskwU3kw29o • Explicación del concepto de cortafuegos (en inglés). https://www.youtube.com/watch?v=XEqnE_sDzSk • Introducción al concepto de seguridad y privacidad (en inglés). https://www.youtube.com/watch?v=zBFB34YGK1U • Identificación y autenticación (en inglés). https://www.youtube.com/watch?v=pZIlaWhfhpQ • Seguridad de la información del software (en inglés). https://www.youtube.com/watch?v=AeFyCGpclwY • Interesante explicación sobre el concepto de malware (en inglés). https://www.youtube.com/watch?v=wn-uVP8HncA • Concepto de denegación de servicio (DoS) (en inglés). https://www.youtube.com/watch?v=0_59AocrBVo • Explicación sobre la intercepción de datos y la encriptación de clave pública (en inglés). https://www.youtube.com/watch?v=IyafQPFxgjU • Identidad digital (en inglés). https://www.youtube.com/watch?v=gCIN6ObEMcI • Identificación básica de los roles del hacker. https://www.youtube.com/watch?v=zQ470q7z91k • Las mayores amenazas en la seguridad en red (en inglés). https://www.youtube.com/watch?v=XGs2ovAYeRU

Comentarios Adicionales