PLAN DOCENTE DE LA ASIGNATURA: Seguridad de la Información
CÓDIGO: 501453
CURSO ACADÉMICO: 2016-17

UNIVERSIDAD DE EXTREMADURA

PROGRAMA DE LA ASIGNATURA

Curso académico: 2016/2017

Identificación y características de la asignatura					
Código	501453			Créditos ECTS	6(4,5+1,5)
Denominación (español)	Seguridad de la Información				
Denominación (inglés)	Information Security				
Titulaciones	Grado en Ingeniería en Telemática (GIT) Grado en Ingeniería Informática: Tecnologías de la Información (GIITI)				
Centro	Centro Universitario de Mérida				
Semestre	5º(GIITI) /7(GIT)	Carácter	Obligatoria		
Módulo	Tecnología Específica en Tecnologías de la Información (GIITI) Tecnología Específica Telemática (GIT)				
Materia	Redes (GIITI) Telemática (GIT)				
Profesor/es					
Nombre		Despacho	Correo-e	Página web	
Juan Arias Masa		40	juanaria@unex.es	http://campusvirtual.unex.es/portal/	
Área de conocimiento	Ingeniería Telemática				
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos				
Profesor coordinador (si hay más de uno)					

Competencias

Competencias Específicas

CE20	Conocimiento de la normativa y la regulación de las telecomunicaciones en los ámbitos nacional, europeo e internacional. (GIT)
CE22	Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos. (GIT)
CE31	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos. ((GIITI))

Competencias Transversales

Anterior verifica CT2.	Comunicar de forma efectiva (en expresión y comprensión) oral y escrita, conocimientos, procedimientos, resultados e ideas relacionadas con las TIC, con especial énfasis, en la redacción de documentación técnica
Nuevo acredita CT8	Uso de las TIC. Nivel 3
Anterior verifica CT11	Tener motivación por la calidad y la mejora continua, actuando con rigor, responsabilidad y ética profesional.
Nuevo acredita 17	Orientación a la calidad. Nivel 2

Temas y contenidos
Breve descripción del contenido
GIT: SEG: Integridad y confidencialidad en la transmisión de la información. Criptografía. Historia y desarrollo actual de la seguridad informática. (CE20, CE22) GIITI: Seguridad de la Información: Integridad y confidencialidad en la transmisión de la información, riesgos y políticas de seguridad en redes telemáticas. (CE31)
Temario de la asignatura
Módulo I. Principios de Seguridad/Introducción
Tema 1. Introducción a la Seguridad Informática Tema 2. Aspectos legales de Seguridad Informática
Módulo II. Criptografía
Tema 3. Introducción a la Criptografía. Tema 4. Criptografía de Clave Privada. Tema 5. Criptografía de Clave Pública. Tema 6. Funciones Resumen.
Módulo III. Seguridad en las Redes: Internet
Tema 7. Seguridad perimetral. Tema 8. Otras herramientas de seguridad. Tema 9. Servicios en redes seguras. Tema 10. Protocolos de Seguridad.
Practica I. Presentación de los entornos de programación de las prácticas. Práctica II. Utilización y análisis de algunas herramientas de seguridad Práctica III. Algoritmos DES y DES-simplificado. Práctica IV. Herramienta PGP.

Actividades formativas

Horas de trabajo del alumno por tema		Presencial			Actividad de seguimiento	No presencial
Tema	**Real GG y SL**	**Total**	**GG**	**SL**	**TP**	**EP**
Presentación		**1**	**1**	**0**	**0**	**0**
1		5	2	0		3
2		7	3	0	1	3
3		15	7	0		8
4		15	7	0		8
5		10	4	0		5
6		11	4	0		7
7		9	4	0		5
8		10	4	0	1	5
9		9	4	0		5
10		6	3	0		3
P1		3	0	1		2
P2		10	0	3	1	7
P3		10	0	6		7
P4		10	0	3		7
Evaluación del conjunto		19	2	2	0	15
Total		150	45	15	3	87

GG: Grupo Grande (100 estudiantes).
SL: Seminario/Laboratorio (prácticas clínicas hospitalarias = 7 estudiantes; prácticas laboratorio o campo = 15; prácticas sala ordenador o laboratorio de idiomas = 30, clases problemas o seminarios o casos prácticos = 40).
TP: Tutorías Programadas (seguimiento docente, tipo tutorías ECTS).
EP: Estudio personal, trabajos individuales o en grupo, y lectura de bibliografía.

Sistemas de evaluación

La normativa oficial publicada en el título GRADO EN INGENIERÍA EN TELEMÁTICA dice:

Sistema de Evaluación	Ponderación mínima	Ponderación máxima
Examen	50	70
Exposición oral de trabajos realizados	0	30
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	10	50
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	10	35

La normativa oficial publicada en el título GRADO EN INGENIERÍA EN TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN dice:

Sistema de Evaluación	Ponderación mínima	Ponderación máxima
Examen	30	60
Exposición oral de trabajos realizados	0	20
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	30	60
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	10	20

Concreción de la normativa:

Sistema de Evaluación	Ponderación
Examen	60% (50 teoria+10 practicas)
Exposición oral de trabajos realizados	5% (exposición de ECTS3)
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	25% (20 de memorias de las practicas+ 5 memorias ECTS)
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	10%

- Para la parte teórica de la asignatura existirá un examen final teórico con un peso del 50% de la nota final.
- La parte práctica se compondrá de los trabajos o tareas entregadas de cada práctica (20% de la nota total) y un examen final de las mismas (10% de la nota total).
  - Las tareas podrán superarse en evaluación continua más el examen final de prácticas, o bien
  - Entregando la tarea de práctica no_presencial más el correspondiente examen final en cualquiera de las convocatorias ordinarias o extraordinarias del presente curso.
- La participación en clase, en foros del aula virtual, grupos de trabajo, etc., tendrá un peso del 10% sobre la nota final, entrando aquí el 50% la evaluación de las competencias transversales asignadas a esta asignatura
- Las actividades ECTS se evaluarán con una memoria (5% de la nota final) y exposición oral/final del trabajo realizado (5% de la nota final), y el cómputo total tendrá un valor del 10% de la nota, entrando aquí el 50% la evaluación de las competencias transversales asignadas a esta asignatura

Resultados del Aprendizaje

- Conoces las principales técnicas criptográficas para asegurar la integridad y privacidad de las comunicaciones en red, como el uso de infraestructura de clave pública, certificados y firma digit
- Conoce las amenazas exteriores o restricciones internas relacionadas con las políticas de seguridad de la información en los entornos de red e implementa escenarios seguros basados en cortafueg corporativos, sistemas de detección de intrusos (IDS) y listas de control de acceso.
- Muestra una gran autonomía e integración en el seno de un equipo de trabajo, tiene una orientación a seguir aprendiendo a lo largo de la vida y tiene motivación por obtener resultados y productos de calidad.
- Se comunica de forma efectiva, con especial énfasis en la lectura y redacción de documentación técnica, sabiendo además analizar y sintetizar información proveniente d diversas fuentes.
- Tiene iniciativa para aportar y/o evaluar soluciones efectivas, alternativas o novedosas a los problemas, tomando decisiones basadas en criterios objetivos.
- Elabora textos correctos en forma y contenido, así como realiza una adecuada exposició posterior.
- Se comunica de forma efectiva, con especial énfasis en la lectura y redacción de documentación técnica, sabiendo además analizar y sintetizar información proveniente d diversas fuentes.
- Tiene iniciativa para aportar y/o evaluar soluciones efectivas, alternativas o novedosas a los problemas, tomando decisiones basadas en criterios objetivos.
- Demuestra capacidad de razonamiento y comprensión en el ámbito teórico y práctico.
- Aprende autónomamente.

Metodología

- Clases expositivas de teoría y problemas: Presentación de los contenidos de la asignatura y planificación de la participación de todos los estudiantes en las distintas tareas. Discusión de aspectos teóricos.
- Enseñanza participativa: Trabajos prácticos en grupos medianos o pequeños.
- Tutorización: Actividad de seguimiento para tutela de trabajos dirigidos, consultas de dudas y asesoría en grupos pequeños o individuales.
- Aprendizaje autónomo mediante el análisis de documentos escritos, la elaboración de memorias, estudio de la materia impartida y desarrollo de los supuestos prácticos planteados.
- Aprendizaje virtual. Uso de herramientas virtuales de comunicación entre profesor y estudiante e incluso entre los estudiantes entre si.
- Las sesiones prácticas utilizarán la metodología de aprendizaje basada en la experimentación mediante la resolución de ejercicios relativos a los conocimientos y habilidades a adquirir.

Bibliografía (básica y complementaria)

- Básica:
  - Aula virtual de la Asignatura:
    i. http://campusvirtual.unex.es/zonauex/avuex/my/
  - Carracedo,04 Justo Carracedo Gallardo “Seguridad en Redes Telemáticas” McGraw-Hill, Madrid 2004
  - Pfleeger,89 Charles P. Pfleeger “Security in Computing” 2ª Edición, Prentice Hall International, Inc., 1997
  - Schneier,93 B. Schneier “Applied Criptography” John Weley & Sons Ltd., 1993 (Ba-2424)
  - Díaz,04 G. Díaz, F. Mur, E. Sancristóbal, M-A. Castro y J. Peire “Seguridad en las Comunicaciones y en la Información” UNED, 2004
- Complementaria:

- Menezes, Alfred; Oorsschof, Paul; Vanstone, Scott. Handbook of Applied Cryptography. CRC Press, 1977. Libro electrónico gratuito disponible en la página Web del autor
- Stallings, William. Cryptography and Network Security. Principles and Practice. Third ed., Prentice Hall International Editions, 2003.
- Pastor, José; Sarasa, Miguel Angel. Criptografía Digital. Colección Textos Docentes; Prensas Universitarias de Zaragoza, 1998.
- Schneier, Bruce. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed., John Wiley & Sons, Inc., 1996
- Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J. Técnicas Criptográficas de Protección de Datos. 2ª ed, Ra-Ma, 2000
- Caballero, Pino. Introducción a la Criptografía. Ra-Ma, Textos Universitarios, 1996.
- Cariacedo Gallardo, Justo. Seguridad en Redes Telemáticas. McGraw Hill, 2004.
- Areitio, Javier. Seguridad de la Información. Redes, informática y sistemas de información. Paraninfo, 2008.

Otros recursos y materiales docentes complementarios

- http://netbeans.org/index_es.html
-

Horario de tutorías

Tutorías Programadas:
* Pendiente del horario del curso, pero serán en el despacho del profesor

Tutorías de libre acceso:

- Pendiente del horario del curso, pero serán en el despacho del profesor

Recomendaciones

Como norma general sería muy positivo tener aprobadas todas las asignaturas de primer curso.
Como norma específica, concreta o particular, se recomienda que al menos las siguientes asignaturas estén superadas y adquiridas las capacidades que en ellas se detallan, a saber:

- Fundamentos de Programación
- Estructuras de Datos y de la Información
- Fundamentos de Computadores