PLAN DOCENTE DE LA ASIGNATURA

Curso académico: 2024/25

Identificación y características de la asignatura				
Código	502299		Créditos ECTS	6
Denominación (español)	Seguridad en Redes Telemáticas			
Denominación (inglés)	*Network Security*			
Titulaciones	Grado en Ingeniería Informática en Ingeniería del Software			
Centro	Escuela Politécnica			
Semestre	7	Carácter	Optativa	
Módulo	Optatividad en Ingeniería del Software			
Materia	Redes Telemáticas			

Profesor			
Nombre	Despacho	Correo-e	Página web
Lorenzo M. Martínez Bravo	Nº 7, Informática	lorenzom@unex.es	Grupo GITACA

Área de conocimiento	Ingeniería Telemática
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos

Competencias

CB1 - Que los estudiantes hayan demostrado 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.
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
CB3 - Que los estudiantes tengan la capacidad de 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.
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
CIS05 - Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.

Contenidos

Breve descripción del contenido

Fundamentos de seguridad de la información. Políticas de seguridad. Tecnologías de seguridad. Seguridad telemática.

Temario de la asignatura

Denominación del tema 1: Fundamentos de Seguridad de la Información y de los Redes.
Contenidos del tema 1: Conceptos básicos de Seguridad. Ataques de seguridad. Servicios de seguridad. Mecanismos de seguridad. Modelos de seguridad en redes. Normas y Estándares. Políticas de Seguridad.
Descripción de las actividades prácticas del tema 1: Análisis y propuesta de políticas de seguridad. Herramientas básicas de seguridad de la información.

Denominación del tema 2: Introducción a la Criptografía.

Contenidos del tema 2: Fundamentos de criptografía. Algoritmos de Cifrado de bloques simétricos. Números aleatorios y seudoaleatorios. Cifrados en flujo y RC4. Modos de operación. **Descripción de las actividades prácticas del tema 2:** Cifrado simétrico usando la JCA.
Denominación del tema 3: Criptografía de Clave pública y Autenticación de mensajes **Contenidos del tema 3:** Principios. Funciones Hash seguras. MACs. Algoritmos de clave pública. Firmas digitales. **Descripción de las actividades prácticas del tema 3:** Cifrado asimétrico y firma digital usando la JCA.
Denominación del tema 4: Distribución de claves y autenticación de usuarios. **Contenidos del tema 4:** Introducción. Distribución de claves simétricas. Kerberos. Distribución de claves públicas. Certificados X.509. Infraestructuras de Clave Pública. Gestión de Identidades. **Descripción de las actividades prácticas del tema 4:** Gestión de claves usando la JCA. Gestión de certificados personales X.509.
Denominación del tema 5: Desarrollo y gestión de sistemas seguros. **Contenidos del tema 5**: Ciclo de desarrollo de sistemas seguros. Gestión segura de sistemas. **Descripción de las actividades prácticas del tema 5:** Análisis de modelos de desarrollo seguro
Denominación del tema 6: Seguridad en el nivel de transporte. **Contenidos del tema 6**: Seguridad en la Web. SSL/TLS. HTTPS. SSH. **Descripción de las actividades prácticas del tema 6:** Análisis de tráfico TLS y SSH.
Denominación del tema 7: Control de Acceso en red. Seguridad en redes inalámbricas. Cloud Security. **Contenidos del tema 7**: Control de acceso en red. EAP. IEE 802.1X. Seguridad inalámbrica. Seguridad en dispositivos móviles. IEEE 802.11. 802.11i. Computación cloud. Seguridad en el cloud. **Descripción de las actividades prácticas del tema 7:** Análisis de tráfico Wifi.
Denominación del tema 8: Correo electrónico seguro. **Contenidos del tema 8**: PGP. S/MIME. DKIM, etc. **Descripción de las actividades prácticas del tema 8:** Análisis de proveedores de correo electrónico.
Denominación del tema 9: Herramientas de seguridad en redes. **Contenidos del tema 9**: Firewalls, IDSs/IPSs, VPNs, Malware. **Descripción de las actividades prácticas del tema 9:** Uso y configuración de herramientas.

Actividades formativas

Horas de trabajo del alumno/a por tema		Horas gran Grupo	Actividades prácticas	Actividad de seguimiento	No presencial
Tema	**Total**	**GG**	**LAB**	**TP**	**EP**
1	10,25	2*	0	0,25	8
2	16,25	3*	4	0,25	9
3	17,5	3	5	0,5	9
4	16,25	3	4	0,25	9
5	14,25	3	3	0,25	8
6	16,5	4	3	0,5	9
7	16,25	4	3	0,25	9
8	15,5	3	3	0,5	9
9	15,25	3	4	0,25	8
Evaluación	12	2	1	0	9
Total	**150**	**30**	**30**	**3**	**87**

GG: Grupo Grande (85 estudiantes) (* Actividades en inglés)
LAB: Prácticas laboratorio (15 estudiantes).
TP: Tutorías Programadas (seguimiento docente, tipo tutorías ECTS).
EP: Estudio personal, trabajos individuales o en grupo, y lectura de bibliografía.

Metodologías docentes

Clases teórico-prácticas en el aula, para el desarrollo de los contenidos fundamentales de la materia; actividades breves, individuales o en grupo que permitan aplicar los conceptos expuestos y resolver problemas, facilitando la participación de los estudiantes.
Sesiones de laboratorio, actividades prácticas, sesiones de laboratorio guiadas, seminarios de resolución de problemas, etc. en grupos bajo la dirección de un profesor.
Tutorías programadas, individuales o en grupos pequeños se realizará un seguimiento más individualizado del estudiante, con actividades de formación y orientación. Principalmente, se utilizarán para el seguimiento de los trabajos planteados, debate sobre alternativas y evaluación de los objetivos alcanzados.
Realización de actividades, trabajos y estudio por parte del estudiante, de manera autónoma, individualmente o en grupo. Las actividades que el estudiante desarrollará de manera no presencial estarán orientadas principalmente al desarrollo de los proyectos y trabajos solicitados, bien individualmente o en grupo.

Resultados de aprendizaje

Domina los conceptos de seguridad de la información y de seguridad informática. Conoce los principales pilares de la seguridad de la información, así como conceptos como amenaza, riesgo y privacidad. Sabe aplica métodos para garantizar la seguridad de la información almacenada en ordenadores y transferida por medios telemáticos.
Comprende los fundamentos de la seguridad de sistemas, sabiendo aplicar dichas técnicas a la seguridad avanzada de sistemas operativos y web. Conoce los fundamentos de la seguridad de la información y de los sistemas informáticos. Domina los conceptos relacionados con las políticas de seguridad en sistemas. Conoce las metodologías, las técnicas y las herramientas para proporcionar seguridad a los sistemas.

Sistemas de evaluación

De acuerdo a la *Normativa de Evaluación de las Titulaciones oficiales de Grado y Máster de la Universidad de Extremadura*, la asignatura puede superarse siguiendo un sistema de evaluación continua o de evaluación global.
De acuerdo a dicha normativa, el estudiante debe elegir el sistema de evaluación a seguir siguiendo el procedimiento indicado que se pondrá a disposición del estudiante (campus virtual de la asignatura, en las primeras semanas del semestre). Por omisión, se entiende que el estudiante elige la evaluación continua.
La evaluación de la asignatura se encuentra dividida en dos grandes bloques: Teoría y Práctica.

Bloque de Teoría

En este bloque se hará hincapié en la adquisición de las competencias y en el logro de los resultados de aprendizaje, desde un punto de vista más conceptual. Para ello, se van a utilizar los siguientes mecanismos de evaluación:

Actividades teóricas

A lo largo del semestre, se propondrán una serie de actividades para su realización de manera individual o grupal. Dichas actividades se realizarán dentro del horario de clase y/o en horario no presencial.
Las actividades pueden ser de diferentes tipos: búsqueda y análisis de información sobre casos, análisis de documentos técnicos, resolución de supuestos, análisis de herramientas, etc. Estas actividades fomentan el trabajo y recibirán una calificación y la realimentación del profesor.

Pruebas escritas

Se realizarán varias pruebas escritas (en papel y/o campus virtual) con preguntas de teoría, ejercicios y problemas sobre los conceptos fundamentales y su aplicación. Las pruebas se distribuyen a lo largo del semestre, cubriendo los diferentes temas.

Bloque de prácticas

Se realizarán, entregarán y evaluarán varias actividades de carácter práctico relacionadas con los contenidos explicados y trabajados en las clases de laboratorio. Además, se contempla la posibilidad de realizar una prueba de evaluación final de dichas actividades prácticas, para comprobar la correcta adquisición de los conocimientos y competencias trabajadas.

Criterios de evaluación

Como ya se ha indicado, la asignatura se puede superar según dos sistemas de evaluación distintos: Evaluación Continua o Evaluación Global.

Evaluación continua

Para superar la asignatura por evaluación continua, se deben superar todos los requisitos mínimos de cada uno los dos bloques: Teoría y Práctica.

Bloque de Teoría:

Como ya se ha indicado, este bloque tiene dos componentes:

Actividades teóricas:

Este bloque se evaluará y superará realizando las actividades propuestas. Su calificación se calculará como la media ponderada de todas las actividades realizadas. No hay un requisito mínimo de nota en este apartado. Algunas actividades serán recuperables, mientras que otras no. Este bloque supone el 30% de la nota del bloque de teoría.

Pruebas escritas:

Se realizarán varias pruebas escritas, que se evaluarán. La nota de este apartado será la media ponderada de todas las pruebas realizadas. Es necesario obtener una nota media mínima de 5; se pueden compensar pruebas suspensas, siempre y cuando se tenga una nota mínima de 4 en dicha prueba. Este bloque supone el 70% de la nota de teoría.

Bloque de Prácticas:

Este bloque se evaluará y superará realizando las actividades prácticas propuestas. Su calificación se calculará como la media ponderada de todas las actividades propuestas. Hay que obtener una nota mínima de 5 en todas las actividades de este bloque. Estas actividades serán recuperables.

La nota de teoría supone el 70% de la nota de la asignatura, mientras que la nota de prácticas supone el 30% restante.

En caso de superar únicamente una de las dos partes, teoría o prácticas, dicha parte se guardará durante todas las convocatorias del curso actual, por tanto, el estudiante sólo tendrá que recuperar y superar la otra parte. Se darán instrucciones concretas de la forma de recuperar la parte no superada.

Evaluación global:

Constará de un examen final que incluirá una parte de teoría y una parte de prácticas, cubriendo todos los contenidos trabajados en la asignatura. Para superar la asignatura, debe obtenerse una calificación mínima de 5, en ambas partes. La nota final se calculará de la misma manera que en la EC, es decir, 70% teoría y 30% práctica.

Bibliografía (básica y complementaria)

Bibliografía:

- *Effective Cybersecurity. A guide to using best practices and standards*. William Stallings, Ed. Addison-Wesley, 2019.
- *Network Security Essentials. Applications and Standards*, William Stallings, Ed. Pearson, 6ª Ed., 2017.

- *Seguridad en Redes*, Chris McNab, Ed. Anaya-Multimedia, 2ª edición, 2008.

Bibliografía recomendada en la biblioteca de la Uex.

Otros recursos y materiales docentes complementarios

Recursos: Aula virtual de la asignatura, disponible en el Campus Virtual de la Universidad de Extremadura.