FICHA IDENTIFICATIVA

Datos de la Asignatura

Código	34896
Nombre	Seguridad informática
Ciclo	Grado
Créditos ECTS	6.0
Curso académico	2023 - 2024

Titulación(es)

Titulación	Centro	Curso	Periodo
1403 - Grado de Ingeniería Telemática	Escuela Técnica Superior de Ingeniería	3	Segundo cuatrimestre

Materias

Titulación	Materia	Caracter
1403 - Grado de Ingeniería Telemática	16 - Administración de Sistemas	Obligatoria

Coordinación

Nombre	Departamento
PEREZ CONDE, CARLOS	240 - Informática
SORIANO GARCIA, FRANCISCO R	240 - Informática

RESUMEN

La seguridad es un atributo esencial de los sistemas informáticos. Incluso en una disciplina como la informática, en la que los cambios son continuos, los requisitos de seguridad cambian a un ritmo especialmente rápido. Este ritmo se debe sobre todo a dos razones. La primera es la dependencia de sistemas informáticos es cada vez mayor, por lo que el nivel de exigencia aumenta. La segunda es la continua aparición de nuevas tecnologías. Estas nuevas capacidades permiten implantar mecanismos de seguridad más refinados, pero al mismo tiempo también posibilitan la realización de ataques más sofisticados, lo que provoca un cambio continuo.

En este contexto, la asignatura está planteada para dar una visión de conjunto de los elementos esenciales de la seguridad de los sistemas informáticos, buscando que el alumno aprenda a seguir este proceso de cambio continuo y sea capaz de mantenerse al día y de utilizar, en cada momento, las técnicas más apropiadas. En este sentido, la asignatura se apoya sustancialmente

en los conceptos específicos introducidos en las asignaturas de redes, sistemas operativos, bases de datos y programación, al mismo tiempo que los complementa con contenidos propios del ejercicio profesional de la seguridad, como el establecimiento de políticas de seguridad, el análisis de vulnerabilidades, la detección de intrusos o el análisis forense.

La asignatura “Seguridad informática” se imparte en el segundo cuatrimestre de tercer curso como parte de la materia “Administración de sistemas".

CONOCIMIENTOS PREVIOS

Relación con otras asignaturas de la misma titulación

No se han especificado restricciones de matrícula con otras asignaturas del plan de estudios.

Otros tipos de requisitos

Se recomienda haber cursado las siguientes asignaturas: Informática, Ampliación de Informática, Sistemas operativos y Arquitectura de redes de computadores. De entre ellas, son especialmente relevantes las dos últimas, por tratar algunos conceptos relacionados con la seguridad que complementan los contenidos estudiados en esta asignatura.

COMPETENCIAS

1403 - Grado de Ingeniería Telemática

- R1 - Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación.
- G4 - Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico de Telecomunicación.
- E1 - Capacidad de construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos.
- E2 - 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.

- E3 - Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis.

RESULTADOS DE APRENDIZAJE

- Diseñar y evaluar la política de seguridad de una organización, incluyendo tanto el análisis previo como la gestión de incidentes (G-4, E-2).
- Diseñar, implantar, mantener y evaluar los mecanismos de seguridad necesarios para garantizar el cumplimiento de la política de seguridad (G-4, R-1, E-2).
- Diseñar, implantar, mantener y evaluar los mecanismos necesarios para detectar incidentes y para poder tratarlos adecuadamente (G-4, E-2).
- Evaluar nuevos productos y tecnologías y, en su caso, aplicarlos para mantener el nivel de seguridad requerido (G-4, R-1, E-2).
- Coordinarse con otros profesionales técnicos (administradores de sistemas, de redes, de bases de datos, de aplicaciones...) para lograr un correcto funcionamiento de los sistemas informáticos (G-4, E-2).
- Informar adecuadamente de las incidencias de seguridad, así como interpretar de forma adecuada los avisos de seguridad lanzados por otros, especialmente los de los centros de respuesta (CERTs) (G-4, E-2).
- Explicar tanto a los usuarios como a los directivos el porqué de las medidas de seguridad (G-4, E-2).

DESCRIPCIÓN DE CONTENIDOS

1. Introducción

Concepto de seguridad
¿Qué queremos proteger y por qué? Política de seguridad
¿Frente a qué? Riesgos y vulnerabilidades
El proceso de la seguridad
Normativas (ética, legislación y estándares, ISACA, ISO 27000, IS2)

2. Mecanismos de seguridad

Esta unidad temática está formada por tres temas:
A- Criptografía
-- Simétrica
-- Asimétrica
-- Hashes
-- Laboratorio
B- Seguridad del nodo
-- Validación y autenticación
-- Control de acceso
-- Programación segura
-- Seguridad del servidor y seguridad del cliente

-- Laboratorio
C- Seguridad perimétrica
-- Tecnologías básicas
-- Arquitecturas de cortafuegos
-- Cortafuegos de aplicaciones
--Laboratorio

3. Detección y tratamiento de intrusiones

Detección de intrusos basada en el host (HIDS)
Detección de intrusos basada en la red(NIDS)
Honeypots y honeynets
Análisis forense
Laboratorio

4. Auditoria y Hacking Ético

Introducción al proceso de auditoría
El test de intrusión y sus tipos
Fases de un ataque/test de intrusión
Herramiehttps://webges.uv.es/uvGuiaDocenteWeb/guia#ntas para el hacking ético

VOLUMEN DE TRABAJO

ACTIVIDAD	Horas	% Presencial
Clases de teoría	30,00	100
Prácticas en laboratorio	20,00	100
Prácticas en aula	10,00	100
Elaboración de trabajos en grupo	10,00	0
Estudio y trabajo autónomo	20,00	0
Lecturas de material complementario	10,00	0
Preparación de actividades de evaluación	20,00	0
Preparación de clases de teoría	20,00	0
Preparación de clases prácticas y de problemas	10,00	0
TOTAL	**150,00**	

METODOLOGÍA DOCENTE

Las actividades formativas se desarrollarán de acuerdo con la siguiente distribución:

- Actividades teóricas. En las clases teóricas se desarrollarán los temas proporcionando una visión global e integradora, analizando con mayor detalle los aspectos clave y de mayor complejidad, fomentando, en todo momento, la participación del alumnado (E-2).
- Actividades prácticas. Complementan las actividades teóricas con el objetivo de aplicar los conceptos básicos y ampliarlos con el conocimiento y la experiencia que vayan adquiriendo durante la realización de los trabajos propuestos. Comprenden los siguientes tipos de actividades presenciales: clases de problemas y cuestiones en aula, sesiones de discusión y resolución de problemas y ejercicios previamente trabajados por el alumnado, prácticas de laboratorio , presentaciones orales, conferencias, tutorías programadas (individualizadas o en grupo) (G-4, E-2)
- Trabajo personal del alumnado. Realización (fuera del aula) de trabajos monográficos, búsqueda bibliográfica dirigida, cuestiones y problemas, así como la preparación de clases y exámenes (estudio). Esta tarea se realizará de manera individual e intenta potenciar el trabajo autónomo. (G-4, R-1, E-2)
- Trabajo en pequeños grupos. Realización, por parte de pequeños grupos de estudiantes (2-4) de trabajos, cuestiones, problemas fuera del aula. Esta tarea complementa el trabajo individual y fomenta la capacidad de integración en grupos de trabajo. (G-4, R-1, E-2).

EVALUACIÓN

Primera Convocatoría

L'assignatura podrà ser avaluada de dues formes distintes, una donant major pes a les activitats presencials i altra amb major pes per a l'examen final. Tots els alumnes tindran com nota final la més alta de les dues.

La asignatura podrá ser evaluada de dos formas distintas, una dando mayor peso a las actividades presenciales y otra con mayor peso para el examen final. Todos los alumnos tendrán como nota final la más alta de las dos.

La evaluación de la asignatura se llevará a cabo en la primera convocatoria mediante:

Evaluación de la teoría y los problemas (TP).

Esta parte tendrá un peso del 75 % de la nota final y será necesario llegar a un 4,5 sobre 10 para promediar.

Evaluación continua (EC), basada en la participación y grado de implicación en el proceso de enseñanza-aprendizaje, teniendo en cuenta la asistencia regular a las actividades presenciales previstas y la resolución de cuestiones y problemas propuestos. Esta parte no es recuperable (G-4, R-1, E-2).

Pruebas objetivas individuales, consistentes en varios exámenes o pruebas de conocimiento, que constarán tanto de cuestiones teórico-prácticas como de problemas. Las pruebas se realizarán hacia la primera mitad del cuatrimestre (denominada T1) y fuera del horario lectivo en el periodo de exámenes (denominada T2). (G-4, E-2).

Cada una de estas pruebas abordará todos los contenidos de la asignatura impartidos hasta el momento de su realización.

La nota de TP se calculará de la siguiente forma:

TP = 0,20 * EC + 0,2* T1 + 0,6 * T2.

Evaluación de las actividades prácticas de laboratorio (L) a partir de la consecución de objetivos en las sesiones de laboratorio. (G-4, E-2)

Estas actividades se realizarán por parejas, su peso será del 25 % sobre la nota final y será necesario llegar a un 4,5 sobre 10 para promediar. Todas las sesiones de laboratorio tendrán el mismo peso sobre la nota final.

En caso de no poder asistir a una sesión, el alumno podrá entregar el trabajo correspondiente a su profesor de laboratorio. La entrega deberá ser en persona, en horario de tutorías y el alumno deberá estar preparado para responder cuestiones sobre la realización de la práctica y para realizar partes de la misma en el momento (con pequeños cambios). Este tipo de entrega tiene que ser realizada antes de que ningún grupo de laboratorio haya realizado la práctica y tendrá una penalización del 20 %.

La nota de la asignatura se conformará en el caso de seguir la evaluación continua como la suma de las partes anteriores del siguiente modo:

Si TP es menor 4,5 o L es menor que 4,5

Nota_Final = Mínimo (TP, L)

En otro caso:

Nota_final = 0,75 * TP + 0,25 * L

En caso de no haber superado la asignatura siguiendo la evaluación continua (o en caso de que la nota calculada de esta segunda forma resultara más favorable para el alumno), la prueba de evaluación T2 será el examen final de la asignatura y TP se calculará de la siguiente forma:

TP = 0,20 * EC + 0,80 * T2

La nota final se calculará de la misma forma que con la evaluación continua.

Segunda convocatoria

En la segunda convocatoria la asignatura se evaluará de la misma forma que en la primera

convocatoria, con las siguientes salvedades:

a.- Se abrirá un plazo de entrega de prácticas con las mismas condiciones que en la primera convocatoria (lógicamente no se realizarán en el laboratorio), salvo que la penalización será del 30 % y que la entrega deberá realizarse antes del examen de la segunda convocatoria.

b.- El examen de la segunda convocatoria sustituirá a la prueba T2.

c.- En la parte EC se mantendrá la nota del alumno.

Adelanto de convocatoria

Para poder solicitar adelanto de convocatoria, los estudiantes deberán haber cursado previamente la asignatura y haber obtenido la nota mínima exigida en la evaluación de las actividades prácticas de laboratorio (L). De esta forma se trata de conciliar el derecho de los estudiantes a dicho adelanto con la metodología docente y el mecanismo de evaluación de la asignatura.

En cualquier caso, el sistema de evaluación se regirà por lo establecido en el Reglamento de Evaluación y Calificación de la Universitat de València para grados y masters

(https://webges.uv.es/uvTaeWeb/MuestraInformacionEdictoPublicoFrontAction.do?accion=inicio&idEdictoSeleccionado=5639).

REFERENCIAS

Básicas

- Referencia b1: Charles P.Pfleeger et altres, Security in Computing, Fifth Edition, Prentice Hall, 2015, ISBN-13: 978-0-13-408507-4
- Referencia b2: Stephen Northcutt et altres, Inside Network Perimeter Security. Sams; 2005, ISBN-13: 978-0672327377
- Referencia b3: Schneier, Bruce. Applied Cryptography : Protocols, Algorithms and Source Code in C, John Wiley & Sons, Incorporated, 2015. ISBN: ISBN:9781119096726, 9781119439028.

Complementarias

- Referencia c1:Elizabeth D. Zwicky et altres, Building Internet Firewalls, O'Reilly Media, Inc 2nd edition;2000, ISBN-13: 978-1-56592-871-8
- Referencia c2: Sammons, John. Waltham, Mass. The basics of digital forensics: the primer for getting started in digital forensics. Syngress, c2012. 1st edition. ISBN: 1-59749-662-6, 1-59749-661-8.
- Referencia c3: John Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2012, ISBN-13: 978-0-12-394397-2
- Referencia c4: B. Carrier, File system forensic analysis, Addison-Wesley Professional; 2005, ISBN-13: 978-0321268174
- Referencia c5: Bruce Nikkel. Practical Linux Forensics. No Starch Press, 2021. ISBN: 1098129784, 9781098129781
- Referencia c6: D. Farmer, W. Venema, Forensic Discovery, Addison-Wesley Professional; 2005, ISBN-13: 978-0201634976