FICHA IDENTIFICATIVA

Datos de la Asignatura

Código	34681
Nombre	Seguridad Informática
Ciclo	Grado
Créditos ECTS	6.0
Curso académico	2019 - 2020

Titulación(es)

Titulación	Centro	Curso	Periodo
1400 - Grado de Ingeniería Informática	Escuela Técnica Superior de Ingeniería	3	Segundo cuatrimestre
1407 - Grado de Ingeniería Multimedia	Escuela Técnica Superior de Ingeniería	4	Segundo cuatrimestre

Materias

Titulación	Materia	Caracter
1400 - Grado de Ingeniería Informática	14 - Sistemas Operativos, Sistemas Distribuidos y Redes	Obligatoria
1407 - Grado de Ingeniería Multimedia	19 - Optatividad	Optativa

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 “Sistemas operativos, sistemas distribuidos y redes”.

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: Programación, Estructuras de datos y algoritmos, 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

1400 - Grado de Ingeniería Informática

- G3 - Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
- G4 - Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos según las competencias específicas establecidas.
- G6 - Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes de acuerdo con los conocimientos adquiridos según las competencias específicas establecidas.
- R1 - 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.

- R5 - Conocimiento, administración y mantenimiento sistemas, servicios y aplicaciones informáticas.
- TI2 - Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.
- TI7 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
- SI2 - 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.

RESULTADOS DE APRENDIZAJE

- Diseñar y evaluar la política de seguridad de una organización, incluyendo tanto el análisis previo como la gestión de incidentes.
- Diseñar, implantar, mantener y evaluar los mecanismos de seguridad necesarios para garantizar el cumplimiento de la política de seguridad.
- Diseñar, implantar, mantener y evaluar los mecanismos necesarios para detectar incidentes y para poder tratarlos adecuadamente.
- Evaluar nuevos productos y tecnologías y, en su caso, aplicarlos para mantener el nivel de seguridad requerido.
- 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.
- 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).
- Explicar tanto a los usuarios como a los directivos el porqué de las medidas de seguridad.

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:
- Criptografía (3 horas TP)
Simétrica
Asimétrica
Hashes
- Seguridad del nodo

Validación y autenticación
Control de acceso
Programación segura
Seguridad del servidor y seguridad del cliente
- Seguridad perimétrica
Tecnologías básicas
Arquitecturas de cortafuegos
Cortafuegos de aplicaciones

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

4. Auditoría y hacking ético

Introducción al proceso de auditoría
El test de intrusión y sus tipos
Fases de un ataque/test de intrusión
Herramientas 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 unavisión global e integradora, analizando con mayor detalle los aspectos clave y de mayor complejidad, fomentando, en todo momento, la participación del alumnado.

Actividades prácticas. Complementan las actividades teóricas con el objetivo de aplicarlos 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)

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.

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.

EVALUACIÓN

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

- 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.
- 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), durante la segunda mitad del cuatrimestre (T2)y fuera del horario lectivo en el periodo de exámenes (denominada T3).

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 = 0,15 * EC + 0,15* T1 + 0,25 * T2 + 0,45 * T3.

- Evaluación de las actividades prácticas de laboratorio (L) a partir de la consecución de objetivos en las sesiones de laboratorio.

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 < 4,5 ó L < 4,5

Nota_Final = Mínimo(TP, TL)

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 T3 será el examen final de la asignatura y TP se calculará de la siguiente forma:

TP = 0,15 * EC + 0,85 * T3

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

En la segunda convocatoria la asignatura se evaluará de la misma forma que en la primera convocatoria, con las siguientes salvedades:

- 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.

- El examen de la segunda convocatoria sustituirá a la prueba T3.

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

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, la evaluación de la asignatura se hará de acuerdo con el Reglamento de evaluación y calificación de la Universitat de València para los títulos de grado y master aprobado por Consejo de Gobierno de 30 de mayo de 2017 (ACGUV 108/2017).

REFERENCIAS

Básicas

- Charles P. Pfleeger; Shari Lawrence Pfleeger; Jonathan Margulies. Security in Computing, Fifth Edition. Prentice Hall, 2015. ISBN-13: 978-0-13-408504-3.
- Stephen Northcutt et altres, Inside Network Perimeter Security. Sams; 2005, ISBN-13: 978-0672327377.

Complementarias

- Elizabeth D. Zwicky et altres, Building Internet Firewalls, O'Reilly Media, Inc 2nd edition;2000, ISBN-13: 978-1-56592-871-8
- C. Pogue et altres, Unix and Linux Forensic Analysis DVD Toolkit. Syngress; 2008, ISBN-13: 978-1597492690
- John Vacca, Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann, 2012, ISBN-13: 978-0-12-394397-2
- B. Carrier, File system forensic analisys, Addison-Wesley Professional; 2005, ISBN-13: 978-0321268174
- Lance Spitzner, Honeypots: tracking hackers, Addison-Wesley Professional, 2002, ISBN-13: 978-0321108951
- D. Farmer, W. Venema, Forensic Discovery, Addison-Wesley Professional; 2005, ISBN-13: 978-0201634976
- Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. John Wiley & Sons, 1996. ISBN: 978-0-471-11709-4

ADENDA COVID-19

Esta adenda solo se activará si la situación sanitaria lo requiere y previo acuerdo del Consejo de Gobierno

1. Contenidos

Sin cambios.

2. Volumen de trabajo y planificación temporal de la docencia

Se mantiene, en la medida de lo posible, el volumen de trabajo, sustituyendo las sesiones presenciales por videos de apoyo para la explicación de contenidos y la realización de demostraciones prácticas, y por foros específicos de Aula Virtual para discusión y resolución de dudas.

La planificación temporal se mantiene a nivel semanal, aunque se han sustituido las actividades presenciales por actividades asíncronas (videos, foros y trabajo con máquinas virtuales).

3. Metodología docente

Las actividades presenciales de teoría se sustituyen por presentaciones locutadas, videos con demostraciones y videos de resolución de problemas y casos prácticos. Además, se habilita un foro específico por tema para fomentar la discusión reflexiva y resolver dudas, completando así el aprendizaje.

Las actividades presenciales de laboratorio incluyen un guion detallado que puede llevarse a cabo usando la máquina virtual de la asignatura. Como con la teoría, se habilita un foro por práctica para fomentar la discusión reflexiva y resolver dudas, como forma de completar el aprendizaje.

4. Evaluación

Modificaciones:

- Se elimina la prueba T2.
- Se aumenta el peso de la evaluación continua (EC) dentro de la parte de teoría y práctica (TP), pasando al 25% de TP.
- Se aumenta el peso de la prueba T1, realizada presencialmente, pasando al 25% de TP.
- Se aumenta el peso de las prácticas de laboratorio (L), pasando al 30% de la nota final (NF).
- Se cambia el examen T3 (examen final) a modalidad no presencial, formado por cuestionarios en Aula Virtual que incluirán preguntas tipo test, de respuesta breve y de resolución de problemas y/o casos prácticos. Las preguntas no serán necesariamente las mismas para todo el alumnado y se podrán establecer franjas de tiempo separadas para diferentes partes de la prueba (por ejemplo, para el test y para las cuestiones). En caso de considerarlo necesario, el profesorado podrá requerir una entrevista personal telemática para que la o el estudiante pueda justificar sus respuestas y demostrar sus conocimientos.
- Se cambia la realización presencial de las prácticas de laboratorio (L) por la entrega de una memoria explicativa del trabajo realizado, que debe acompañar al resto de evidencias ya solicitadas (programas, ficheros de configuración…).

Con estas modificaciones, el cálculo de la nota final (NF) se realizará de la siguiente forma:

TP = Máximo(0,25*EC+0,25*T1+0,5*T3; 0,25*EC+0,75*T3)

L continúa siendo la media aritmética de las 8 sesiones de laboratorio.

Si TP o L < 4,5, NF es el mínimo de las dos.

Si TP y L >= 4,5, NF = 0,7*TP + 0,3*L

En 2ª convocatoria se repetirá el examen T3. Adicionalmente, se permitirá la entrega en línea de prácticas de laboratorio hasta el día de la 2ª convocatoria. Esta entrega tendrá una penalización del 30%.

5. Bibliografía

Ya se utilizaban libros y referencias electrónicas, por lo que no ha sido necesario hacer cambios.