19-20

GRADO EN INGENIERÍA INFORMÁTICA
TERCER CURSO

GUÍA DE ESTUDIO PÚBLICA

SEGURIDAD

CÓDIGO 71013124

UNED

19-20

SEGURIDAD

CÓDIGO 71013124

ÍNDICE

Nombre de la asignatura	SEGURIDAD
Código	71013124
Curso académico	2019/2020
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL
Título en que se imparte	GRADO EN INGENIERÍA INFORMÁTICA - TIPO: OBLIGATORIAS - CURSO: TERCER CURSO / MÁSTER UNIVERSITARIO EN INGENIERÍA Y CIENCIA DE DATOS (complemento) / MÁSTER UNIVERSITARIO EN CIBERSEGURIDAD (complemento)
Nº ETCS	6
Horas	150.0
Periodo	SEMESTRE 2
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

Esta guía presenta las orientaciones básicas que requiere el alumno para el estudio de la asignatura de Seguridad. Por esta razón es muy recomendable leer con atención esta guía antes de iniciar el estudio, para adquirir una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

Seguridad es una asignatura de seis créditos ECTS de carácter obligatorio que se imparte en el segundo semestre del tercer curso de la carrera en la titulación de Grado en Ingeniería Informática dentro de la materia de Redes y Conexión de Dispositivos. Esta asignatura inicia el contacto del alumno con el mundo real de la seguridad informática de sistemas, datos y comunicaciones.

Dentro de esta misma materia, nos encontramos con las siguientes asignaturas:

•*Redes de Computadores*, asignatura de segundo curso de grado de carácter obligatorio.

•*Sistemas distribuidos*, asignatura de tercer curso de grado de carácter obligatorio.

•*Periféricos e Interfaces*, asignatura de cuatro curso de grado de carácter opcional.

El objetivo esencial de la asignatura es adquirir los conocimientos asociados a todos los aspectos del problema de la seguridad informática, orientándolos a la consecución de la creación de una política de seguridad de una organización. En ese sentido, se analizan los problemas de seguridad física y lógica asociados con los componentes hardware (cableado, repetidores, encaminadores, etc.) así como software (sistemas operativos, aplicaciones y protocolos). Se estudian los distintos tipos de ataques a la seguridad, haciendo una taxonomía lo más exhaustiva posible, así como los distintos tipos de defensas posibles. Se estudian las distintas herramientas de defensa habituales como cortafuegos, analizadores de vulnerabilidades, sistemas de detección de intrusiones y otros.

Una posible extensión de esta asignatura la encontramos en 4º curso con la asignatura optativa de "*Teoría de la Información y criptografía básica*" que amplia los contenidos de la asignatura profundizando en los métodos criptográficos.

El nivel de conocimientos alcanzado de la materia está entre bajo y medio, un nivel considerado suficiente para poder integrar con éxito la seguridad informática como un criterio más, y esencial, en cualquier proyecto de ingeniería informática.

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR LA ASIGNATURA

Como se ha descrito previamente esta asignatura, que inicia el estudio de una nueva materia, se apoya fuertemente en los conocimientos y competencias adquiridos en asignaturas de segundo curso. Sin esta base de conocimientos la asignatura presentará un nivel alto de dificultad al alumno que la aborde por primera vez.
En concreto, guarda gran relación con las asignaturas de:

- *Sistemas Operativos.* Por una parte, todos los sistemas operativos ofrecen herramientas de seguridad propias. El conocimiento del funcionamiento del sistema operativo y sus posibilidades nos permiten una primera aproximación a la seguridad. Por otra parte, las herramientas de detección y prevención de ataques se instalar en contextos específicos que incluyen las características del sistema operativo. Así que es recomendable conocer los procesos de instalación y configuración de aplicaciones en el sistema operativo objetivo. Junto que existen vulnerabilidades orientadas a explotar defectos de programación de algunos sistemas operativos.
- *Redes de computadores*. Es evidente que gran parte del proceso de seguridad se va centrar en las redes como origen de posibles amenazas. Por ello es importante conocer los diferentes protocolos de comunicación así como los diferentes elementos de interconexión entre dichas redes, que dan lugar a las arquitecturas de redes. Luego, será fundamental un conocimiento de la arquitectura OSI así como la arquitectura TCP/IP que engloban la mayoría de los protocolos en los que se basa Internet.

Además es recomendable el conocimiento de lenguajes de programación orientado a objetos, tales como Java, Python óC#, que permitan el desarrollo de pequeñas herramientas propias de prevención o detección de intrusiones así como pequeños simuladores de ataques a sistemas informáticos que permitan la realización de actividades prácticas fundamentadas en los contenidos de la asignatura.

EQUIPO DOCENTE

Nombre y Apellidos	ROBERTO HERNANDEZ BERLINCHES
Correo Electrónico	roberto@scc.uned.es
Teléfono	91398-7196
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	MARIA DE LOS LLANOS TOBARRA ABAD
Correo Electrónico	llanos@scc.uned.es
Teléfono	91398-9566
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

HORARIO DE ATENCIÓN AL ESTUDIANTE

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al alumno, dispone de los siguientes recursos:
1. **Tutores en los centros asociados.** Los tutores serán los encargados del seguimiento del aprendizaje del estudiante.
2. **Tutorías presenciales** o **virtuales** en el centro asociado correspondiente.
3. **Entorno Virtual**. A través de CiberUNED el equipo docente de la asignatura pondrá a disposición de los alumnos diverso material de apoyo al estudio, así como el enunciado del trabajo de prácticas. Se dispone además de foros donde los alumnos podrán plantear sus dudas para que sean respondidas por los tutores o por el propio equipo docente. Es el SOPORTE FUNDAMENTAL de la asignatura, y supone la principal herramienta de comunicación entre el equipo docente, los tutores y los alumnos, así como de los alumnos entre sí.
4. **Tutorías con el equipo docente**: los lunes de 15:00 a 19:00 h para el periodo durante el que se desarrolla la asignatura, en el teléfono 913989566 o presencialmente. También en cualquier momento del curso por correo electrónico a llanos@scc.uned.es o en el entorno CiberUNED.
- **Profesora D.ª M.ª de los Llanos Tobarra Abad**
Horario de asistencia al estudiante: Miércoles de 12:00 a 14:00, y de 16:00 a 18:00 horas.

TUTORIZACIÓN EN CENTROS ASOCIADOS

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

En relación con las competencias de la materia, la asignatura Seguridad contribuye al desarrollo de las siguientes competencias, generales y específicas, que son comunes a los dos grados en que se imparte:

- **Competencias de bloque común de la rama de Informática**:
- BC.1 - Capacidad para diseñar, desarrollar, seleccionar y evaluar, aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a los principios éticos y a la legislación y normativa vigente.
- BC.5 - Conocimiento, administración y mantenimiento de sistemas, servicios y aplicaciones informáticas
- **Competencias del bloque tecnológico de Tecnologías de la Información:**
- BTEti.7 - Capacidad de comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
- **Competencias generales:**
- CG.1 - Competencias de gestión y planificación: Iniciativa y motivación. Planificación y organización (establecimiento de objetivos y prioridades, secuenciación y organización del tiempo de realización, etc.). Manejo adecuado del tiempo

•CG.2 - Competencias cognitivas superiores: selección y manejo adecuado de conocimientos, recursos y estrategias cognitivas de nivel superior apropiados para el afrontamiento y resolución de diversos tipos dtareas/problemas con distinto nivel de complejidad y novedad: Análisis y Síntesis. Aplicación de los conocimientos a la práctica Resolución de problemas en entornos nuevos o poco conocidos. Pensamiento creativo. Razonamiento crítico. Toma de decisiones

•CG.5 - Competencias en el uso de las herramientas y recursos de la Sociedad del Conocimiento: Manejo de las TIC. Competencia en la búsqueda de información relevante. Competencia en la gestión y organización de la información.Competencia en la recolecciónde datos, el manejo de bases de datos y su presentación

RESULTADOS DE APRENDIZAJE

El objetivo básico de la asignatura Seguridad es dar una visión completa y clara de los fundamentos básicos de la seguridad informática aplicada. Como resultado del estudio y aprendizaje de los contenidos de esta asignatura el estudiante será capaz de:

RA9. *Comprender el entorno operativo de seguridad de red (NSM) y las buenas prácticas asociadas a la implementación de dicho modelo. Por ello se plantean los siguientes objetivos:*

Objetivo 1. Comprender la trascendencia de introducir (o no) la seguridad como un criterio de diseño en cualquier sistema o aplicación informática.

Objetivo 2.Comprender los problemas más habituales actuales que implica la falta de seguridad en sistemas, aplicaciones y redes.

Objetivo 3.Clasificar los diferentes ataques desde el punto de vista de peligrosidad, organización y necesidad de recursos.

Objetivo 4. Comprender la necesidad de la puesta en marcha de una política de seguridad informática en cualquier organización.

Objetivo 5. Entender la trascendencia para las organizaciones de una correcta implementación de la LOPD (Ley Orgánica de Protección de Datos).

Objetivo 6.Entender la relevancia de la puesta en marcha de un Sistema de Gestión de Seguridad Informática que siga las buenas prácticas recomendadas en los estándares internacionales ISO/IEC 27001 e ISO/IEC 27002.

RA10. *Utilizar toda una gama de herramientas de software libre, entre las que se encuentran Sguil, Argus y Wireshark, para hacer prospecciones en el tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta. Por ello se plantean los siguientes objetivos:*

Objetivo 7. Entender, y saber implantar, las defensas básicas en sistemas operativos, aplicaciones y dispositivos básicos de comunicaciones.

Objetivo 8.Aplicar los conceptos más elementales aprendidos, relacionados con la seguridad en redes, sistemas y datos, a una organización concreta.

Objetivo 9. Comprender qué son los analizadores de vulnerabilidades de seguridad y cómo se usan.

Objetivo 10.Comprender qué son los cortafuegos y herramientas de scanning de seguridad, cómo se usan y qué papel juegan en una política de seguridad.
Objetivo 11.Comprender qué son los sistemas de detección de intrusiones (IDS) y qué papel juegan en una política de seguridad.
Objetivo 12. Conocer herramientas de software libre para el análisis del tráfico de red en busca de datos de contenido completo, de sesión, estadístico y de alerta.
RA11. *Conocer y emplear las mejores herramientas para generar paquetes arbitrarios, explorar defectos, manipular el tráfico y efectuar reconocimientos. Por ello se plantean los siguientes objetivos:*
Objetivo 13. Describir las mejores herramientas para la puesta en marcha de una política de seguridad.
Así mismo, y como resultados de aprendizaje transversales del grado de Ingeniería Informática tenemos los siguientes objetivos:
Objetivo 14. Revisar, conocer y juzgar los conocimientos adquiridos.
Objetivo 15.Reconocer el espacio de trabajo virtual personalizado del curso y diferenciar las herramientas disponibles por parte del equipo docente.
Objetivo 16.Conocer el funcionamiento básico de la entrega de actividades y/o ejercicios prácticos relativos al seguimiento y evaluación de los progresos del curso.

CONTENIDOS

Módulo 1: Conceptos e implementación de la monitorización de la seguridad en redes.

Módulo 2: Prácticas recomendadas en la implantación de procesos de seguridad.

Módulo 3: Sistemas de gestión de la seguridad en redes.

Módulo 4: Análisis de Operaciones Intrusivas y herramientas disponibles.

METODOLOGÍA

La metodología de estudio utiliza la tecnología actual para la formación a distancia en aulas virtuales, con la participación del Equipo Docente, los Profesores Tutores y todos los alumnos matriculados. En este entorno se trabajaran los contenidos teórico- prácticos cuya herramienta fundamental de comunicación será el curso virtual, utilizando la bibliografía básica y el material complementario. Esta actividad del alumno en el aula virtual corresponde aproximadamente a un 10% del tiempo total asignado al estudio de la asignatura.
El trabajo autónomo de estudio, junto con las actividades de ejercicios y pruebas de

autoevaluación disponibles, bajo la supervisión del tutor, con las herramientas y directrices preparadas por el equipo docente, completará aproximadamente un 70% del tiempo de preparación de la asignatura.
Por último esta asignatura tiene además programadas unas prácticas a distancia. Esta actividad formativa representa
aproximadamente el 20% del tiempo dedicado a la asignatura.

SISTEMA DE EVALUACIÓN

TIPO DE PRUEBA PRESENCIAL

Tipo de examen	Examen mixto
Preguntas test	10
Preguntas desarrollo	1
Duración del examen	120 (minutos)

Material permitido en el examen

No hay material permitido.

Criterios de evaluación

La prueba consta de un test de 10 preguntas a contestar en una hoja de lectura óptica y un ejercicio a desarrollar durante un tiempo máximo de 2 horas.
Para superar la prueba se deberá obtener una puntuación mínima de 5 puntos. En cada pregunta del test se proponen cuatro respuestas de las cuales sólo una es correcta. Únicamente puntuarán las preguntas contestadas. Si la respuesta es correcta la puntuación será de 0,75 puntos y si es incorrecta restará 0,25 puntos.
Para la corrección del ejercicio es necesario haber logrado el 50% de los puntos del cuestionario. Es decir, obtener al menos 3,75 puntos de los 7,5 puntos del test.
El ejercicio se valorará con 2.5 puntos.

% del examen sobre la nota final	70
Nota del examen para aprobar sin PEC	7
Nota máxima que aporta el examen a la calificación final sin PEC	7
Nota mínima en el examen para sumar la PEC	5

Comentarios y observaciones

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	Si

Descripción

Cada una de las pruebas a realizar por el estudiante a distancia se encargará de evaluar lo siguiente:

En la primera prueba de evaluación a distancia se evaluarán los conocimientos adquiridos sobre la Unidad I. Esta prueba vale un 20% de la calificación dedicada a las pruebas de evaluación a distancia.

En la segunda prueba de evaluación a distancia se evaluarán los conocimientos adquiridos sobre la Unidad II, en concreto, a la parte dedicada a Cortafuegos. Esta prueba vale un 40% de la calificación dedicada a las pruebas de evaluación a distancia.

En la tercera prueba de evaluación a distancia se evaluarán los conocimientos adquiridos sobre la Unidad II, en concreto, a la parte dedicada a Sistemas de Detección de Intrusos. Esta prueba vale un 40 % de la calificación dedicada a las pruebas de evaluación a distancia.

Con respecto a la pruebas de evaluación a distancia, no será necesario que el estudiante acuda al Centro Asociado para realizar las mismas, ya que éstas podrán realizarse en su totalidad a través del curso virtual. Durante el curso se realizarán tres pruebas, siendo la nota máxima que se puede obtener de 3 puntos

Criterios de evaluación

En términos de calificación:

En la primera prueba de evaluación a distancia vale un 20% de la calificación dedicada a las pruebas de evaluación a distancia.

En la segunda prueba de evaluación a distancia vale un 40% de la calificación dedicada a las pruebas de evaluación a distancia.

En la tercera prueba de evaluación a distancia vale un 40 % de la calificación dedicada a las pruebas de evaluación a distancia.

Cada prueba consistirá en varias preguntas de test y/o ejercicios prácticos. El equipo docente publicará las guías para la realización de los cuestionarios o ejercicios prácticos. Las pruebas de evaluación a distancia se realizarán en la plataforma virtual en las fechas y horarios que se indiquen en dicha plataforma, y se dispondrá de un tiempo límite para contestar y enviar la prueba, pasado ese tiempo la puntuación será de 0 puntos. Sólo se dispondrá de un intento para realizar cada una de las pruebas.

El estudiante debe tener en cuenta que sólo se corregirán las pruebas de evaluación a distancia durante el cuatrimestre en el que se imparte la asignatura. Por tanto, en la convocatoria extraordinaria de septiembre, para que se añada la nota correspondiente a las pruebas de evaluación a distancia a la nota final, es necesario que el estudiante haya entregado las pruebas de evaluación durante el cuatrimestre. No existiendo la posiblidad de su realización en septiembre. En estos casos se mantendrá la nota obtenida en las mismas para la convocatoria de septiembre.

Ponderación de la PEC en la nota final 30

Fecha aproximada de entrega

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s?	No
Descripción	
Criterios de evaluación	
Ponderación en la nota final	0
Fecha aproximada de entrega	
Comentarios y observaciones	

¿CÓMO SE OBTIENE LA NOTA FINAL?

De esta manera la calificación final se calcula usando la siguiente fórmula:

Nota final = 0,7x [nota prueba presencial] + 0,3x (0,2 x [nota de la primera prueba de evaluación] + 0,4 x [nota de la primera segunda de evaluación] + 0,4 x [nota de la tercera prueba de evaluación])

Para aquellos alumnos cuya nota final del curso esté entre 4,5 y 5 puntos, se les ofrecerá la posibilidad de realizar de forma optativa una prueba teórico-práctica de evaluación a distancia. La realización de este ejercicio optativo servirá para subir la nota en 0,5 puntos. Esta práctica optativa solamente se corregirá en el cuatrimestre en el que se imparte la asignatura.

BIBLIOGRAFÍA BÁSICA

ISBN(13):9788436249750
Título:SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es:Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial:U.N.E.D.

Igualmente, el equipo docente ha desarrollado a medida un contenido que intentará actualizar constantemente el temario de la asignatura, que se distribuirá en el curso virtual de la asignatura en formato electrónico bajo licencia Creative Commons.

BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13):
Título:SEGURIDAD EN UNIX Y REDES (http://es.tldp.org/Manuales-LuCAS/doc-unixsec/uni)
Autor/es:Antonio Villalón Huerta ;
Editorial:http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec.pdf

ISBN(13):9780201634662
Título:FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER (2ND EDITION) (2º)
Autor/es:Steven M. Bellovin ; William Cheswick ;
Editorial:Addisson-Wesley

ISBN(13):9788420541105
Título:COMUNICACIONES Y REDES DE COMPUTADORES (7ª)
Autor/es:Stallings, William ;
Editorial:PRENTICE-HALL

ISBN(13):9788420546001
Título:EL TAO DE LA MONITORIZACIÓN DE SEGURIDAD EN REDES (2005)
Autor/es:R. Bejtlich ;
Editorial:PEARSON EDUCACIÓN

ISBN(13):9789688805411
Título:REDES GLOBALES DE INFORMACIÓN CON INTERNET Y TCP/IP
Autor/es:D. E. Comer ;
Editorial:PEARSON-PRENTICE HALL

Los libros de Stalling y Comer son un gran complemento para repasar toda una serie de conceptos, estándares y protocolos de comunicación (especialmente TCP/IP) necesarios como base para la adquisición correcta de conocimientos y capacidades asociadas con los contenidos de la asignatura.
El libro de Cheswick y otros es una muy buena aproximación a los conceptos e implementaciones más inteligentes de los cortafuegos, herramientas con poco más de 20 años de historia, pero que se han convertido en una herramienta imprescindible para la puesta en marcha de cualquier política de seguridad informática para cualquier tipo de organización.
Seguridad en Unix y Redes, aborda de manera global el tema de seguridad, no solo a nivel de las redes de comunicaciones, en entornos Linux/Unix. Abarca desde la securización de componentes hardware hasta el conchero de auditoria (y sus herramientas Unix/Linux asociadas). Se presentan diferentes sistemas operativos basados en Linux junto a sus premisas de seguridad. Dispone de una parte dedicada totalmente a las herramientas de seguridad de redes en entornos Unix, con especial detalle en los sistemas de prevención (cortafuegos) y detección (IDS). Es una obra muy completa que cubre muchos conceptos globales de seguridad como la propia criptografía entre otras
El Tao de la monitorización de Seguridad en redes, aborda de una manera profunda los conceptos básicos sobre el modelo de seguridad de redes en todas sus fases: definición, diseño, implantación y evaluación. Se hace especial hincapié en las herramientas de monitorización de redes, en concreto las disponibles como Open Source, como piezas clave

para la obtención de información sobre posibles ataques que permita detectar problemas en el modelo de seguridad. Se presentan casos prácticos desde el punto de vista de los administradores de la seguridad de red y sistemas para poder evaluar la seguridad desde el punto de vista de un atacante externo.

RECURSOS DE APOYO Y WEBGRAFÍA

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:
•Esta guía de estudio y la guía didáctica de estudio de la asignatura.
•Distintos libros electrónicos gratuitos, algunos interactivos.
•Material desarrollado exprofeso para el curso por el equipo docente
•Apartado de noticias y enlaces interesantes, relacionados con el desarrollo de la asignatura
•Pruebas prácticas de evaluación a distancia.
•Enunciados y soluciones de ejercicios teórico-prácticos que el alumno puede usar como ejercicios de autoevaluación.
•Lista de preguntas frecuentes.

IGUALDAD DE GÉNERO

En coherencia con el valor asumido de la igualdad de género, todas las denominaciones que en esta Guía hacen referencia a órganos de gobierno unipersonales, de representación, o miembros de la comunidad universitaria y se efectúan en género masculino, cuando no se hayan sustituido por términos genéricos, se entenderán hechas indistintamente en género femenino o masculino, según el sexo del titular que los desempeñe.