ASIGNATURA DE MÁSTER:

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Curso 2016/2017

(Código:31106099)

1.PRESENTACIÓN

Esta guía presenta las orientaciones básicas que requiere el estudiante para el estudio de la asignatura de *Seguridad en los Sistemas de Información*. 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.

La asignatura tiene como objetivo profundizar y ampliar la formación del estudiante en relación al mundo de la seguridad informática desde sus distintas perspectivas. Por un lado se presentarán distintas políticas, normativas y certificaciones de seguridad existentes, cubriendo a modo de ejemplo el ISO 27001. Por otro lado, se especializará al estudiante en aquellas tecnologías de seguridad que se consideren más avanzadas, prestando especial atención al análisis, diseño y verificación de protocolos de seguridad avanzados para los Sistemas de Información. Se explorarán otros paradigmas todavía en desarrollo con idea de tener una visión global de las necesidades de seguridad que irán apareciendo con los años.

2.CONTEXTUALIZACIÓN

La asignatura de Seguridad en los Sistemas de Información se trata de una asignatura de cuatro créditos, obligatoria, impartida en el primer semestre del primer curso y pertenece al módulo de Tecnologías Informáticas de la titulación de Máster Universitario de Ingeniería de Informática. Guarda relación con las siguientes asignaturas también disponibles en el mismo Master:

- *Temas Avanzados en Redes e Internet*, asignatura del primer semestre del primer curso de grado de carácter obligatorio.
- Cloud Computing y Gestión de Servicios de Red, asignatura del primer semestre del primer curso de grado de carácter obligatorio.
- *Gestión y mejora de los procesos*, asignatura del primer semestre del primer curso de grado de carácter obligatorio.

Una asignatura fuertemente relacionada con los contenidos desarrollados en esta asignatura y complementaria a los mismos, sin solapamientos, la encontramos en el primer semestre con la asignatura optativa de “Desarrollo de software seguro” que amplía los contenidos de la asignatura profundizando en el desarrollo seguro de aplicaciones, evitando los posibles ataques derivados de bugs de programación.

Las competencias de esta asignatura se pueden consultar en la guía del máster.

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

3.REQUISITOS PREVIOS RECOMENDABLES

Como se ha descrito previamente esta asignatura, que profundiza el estudio de la seguridad en los sistemas informáticos, se apoya fuertemente en los conocimientos y competencias adquiridos en asignaturas del grado de informática. Sin esta base de conocimientos la asignatura presentará un nivel alto de dificultad al estudiante que la aborde por primera vez.

En concreto, guarda gran relación con las materias de:

- *Seguridad* dentro del Grado de Ingeniería Informática.
- *Procesos y herramientas de gestión de la seguridad de redes* en el Grado de Ingeniería en las Tecnologías de la Información.
- *Sistemas Operativos* o en el Grado de Ingeniería Informática o en el Grado de Ingeniería en las Tecnologías de la Información.
- *Fundamentos de Programación* o en el Grado de Ingeniería Informática o en el Grado de Ingeniería en las Tecnologías de la Información.
- *Redes de Computadores* dentro del Grado de Ingeniería Informática. *Redes y Comunicaciones* dentro del Grado de Ingeniería en las Tecnologías de la Información.

Además es necesario *conocer (leer y escribir) el inglés técnico.* Debido a que parte de la bibliografía proporcionada al estudiante puede estar disponible únicamente en inglés, como consecuencia de la novedad de algunos contenidos propuestos en la asignatura.

4.RESULTADOS DE APRENDIZAJE

El objetivo básico de la asignatura *Seguridad en los Sistemas de Información* es ampliar los conocimientos básicos de la seguridad informática aplicada adquirida por los estudiantes durante el grado. Como resultado del estudio y aprendizaje de los contenidos de esta asignatura el estudiante será capaz de:

RA1. Comprender los conceptos avanzados de la seguridad en el tratamiento y acceso de la información en un sistema de información.

Objetivo 1.Comprender la trascendencia y los mecanismos avanzados de introducir 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.Comprender la necesidad de la puesta en marcha de una política de seguridad informática en cualquier organización.

RA2. Conocer los mecanismos avanzados de certificación y garantía de la seguridad en sistemas información.

Objetivo 4.Conocer los principales mecanismos de certificación de la puesta en marcha de un Sistema de Gestión de Seguridad Informática que siga las buenas prácticas recomendadas en los estándares internacionales como la familia ISO 27000, NIST o COBIT.

Objetivo 5.Capacidad de evaluar el cumplimiento en una empresa del seguimiento de un Sistema de Gestión de Seguridad Informático implantada en base a las certificaciones aplicadas.

RA3. Conocer los retos y soluciones de seguridad de los sistemas de información dentro del contexto de Internet.

Objetivo 6.Entender, y saber implantar, las defensas avanzadas en sistemas de la información no tradicionales.

RA4. Diseño, desarrollo y gestión de los mecanismos de la seguridad en Sistemas de Información

Objetivo 7.Conocer herramientas de software libre para el análisis del tráfico de red y monitorización de

eventos en busca de datos de contenido completo, de sesión, estadístico y de alerta para la detección de vulnerabilidades.

Objetivo 8.Conocer mecanismos de recuperación ante incidentes.

Objetivo 9.Conocer mecanismos de realización de análisis forense para el análisis del sistema tras un incidente.

Así mismo, y como resultados de aprendizaje transversales del master tenemos los siguientes objetivos:

Objetivo 10.Revisar, conocer y juzgar los conocimientos adquiridos.

Objetivo 11.Reconocer el espacio de trabajo virtual personalizado del curso y diferenciar las herramientas disponibles por parte del equipo docente.

Objetivo 12.Conocer el funcionamiento básico de la entrega de actividades y/o ejercicios prácticos relativos al seguimiento y evaluación de los progresos del curso.

5.CONTENIDOS DE LA ASIGNATURA

Los contenidos de la asignatura se dividen en cuatro módulos o bloques:

Módulo 1: Diseño Avanzado de un Programa de Seguridad.

Contenidos:

1.1 Construcción de un programa de Seguridad.

1.2 Análisis de riesgos para un programa de seguridad.

1.3 Principios de diseño.

1.4 Políticas, estándares, procedimientos y guías de la seguridad.

Módulo 2: Modelos de Seguridad Avanzados en los Sistemas de Información.

Contenidos:

2.1 Seguridad en contextos de Cloud Computing.

2.2 Seguridad en dispositivos móviles Smartphones e Internet de las Cosas.

2.3 Seguridad en sistemas industriales.

Módulo 3: Gestión de las Operaciones de Seguridad

Contenidos:

3.1 Comunicación e informes.

3.1.1. Métricas y KPIs

3.1.2. Cybersecurity Capability Maturity Model (C2M2)

3.2 Gestión de Cambios

3.2.1 ITIL

3.3 Seguridad Administrativa

3.4 Controles

Módulo 4: Monitorización, Recuperación y Respuesta ante Vulnerabilidades

Contenidos:

4.1 Monitorización de Eventos

4.2 Recuperación ante desastres y continuidad del negocio.

4.2.1 Recuperación ante desastres

4.2.2 Continuidad del Negocio

4.2.3 Backups

4.2.4 Alta disponibilidad

4.3. Respuesta ante vulnerabilidades y Análisis Forense

6.EQUIPO DOCENTE

- ROBERTO HERNANDEZ BERLINCHES
- MARIA DE LOS LLANOS TOBARRA ABAD
- LUIS GRAU FERNANDEZ
- IGNACIO JOSE LOPEZ RODRIGUEZ
- PABLO RUIPEREZ GARCIA

7.METODOLOGÍA

Las diferentes asignaturas que integran este Master, se impartirán todas ellas conforme a la metodología no presencial que caracteriza a la UNED, en la cual prima el autoaprendizaje del estudiante, pero asistido por el profesor y articulado a través de diversos sistemas de comunicación docente-discente. Dentro de estos sistemas, cabe destacar que el Máster en Ingeniería Informática se imparte con apoyo en una plataforma virtual interactiva de la UNED donde el estudiante encuentra tanto materiales didácticos básicos como materiales didácticos complementarios, informaciones, noticias, ejercicios y también permite la evaluación correspondiente a las diferentes materias.

Esta asignatura de 4 créditos ECTS está planificada en 100 horas. El tiempo de las actividades formativas, siguiendo la anterior metodología, se han distribuido de forma orientativa de la siguiente manera:

- Estudio de los contenidos teóricos-prácticos utilizando la bibliografía y los materiales complementarios: 40 horas.
- Tutorías: 10 horas.
- Actividades en la plataforma virtual, incluyendo participación en los debates propuestos en los foros: 10 horas.
- Realización de trabajos autónomos de carácter individual (10 horas) o de carácter colectivo (10 horas): 20 horas.
- Prácticas que incluyen la resolución de casos prácticos así como supuestos: 20 horas.

Tanto los trabajos individuales como los colectivos, además de las prácticas se podrán basar en el uso de software libre, así como de máquinas virtuales o simuladores disponibles que permitan emular diversos casos de estudio

asociados con los objetivos propuestos en la asignatura.

8.BIBLIOGRAFÍA BÁSICA

Comentarios y anexos:

La documentación básica la pondrá el equipo docente a disposición de los estudiantes en el curso virtual.

9.BIBLIOGRAFÍA COMPLEMENTARIA

ISBN(13): 9780071784351
Título: INFORMATION SECURITY: THE COMPLETE REFERENCE (Second Edition)
Autor/es: Mark Rhodes-Ousley ;
Editorial: : MCGRAW-HILL

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9781430261452
Título: BUILDING THE INFRASTRUCTURE FOR CLOUD SECURITY A SOLUTIONS VIEW (1ª edición)
Autor/es: Raghuram Yeluri ; Enrique Castro-Leon ;
Editorial: Apress Open

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9781430263821
Título: THE INFOSEC HANDBOOK: AN INTRODUCTION TO INFORMATION SECURITY
Autor/es: Umesha Nayak ; Umesh Hodeghatta Rao ;
Editorial: Apress Open

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

ISBN(13): 9781593275099
Título: THE PRACTICE OF NETWORK SECURITY MONITORING. (1ª edición)

Autor/es: Richard Bejtlich ;
Editorial: No starch Press

Buscarlo en libreria virtual UNED

Buscarlo en bibliotecas UNED

Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

10.RECURSOS DE APOYO AL ESTUDIO

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 estudiante puede usar como ejercicios de autoevaluación.

11.TUTORIZACIÓN Y SEGUIMIENTO

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al estudiante, dispone de los siguientes recursos:

1. Tutores en los centros asociados. Los tutores serán los encargados del seguimiento y control de las pruebas que constituyen la evaluación continua del estudiante.

2. Entorno Virtual. A través de CiberUNED el equipo docente de la asignatura pondrá a disposición de los estudiantes diverso material de apoyo al estudio, así como el enunciado del trabajo de prácticas. Se dispone además de foros donde los estudiantes 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 estudiantes, así como de los estudiantes entre sí.

3. Tutorías con el equipo docente.

Dra. Llanos Tobarra (llanos@scc.uned.es)

Dr. Roberto Hernández (roberto@scc.uned.es)

Dr. Luis Grau (lgrau@scc.uned.es)

Dr. Pablo Ruipérez (pablo@scc.uned.es)

Dr. Ignacio Lopez (ilopez@scc.uned.es)

12.EVALUACIÓN DE LOS APRENDIZAJES

En esta asignatura se hará uso para la evaluación final de tres elementos: evaluación continua, trabajos o prácticas y prueba presencial, de la siguiente forma:

- Pruebas de evaluación continúa (10%):
  - Autoevaluación: En esta asignatura se plantea a los estudiantes un proceso de autoevaluación, basado en la realización de pruebas de test o ejercicios prácticos guiados ya resueltos. En el módulo de contenidos dentro del entorno virtual los estudiantes podrán encontrar el apartado de "Autoevaluación" donde se alojarán tanto las pruebas como sus soluciones, con las que el estudiante podrá autoevaluar sus conocimientos.
  - Actividades de desarrollo en equipo o debates sobre cuestiones y casos prácticos relevantes para la asignatura que se realizarán a través de los foros disponibles en la plataforma virtual del curso.
  - Pruebas de evaluación a distancia: cuestionarios sobre parte del temario desarrollado en la asignatura. Se propondrá al menos una prueba de evaluación a distancia.
- Trabajos o prácticas (30%): Consistirán en pequeños trabajos prácticos que permitirán comprobar la correcta asimilación de contenidos y la adquisición real de competencias relacionadas. Podrán tener carácter individual o colectivo.
- Examen presencial (60%): Realización de un examen teórico/práctico, que es indispensable aprobar para la superación de la asignatura.

13.COLABORADORES DOCENTES

Véase equipo docente.