18-19

MÁSTER UNIVERSITARIO EN
INGENIERÍA INFORMÁTICA

GUÍA DE ESTUDIO PÚBLICA

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

CÓDIGO 31106099

UNED

18-19

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

CÓDIGO 31106099

ÍNDICE

Nombre de la asignatura	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN
Código	31106099
Curso académico	2018/2019
Título en que se imparte	MÁSTER UNIVERSITARIO EN INGENIERÍA INFORMÁTICA
Tipo	CONTENIDOS
Nº ETCS	4
Horas	100.0
Periodo	SEMESTRE 1
Idiomas en que se imparte	CASTELLANO

PRESENTACIÓN Y CONTEXTUALIZACIÓN

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.

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 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”, en la que se abordan en concreto las aplicaciones y 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 entender y considerar adecuadamente la seguridad informática como un criterio esencial, en cualquier proyecto de ingeniería informática

REQUISITOS Y/O RECOMENDACIONES PARA CURSAR ESTA ASIGNATURA

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. P*arte de la bibliografía proporcionada al estudiante puede estar disponible únicamente en inglés.

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

Nombre y Apellidos	LUIS GRAU FERNANDEZ
Correo Electrónico	lgrau@scc.uned.es
Teléfono	91398-7153
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	IGNACIO JOSE LOPEZ RODRIGUEZ
Correo Electrónico	ilopez@scc.uned.es
Teléfono	91398-7195
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	PABLO RUIPEREZ GARCIA
Correo Electrónico	pablo@dia.uned.es
Teléfono	91398-7159
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	PABLO RUIPEREZ GARCIA
Correo Electrónico	pablo@scc.uned.es
Teléfono	91398-7159
Facultad	ESCUELA TÉCN.SUP INGENIERÍA INFORMÁTICA
Departamento	SISTEMAS DE COMUNICACIÓN Y CONTROL

Nombre y Apellidos	PABLO RUIPEREZ GARCIA
Correo Electrónico	pruip@dia.uned.es
Teléfono	91398-7159
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 estudiante, dispone de los siguientes recursos:
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.
Equipo docente.
Dra. Llanos Tobarra (llanos@scc.uned.es)
Miercoles de 12:00 a 14:00 y 16:00 a 18:00
Dr. Roberto Hernández (roberto@scc.uned.es)
Martes de 15.00 a 19.00 h
Dr. Luis Grau (lgrau@scc.uned.es)
Martes de 15 a 19 horas
Dr. Pablo Ruipérez (pablo@scc.uned.es)
Lunes de 15 a 19 horas
Dr. Ignacio Lopez (ilopez@scc.uned.es)
Lunes de 15 a 19 horas

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE

Competencias Básicas:

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

Competencias Generales:

G1 - Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática.

G2 - Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio.

G4 - Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería en Informática.

G7 - Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.

G8 - Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.

Competencias Transversales:

CT1 - Capacidad para emprender y liderar proyectos innovadores en entornos científicos, tecnológicos y multidisciplinares.

CT2 - Capacidad para tomar decisiones y formular juicios basados en criterios objetivos (datos experimentales, científicos o de simulación disponibles).

Competencias Específicas:

DG2 - Capacidad para la planificación estratégica, elaboración, dirección, coordinación, y gestión técnica y económica en los ámbitos de la ingeniería informática relacionados, entre otros, con: sistemas, aplicaciones, servicios, redes, infraestructuras o instalaciones

informáticas y centros o factorías de desarrollo de software, respetando el adecuado cumplimiento de los criterios de calidad y medioambientales y en entornos de trabajo multidisciplinares.
TI4 - Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.

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.

CONTENIDOS

MÓDULO I: Diseño Avanzado de un Programa de Seguridad

1. Construcción de un programa de seguridad
1. El concepto de seguridad
2. Frameworks y estándares
3. Construcción de un programa de seguridad

2. Gestión de riesgos para un programa de seguridad
1. Vulnerabilidades y amenazas
2. Gestión y análisis de riesgos
3. Gestión y análisis de riesgos en ISO 27001

3. Principios de Diseño
1. Las tres Ds
2. CIA
3. Modelos básicos de defensa
4. Buenas prácticas

4. Políticas, estándares, procedimientos y guías de seguridad
1. Definición de políticas
2. Definición de procedimientos y guías
3. Documentación en ISO 27001

MÓDULO II: Gestión de las Operaciones de Seguridad.

2.1. Métricas de la Seguridad
2.1.1. Métricas y KPIs
2.1.2. Cyber Capability Mature Model

2.2 Gestión de cambios y documentación
2.2.1. ITIL

2.3 Seguridad Administrativa

2.4 Controles

2.4.1 Diseño de controles en ISO 27001
2.4.2 Implementación de Controles
2.4.3 Monitorización, revisión y medida del proceso de ISMS en ISO 27001

MÓDULO III: Monitorización, Recuperación y Respuesta ante Vulnerabilidades.

4.1 Monitorización de Eventos
4.1.1 Controles dela seguridad
4.1.2 Monitorización de la actividad
4.2 Recuperación ante desastres y continuidad del negocio
4.2.1 Recuperación ante desastres y continuidad del negocio
4.2.2 Plan de Continuidad del Negocio
4.2.3 Backups
4.2.4 Alta Disponibilidad
4.3. Respuesta ante vulnerabilidades y análisis forense
4.3.1 Respuesta ante incidentes
4.3.2 Análisis forense

MÓDULO IV: Modelos de Seguridad Avanzados en los Sistemas de Información.

4.1 Seguridad en contextos de Cloud Computing.
4.2 Seguridad en dispositivos móviles Smartphones e Internet de las Cosas.
4.3 Seguridad en infraestructuras críticas.

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.

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

Ninguno

Criterios de evaluación

La **prueba presencial** consistirá en un **examen teórico/práctico** a realizar en un **tiempo máximo de 2 horas**. Como se ha indicado, la **nota máxima** que se puede alcanzar en esta prueba es de **6 puntos** en la nota final y **para superarla** se deberá obtener una **puntuación mínima** de **3 puntos**. Durante la realización de la prueba no se podrá utilizar ningún tipo de material. La **prueba presencial** se realizará en el Centro Asociado que corresponda a cada estudiante, en las fechas y horarios establecidos por la UNED. Esta prueba consistirá en un cuestionario de 10 preguntas tipo test junto con un ejercicio de desarrollo. El cuestionario es eliminatorio y debe superarse el 60% del mismo para que el ejercicio de desarrollo sea corregido.

% del examen sobre la nota final	60
Nota del examen para aprobar sin PEC	8,2
Nota máxima que aporta el examen a la calificación final sin PEC	6
Nota mínima en el examen para sumar la PEC	5

Comentarios y observaciones

CARACTERÍSTICAS DE LA PRUEBA PRESENCIAL Y/O LOS TRABAJOS

Requiere Presencialidad	No

Descripción

A lo largo del curso se propondrán **al menos tres trabajos prácticos** relacionados con:
Análisis de riesgos
Análisis de vulnerabilidades
Análisis forense y respuesta ante incidentes.
Cada trabajo práctico tendrá asociado una guía donde se explique claramente los objetivos, el desarrollo, así como los criterios de corrección. Ambos estarán fuertemente correlacionados con el contenido de la asignatura.

Criterios de evaluación

Con respecto a las **trabajos prácticos**, 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 al menos tres trabajos prácticos**, siendo la **nota máxima** que se puede obtener de **2 puntos de la nota final**. La entrega de los **trabajos prácticos se realizarán en la plataforma virtual** en las fechas que se indiquen en dicha plataforma para enviar la prueba, pasado ese tiempo la puntuación será de 0 puntos.
El estudiante deberá obtener al menos el 50% de la nota posible mediante la pruebas de evaluación a distancia para superar la asignatura.
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, para poder presentarse en la convocatoria extraordinaria de septiembre, es necesario que el estudiante haya entregado las pruebas de evaluación que son condición necesaria para aprobar durante el plazo establecido en el cuatrimestre. En estos casos se mantendrá la nota obtenida en las mismas para la convocatoria de septiembre.

Ponderación de la prueba presencial y/o los trabajos en la nota final	20% nota final
Fecha aproximada de entrega	10/01/2019
Comentarios y observaciones	

PRUEBAS DE EVALUACIÓN CONTINUA (PEC)

¿Hay PEC?	Si,PEC no presencial

Descripción

La prueba de evaluación a distancia consistirá en un cuestionario con un máximo de 10 preguntas relacionadas con los primeros módulos de la asignatura.

Criterios de evaluación

Para el superar esta prueba el estudiante debe responder correctamente a al menos el 50% de las cuestiones.
El estudiante dispondrá de un máximo de una hora para contestarlo y el cuestionario estará disponible durante 48 horas en las fechas comunicadas por el equipo docente con suficiente antelación. El estudiante sólo podrá realizar un intento.

Ponderación de la PEC en la nota final	10% de la nota final
Fecha aproximada de entrega	28/11/2018

Comentarios y observaciones

OTRAS ACTIVIDADES EVALUABLES

¿Hay otra/s actividad/es evaluable/s? Si,no presencial

Descripción

El equipo docente valorará la participación activa en los ejercicios y las cuestiones no evaluables planteadas a lo largo de la asignatura a través de los foros.

Además, a lo largo del curso el Equipo Docente propondrá en los foros algunos temas de debate relacionados con la materia de estudio así como promoverán la discusión de casos de estudio con el fin de promover las discusiones y participaciones de los estudiantes.

Y 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.

Criterios de evaluación

Participación activa en los foros, expresando su opinion o respondiendo a los ejercicios propuestos.

Ponderación en la nota final: 10% de la nota (supondrá, por tanto, un máximo de 1 puntos en la nota final de la asignatura).

Fecha aproximada de entrega: 20/01/2019

Comentarios y observaciones

¿CÓMO SE OBTIENE LA NOTA FINAL?

Nota final = 0,6x [nota prueba presencial] + 0,3x [pruebas de evaluación a distancia]+0,1x [Participación en las actividades de evaluación continua]

Donde las pruebas de evaluación a distancia son:

10% de Prueba de Evaluación Continua

20% Trabajos propuestos.

BIBLIOGRAFÍA BÁSICA

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

BIBLIOGRAFÍA COMPLEMENTARIA

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

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

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

ISBN(13):9781593275099
Título:THE PRACTICE OF NETWORK SECURITY MONITORING. (1ª edición)
Autor/es:Richard Bejtlich ;
Editorial:No starch Press

Módulo I:

- Portal de ISO 27001: http://www.iso27000.es/
- The InfoSec Handbook. Umesh Hodeghatta Rao y Umesha Nayak. Editorial Apress Open.
- Information Security, the Complete Reference. Mark Rhodes-Ousley. Editorial McGraw-Hill .2ª Edición. 2013
- Sitio Web de ISO para la norma 27001: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- Informe sobre gestión de riesgos de la Unión Europea de para la seguridad de la información y las redes: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory
- Practical Thread Analysis tool: http://www.ptatechnologies.com/
- Plantillas de Word de SANS para la creación de políticas de seguridad: http://www.sans.org/security-resources/policies/

Módulo II:

- Cybersecurity capability maturity model (C2M2): http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

- Curso gratuito de ITIL v3: http://itilv3.osiatis.es/.
- Security Metrics: Replacing Fear, Uncertainty, and Doubt.. Andrew Jaquith. Editorial Addison Wesley, 1ª Edicion.
- The CIS Security Metrics: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf
- Artículos de Educase dedicados a las métricas de seguridad: https://library.educause.edu/topics/cybersecurity/security-metrics

Módulo III:

- "Practice of Network Security Monitoring", Richard Bejtlich. Editorial: no starch press.
- "Building Virtual Pentesting Labs for Advanced Penetration Testing", Kevin Cardwell. Editorial: Packt Publishing.
- Blog de Richard Beijtlich: http://taosecurity.blogspot.com.es/
- Distribución Kali: https://www.kali.org/
- Distribución Onion: https://security-onion-solutions.github.io/security-onion/
- Suite SILK creada por el CERT para monitorización de redes: https://tools.netsa.cert.org/silk/

Módulo IV:

- Recursos dedicados a Internet de las Cosas:

•Capítulo del documental "Mundo hacker" emitido por La 2 dedicado a Internet de las Cosas: http://www.rtve.es/drmn/embed/video/3571505

•Recursos dedicados a la seguridad en Sistemas de Control Industrial:

•NIST Guide Guide to Industrial Control Systems (ICS) Security: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

• The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT): https://ics-cert.us-cert.gov/

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 estudiante puede usar como ejercicios de autoevaluación.

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.