ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

93001002 - Ciberseguridad: Contexto y Amenazas

PLAN DE ESTUDIOS

09AW - Master Universitario En Ciberseguridad

CURSO ACADÉMICO Y SEMESTRE

2019/20 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	93001002 - Ciberseguridad: Contexto y Amenazas
No de créditos	6 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Primer semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	09AW - Master Universitario En Ciberseguridad
Centro responsable de la titulación	09 - Escuela Tecnica Superior de Ingenieros de Telecomunicacion
Curso académico	2019-20

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Aurea Maria Anguera De Sojo Hernandez	ETSI SI 8307	aureamaria.angueradesojo@upm.es	L - 11:30 - 13:00 V - 11:30 - 13:00
Maria Del Socorro Bernardos Galindo	ETSI Infor 5206	mariadelsocorro.bernardos@upm.es	L - 11:30 - 13:00 V - 11:30 - 13:00
Jorge Davila Muro (Coordinador/a)	ETSI Infor 5205	jorge.davila@upm.es	L - 11:30 - 13:00 V - 11:30 - 13:00

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Competencias y resultados de aprendizaje

3.1. Competencias

CB06 - 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

CB07 - 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

CB08 - 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

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

CE01 - Capacidad para comprender los conceptos que intervienen en la gestión e implantación de un sistema de ciberseguridad en una organización

CE08 - Capacidad para abordar técnicamente la gestión de un incidente de ciberseguridad, incluyendo análisis de malware, análisis forense e ingeniería inversa

CG02 - Dotar al alumno del conocimiento de los distintos tipos de amenazas que pueden afectar a una organización y sus consecuencias en diferentes escenarios sociales, económicos e industriales y dotarle de la capacidad de aplicar las técnicas de análisis y gestión de todo tipo de riesgos para definir e implantar las salvaguardas necesarias para mitigar o eliminar sus impactos hacer resiliente a la organización

CG05 - Dotar al alumno de la capacidad de estar al día de los desarrollos más recientes que tengan que ver con la ciberseguridad, así como de contribuir con ideas contrastadas al desarrollo técnico de lo aprendido y a nuevas áreas en las que sea de aplicación la ciberseguridad, con posibilidad de participar en actividades directivas de nivel medio de gerencia

CT09 - Capacidad de análisis y síntesis

CT12 - Aprendizaje autónomo, adaptación a nuevas situaciones y motivación por el desarrollo profesional permanente

3.2. Resultados del aprendizaje

RA2 - Determinar el valor y rentabilidad de las inversiones en activos de seguridad

RA25 - Tratamiento de los riesgos de confidencialidad, integridad y disponibilidad utilizando distinta herramientas y servicios criptográ- fícos

RA4 - Comprender la importancia de la Ingeniería Social, los atacantes y ataques más comunes y aplicar las técnicas para prevenir dichos ataques

RA5 - Comprender y aplicar técnicas para el tratamiento de riesgos

RA3 - .Conocer y comprender los elementos que intervienen en un sistema de ciberseguridad así como crear las infraestructuras y procesos necesarios para ello

RA1 - .Comprender la importancia de la ciberseguridad para las organizaciones y su gobernanza corporativa así como los principios, estructuras, roles y responsabilidades que deben seguirse para su gestión

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

En esta asignatura se persigue hacer una revisioinde todos lso aspectos que tiene la Cibersefguridad en diferentes escenarios y circunstancias. Se pretende exponer dón de nace el escenario actual de la ciberseguridad, y mostrar coimo los riesgos actuales tienen su razon de ser en decisiones estructurales que se tomeran con anteriorida a la hora de diseñar y pooner en pie loos sistemas informatiocos, lso sistemas de informacióin e Intenernet. Se persigue prestar atenciona

1. La Informatización de la Sociedad y del Sistema Productivo: Aspectos económicos y sociales, beneficios y riesgos.
2. Los Objetivos y Estrategias de seguridad: Prevención, Detección, Respuesta y Recuperación.
3. Los Principios, estructuras, roles y responsabilidades en la gestión de la Ciberseguridad.
4. Las Políticas y Normativas de Ciberseguridad. Procesos de seguridad, Activos de Información, su clasificación e inventario.
5. Las Amenazas, Riesgos, Control de Acceso, Seguridad en Red, Sistemas y Servicios. Sistemas Operativos. El desarrollo de software y de la información
6. La seguridad criptográfica y los servicios criptográficos.
7. La continuidad de la organización: la Resiliencia. Big Data y capacidades predictivas y prescriptivas para la

resiliencia.

8. Los tipos de amenazas clásicas y APTs. La Seguridad de los Datos. Aplicaciones y ejecutables. La Seguridad del Hardware. Nubes y Virtualización.
9. La clasificación de la información. La seguridad del dato y su cifrado. La destrucción de medios físicos o dañados y la destrucción de datos.
10. La Ingeniería Social, categorías de actores, y ataques más comunes. Técnicas para prevenir los ataques de Ingeniería Socia
11. Las Privacidad y legislación sobre Protección de Datos. Marcos jurídicos de la Seguridad y la Auditoría de la Información.

4.2. Temario de la asignatura

1. Informatización de la Sociedad y del Sistema Productivo: Aspectos económicos y sociales, beneficios y riesgos.

2. Objetivos y Estrategias de seguridad: Prevención, Detección, Respuesta y Recuperación.

3. Principios, estructuras, roles y responsabilidades en la gestión de la Ciberseguridad.

4. Políticas y Normativas de Ciberseguridad. Procesos de seguridad, Activos de Información, su clasificación e inventario.

5. Amenazas, Riesgos, Control de Acceso, Seguridad en Red, Sistemas y Servicios. Sistemas Operativos. El desarrollo de software y de la información

6. La seguridad criptográfica y los servicios criptográficos.

7. La continuidad de la organización: la Resiliencia. Big Data y capacidades predictivas y prescriptivas para la resiliencia.

8. Privacidad y legislación sobre Protección de Datos. Marcos jurídicos de la Seguridad y la Auditoría de la Información.

9. Tipos de amenazas clásicas y APTs. La Seguridad de los Datos. Aplicaciones y ejecutables. La Seguridad del Hardware. Nubes y Virtualización.

10. La clasificación de la información. La seguridad del dato y su cifrado. La destrucción de medios físicos o dañados y la destrucción de datos.

11. La Ingeniería Social, categorías de actores, y ataques más comunes. Técnicas para prevenir los ataques por Ingeniería Social

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	**Clases de Teoria Presencial** Duración: 20:00 LM: Actividad del tipo Lección Magistral			
2	**Clases de Teoria Presencial** Duración: 20:00 LM: Actividad del tipo Lección Magistral			
3	**Clases de Teoria Presencial** Duración: 10:00 LM: Actividad del tipo Lección Magistral			
4	**Clases de Teoria Presencial** Duración: 10:00 LM: Actividad del tipo Lección Magistral			
5	**Clases de Teoria Presencial** Duración: 10:00 LM: Actividad del tipo Lección Magistral			
6				
7				
8				**Examen de la Asignatura** TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 04:00 **Examen de la Asignatura** TI: Técnica del tipo Trabajo Individual Evaluación sólo prueba final Duración: 04:00
9				
10				
11				
12				
13				
14				
15				
16				
17				

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
8	Examen de la Asignatura	TI: Técnica del tipo Trabajo Individual	No Presencial	04:00	100%	5 / 10	CT12 CE01 CG02 CG05 CB07 CB08 CB10 CB06 CT09 CE08

6.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
8	Examen de la Asignatura	TI: Técnica del tipo Trabajo Individual	No Presencial	04:00	100%	5 / 10	CT12 CE01 CG02 CG05 CB07 CB08 CB10 CB06 CT09 CE08

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen de la Asignatura	TI: Técnica del tipo Trabajo Individual	Presencial	04:00	100%	5 / 10	CG02 CG05 CB07 CB08 CB10 CB06 CT09 CT12 CE01 CE08

6.2. Criterios de evaluación

En la evaluación de la asiignatura se valorará:

1. La participación del alumno en el desarrollo de la asigntaura.
2. La madrurez de los argumentos presentados.
3. La actualidad, precisión y detalle de los datos utilizados.

4. La calidad y abundacia de referencias externas.
5. El nivel de comprensión de los problemas tratados.
6. La transversaklidad de los análisis realizados y de las soluciones propuestas.
7. La calidad en la redacción y exposicion de sus trabajos y resultados.

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
@War: The Rise of the Military-Internet Complex	Bibliografía	by Shane Harris Publisher: Eamon Dolan/Houghton Mifflin Harcourt; First Edition edition (November 11, 2014) ISBN-10: 0544251792 ISBN-13: 978-0544251793
15 Minutes: General Curtis LeMay and the Countdown to Nuclear Annihilation	Bibliografía	by L. Douglas Keeney Publisher: St. Martin's Griffin; Reprint edition (February 14, 2012) ISBN-10: 1250002087 ISBN-13: 978-1250002082
American Spies	Bibliografía	de Jennifer Granick Editor: Cambridge University Press (2 de febrero de 2017) ISBN-10: 1107501857 ISBN-13: 978-1107501850
Anonymous File Sharing & Darknet - How to be a Ghost in the Machine	Bibliografía	de Lance Henderson Editor: CreateSpace Independent Publishing Platform (30 de enero de 2013) ISBN-10: 1482323990 ISBN-13: 978-1482323993
Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety	Bibliografía	by Eric Schlosser Hardcover: 656 pages Publisher: Penguin Press; 1st edition (September 17, 2013) ISBN-10: 1594202273 ISBN-13: 978-1594202278

Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon	Bibliografía	by Kim Zetter Publisher: Crown; 1st edition (November 11, 2014) ISBN-10: 077043617X ISBN-13: 978-0770436179
Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis	Bibliografía	by Colleen McCue Publisher: Butterworth-Heinemann; 1 edition (May 1, 2007) ISBN-10: 0750677961 ISBN-13: 978-0750677967
Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers	Bibliografía	by R. A. Ratcliff (Author) Publisher: Cambridge University Press; First Edition edition (August 14, 2006) ISBN-10: 0521855225 ISBN-13: 978-0521855228
Intercept: The Secret History of Computers and Spies	Bibliografía	by Gordon Corera Editor: W&N (9 de junio de 2016) ISBN-10: 1780227841 ISBN-13: 978-1780227849
La guerra secreta: Espías, códigos y guerrillas, 1939-1945	Bibliografía	de Max Hastings Editor: Critica (15 de marzo de 2016) Colección: Memoria Crítica ISBN-10: 8498929342 ISBN-13: 978-8498929348
The Masters of Deception: The Gang That Ruled Cyberspace	Bibliografía	de Michele Slatalla Editor: Harper Collins; Edición: Harperperennial. (1 de diciembre de 1995) ISBN-10: 0060926945 ISBN-13: 978-0060926946
Network Security Through Data Analysis: Building Situational Awareness 1st Edition	Bibliografía	by Michael Collins Publisher: O'Reilly Media; 1 edition (February 23, 2014) ISBN-10: 1449357903 ISBN-13: 978-1449357900

No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State	Bibliografía	by Glenn Greenwald Publisher: Metropolitan Books (May 13, 2014) ISBN-10: 162779073X ISBN-13: 978-1627790734
Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information	Bibliografía	by Michael Bazzell Publisher: CreateSpace Independent Publishing Platform; 3 edition (January 1, 2014) ISBN-10: 149427535X ISBN-13: 978-1494275358
Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up	Bibliografía	de Philip N. Howard Editor: Yale University Press (19 de mayo de 2015) ISBN-10: 0300199473 ISBN-13: 978-0300199475
Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience	Bibliografía	by James B. Rule (Author) Publisher: Oxford University Press; 1 edition (November 11, 2009) ISBN-10: 0195394364 ISBN-13: 978-0195394368
Reverse Deception: Organized Cyber Threat Counter-Exploitation (Networking & Communication - OMG)	Bibliografía	by Sean Bodmer, Dr. Max Kilger, Gregory Carpenter and Jade Jones. Series: Networking & Communication - OMG Publisher: McGraw-Hill Education; 1 edition (July 24, 2012) ISBN-10: 0071772499 ISBN-13: 978-0071772495
The Art of Deception: Controlling the Human Element of Security	Bibliografía	by Kevin D. Mitnick and William L. Simon, Publisher: Wiley; 1 edition (October 17, 2003) ISBN-10: 076454280X ISBN-13: 978-0764542800

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage	Bibliografía	de Cliff Stoll Editor: Pocket Books; Edición: Reissue (1 de septiembre de 2005) ISBN-10: 1416507787 ISBN-13: 978-1416507789
The Dark Net	Bibliografía	de Jamie Bartlett Editor: Random House (16 de enero de 2015) ISBN-10: 0099592029 ISBN-13: 978-0099592020
The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy	Bibliografía	by David Hoffman Publisher: Anchor; 1 edition (August 3, 2010) ISBN-10: 0307387844 ISBN-13: 978-0307387844
The Myths of Security: What the Computer Security Industry Doesn't Want You to Know	Bibliografía	by John Viega Publisher: O'Reilly Media; 1 edition (June 29, 2009) ISBN-10: 0596523025 ISBN-13: 978-0596523022
The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America	Bibliografía	by James Bamford Publisher: Anchor (July 14, 2009) ISBN-10: 0307279391 ISBN-13: 978-0307279392
The Snowden Files: The Inside Story of the World's Most Wanted Man	Bibliografía	by Luke Harding Publisher: Vintage; F First Paperback Edition Used edition (February 7, 2014) ISBN-10: 0804173524 ISBN-13: 978-0804173520
Tor and the Dark Art of Anonymity: How to Be Invisible from NSA Spying	Bibliografía	de Lance Henderson Editor: Createspace Independent Publishing Platform (16 de mayo de 2015) ISBN-10: 1512049581 ISBN-13: 978-1512049589

Understanding Privacy	Bibliografía	by Daniel J. Solove Publisher: Harvard University Press; 2/28/10 edition (March 30, 2010) ISBN-10: 0674035070 ISBN-13: 978-0674035072