Escuela Superior de Ingeniería
Universidad de Cádiz

Avenida de la Universidad de Cádiz, nº 10
CP 11519, Puerto Real (Cádiz).

FICHA DE LA ASIGNATURA SEGURIDAD EN SISTEMAS e INFRAESTRUCTURAS CRÍTICAS			
CARÁCTER:	**Obligatorio**	**LENGUA/S EN LA/S QUE SE IMPARTE:**	**Español/Inglés**
ECTS:	**4**	**CUATRIMESTRE**	**2**
Asignatura de la MATERIA SEGURIDAD EN SISTEMAS			
PROFESORES QUE IMPARTEN LA ASIGNATURA			
Guillermo Bárcena González **Antonia Estero Botaro** **Inmaculada Medina Bulo (coordinadora)** **Francisco Palomo Lozano**			
COMPETENCIAS QUE SE ADQUIEREN: *(indicar código)*			
Comp. Básicas	**Comp. Generales**	**Comp. Específicas**	**Comp. Transversales**
CB6, CB9, CB10	**CG2, CG4, CG5**	**CE16 CE17**	**CT1 CT2**

RESULTADOS DE APRENDIZAJE:

- Diferenciar los sistemas críticos de los de misión crítica y de los no críticos
- Comprender la relación entre los errores y las amenazas a la seguridad
- Conocer los peligros que las amenazas a los sistemas críticos suponen para la seguridad de las personas
- Seleccionar esquemas de autenticación y acceso adecuados a sistemas críticos concretos
- Analizar los requisitos de seguridad de sistemas críticos concretos
- Definir las respuestas a incidencias de seguridad para sistemas críticos concretos
- Definir políticas de seguridad para sistemas críticos concretos
- Conocer la legislación existente en España sobre protección de infraestructuras críticas

CONTENIDOS:

Tema 1: Seguridad en sistemas críticos
1.1 Sistemas críticos y de misión crítica
1.2 Clasificación
1.3 Aspectos específicos de seguridad
1.4 Legislación en materia de infraestructuras críticas
Tema 2: Casos de estudio
2.1 Dispositivos médicos
2.2 Transporte
2.3 Infraestructuras críticas
2.4 Sistemas militares
Tema 3: Esquemas de autenticación y control de acceso a sistemas críticos
3.1 Controles físicos y lógicos
3.2 Autenticación e identificación
3.3 Gestión de la identidad digital
Tema 4: Amenazas a los sistemas críticos

4.1 Ciberdelincuencia
4.2 Ciberespionaje
4.3 Ciberterrorismo
4.4 Ciberguerra
4.5 Prevención, detección y respuesta
Seminario 1: Análisis comparativo de distintos tipos de sistemas críticos
Seminario 2: Análisis de requisitos de seguridad en un sistema crítico concreto (caso de estudio)
Seminario 3: Definición de respuestas ante incidencias de seguridad en un sistema crítico concreto (caso de estudio)
Seminario 4: Definición de políticas de seguridad para un sistema crítico concreto (caso de estudio)
Seminario 5: Legislación sobre protección de las infraestructuras críticas

OBSERVACIONES / REQUISITOS PREVIOS:
Haber cursado las asignaturas:

- Prácticas en análisis forense
- Criptografía aplicada y seguridad en software de sistemas
- Seguridad en redes

Esta asignatura pertenece al Máster en Seguridad Informática, y trabajará la CT2 (competencias idiomáticas), y en especial de las más específicas de la titulación, con 3 créditos ECTS dentro del Programa de Enseñanza Bilingüe (AICLE) de la Escuela Superior de Ingeniería, utilizando como lengua vehicular el inglés. Los contenidos impartidos serán, además, evaluados en la lengua vehicular.

	Id de la Actividad Formativa	Nº de horas	Presencialidad (%)
ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:	Clases teórico-prácticas	28	100%
	Seminarios y conferencias	4	100%
	Actividades académicas no presenciales	65	0%
	Evaluación	3	100%

METODOLOGÍAS DOCENTES:
Lección magistral expositiva
Resolución de problemas y casos prácticos
Realización y exposición de trabajos

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Denominación Sistema Evaluación	Ponderación Mínima	Ponderación Máxima
Trabajos escritos realizados por el alumno	0%	50%
Exposiciones de ejercicios, temas y trabajos	10%	50%
Participación y trabajo realizado en actividades formativas	0%	25%
Pruebas escritas u orales	25%	75%

BIBLIOGRAFÍA RECOMENDADA:

Bibliografía básica

Alur, Rajeev.
Principles of Cyber-Physical Systems
MIT Press. 2015.
ISBN 978-0-262-02911-7

Cappelli, Dawn M.; Moore, Andrew P. & Trzeciak, Randall F.
The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud).
Addison-Wesley. 2012.
ISBN 978-0-321-81257-5

Kindt, Els J.
Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis.
Springer. 2013.
ISBN 978-94-007-7521-3

Loukas, George.
Cyber-Physical Attacks: A Growing Invisible Threat.
Butterworth-Heinemann. 2015.
ISBN 978-0-128-01290-1

Todorov, Dobromir
Mechanics of User Identification and Authentication. Fundamentals of Identity Management.
Auerbach Publications. 2007.
ISBN 978-1-420-05219-0

Bibliografía específica

Bolívar, Juan Francisco
Infraestructuras críticas y sistemas industriales: Auditorías de seguridad y fortificación.
Editorial ZEROXWORD COMPUTING
Materia SEGURIDAD INFORMÁTICA | Fraude informático y hacking. 2016.
ISBN 978-84-617-6003-9

Goodman, Marc.
Future Crimes.
Transworld. 2015.
ISBN 978-0-593-07366-7

Taylor, Robert E.; Fritsch, Eric J. & Liederbach, John C.
Digital Crime and Digital Terrorism.

Pearson. 3ª edición. 2014.
ISBN 978-0-133-45890-9

Zetter, Kim.
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.
Crown. 2014.
ISBN 978-0-770-43617-9

Bibliografía de ampliación

Carpentier, Jean-François
La seguridad informatica en la pyme: Situacion actual y mejores practicas
Editorial Ediciones eni Materia SEGURIDAD INFORMÁTICA Colección DataPro. 2016.
ISBN 978-2-409-00180-2

Chen, Tom; Jarvis, Lee & Macdonald, Stuart (Editores)
Cyberterrorism: Understanding, Assessment, and Response.
Springer. 2014.
ISBN 978-1-493-90961-2

Clarke, Richard A. & Knake, Robert A.
Cyber War: The Next Threat to National Security and What to Do About It.
HarperCollins. 2012.
ISBN 978-0-061-96224-0

Schmitt, Michael N. (Editor).
Tallinn Manual on the International Law Applicable to Cyber Warfare.
Cambridge University Press. 2013.
ISBN 978-1-107-61377-5

Singer, Peter W. & Friedman, Allan.
Cybersecurity and Cyberwar: What Everyone Needs to Know.
Oxford University Press. 2014.
ISBN 978-0-199-91811-9