Ciberdelitos, Ciberterrorismo y Ciberguerra

Curso Académico: (2021 / 2022) **Fecha de revisión: 10-05-2021**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: ESTEVEZ TAPIADOR, JUAN MANUEL

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 1

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Niguna

OBJETIVOS

- 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.

- 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.

- 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.

- 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.

- Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando.

- Comprender y aplicar métodos y técnicas de investigación de ciberataques a una instalación específica.

- Elaborar concisa, clara y razonadamente documentos, planes y proyectos de trabajo en el ámbito de la Ciberseguridad.

- Conocer la normativa técnica y las disposiciones legales de aplicación en la materia de ciberseguridad, sus implicaciones en el diseño de sistemas y en la aplicación de herramientas de seguridad.

- Analizar y detectar anomalías y firmas de ataques en los sistemas y redes.

- Analizar y detectar técnicas de ocultación de ataques a sistemas y redes.

- Conocer las tendencias actuales en técnicas de ciberataque y las experiencias aprendidas en casos reales.

- Conocer y aplicar los mecanismos de cifrado y esteganografiado pertinentes para proteger los datos residentes en un sistema o en tránsito por una red.

Enlace al documento

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción, Definiciones y Conceptos Básicos
1.1. Orígenes
1.2. Ciberataques por doquier
1.3. Una breve historia del malware
1.4. Bienvenidos a la economía sumergida
1.5. Ciberamenazas
1.6. Tendencias

2. Ciberataques y ciberactivismo
2.1. Tipos de Ciberataques
2.2. Ciberdelitos
2.3. Ciberespionaje
2.4. Análisis de Casos Prácticos
2.5. Aspectos Legales

3. Ciberterrorismo y Ciberoperaciones contra Infraestructuras Críticas
3.1. Infraestructuras Críticas: Interconexión y Vulnerabilidades
3.2. Sistemas de Control Industrial
3.3. Otras Infraestructuras Críticas
3.4. Análisis de Casos Prácticos

4. Ciberguerra
4.1. Ciberarmamento: Instrumentos Lógicos, Físicos y Psicológicos
4.2. Ciberdoctrina
4.3. Análisis de Casos Prácticos

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS

- Clases teórico prácticas
- Tutorías
- Trabajo en grupo
- Trabajo individual del estudiante

METODOLOGÍAS DOCENTES

- Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.

- Lectura crítica de textos recomendados por el profesor de la asignatura: Artículos de prensa, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.

- Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.

- Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos .

- Elaboración de trabajos e informes de manera individual o en grupo.

- Realización de ejercicios y cuestiones en pruebas evaluables.

SISTEMA DE EVALUACIÓN

El sistema de evaluación incluye:

1. La evaluación continua del trabajo del alumno a través de uno o más de los siguientes instrumentos:
   1.1. Pruebas de evaluación, escritas u orales, de habilidades y conocimientos teórico-prácticos.
   1.2. Informes y trabajos, individuales o colectivos, asignados por el profesor.
   1.3. Presentaciones realizadas en clase sobre temas relacionados con la materia.
   1.4. Participación en los debates organizados durante el curso.

El peso porcentual de la evaluación continua es el 100% de la nota final.

2. La evaluación final a través de un examen escrito para aquellos estudiantes que no sigan o no superen la evaluación continua. En el examen se evaluará de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. El peso porcentual del examen final sera del 100% de la nota final.

Para la convocatoria extraordinaria la evaluación consistirá en un único examen con un valor del 100% de la calificación total de la asignatura. Este examen podrá contener preguntas pertinentes a las

actividades realizadas durante el curso.

Peso porcentual del Examen Final:	0
Peso porcentual del resto de la evaluación:	100

BIBLIOGRAFÍA BÁSICA

- Bill Blunden, Violet Cheung Behold a Pale Farce: Cyberwar, Threat Inflation, & the Malware Industrial Complex, Trine Day, 2014
- Brian Krebs Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door, Sourcebooks, 2014
- Bruce Schneier Secrets and Lies: Digital Security in a Networked World, Wiley, 2004
- Christopher Hadnagy, Paul Wilson Social Engineering: The Art of Human Hacking, Wiley, 2010
- Christopher Paul Information Operations - Doctrine and Practice: A Reference Handbook, Praeger, 2008
- Cliff Stoll The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, Pocket Books, 2005
- Cristopher Hadnagy, Paul F. Kelly, Paul Ekman Unmasking the Social Engineer: The Human Element of Security, Wiley, 2014
- Dennis F. Poindexter The Chinese Information War: Espionage, Cyberwar, Communications Control and Related Threats to United States Interests, McFarland, 2013
- Derek S. Reveron Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World, Georgetown University Press, 2012
- Edwin L. Armistead Information Operations: Warfare and the Hard Reality of Soft Power, Potomac Books Inc., 2004
- Ian Mann Hacking the Human, Gower, 2008
- Ian Mann Hacking the Human 2, Consilience Media, 2013
- J. D. Lasica Darknet: Hollywood's War Against the Digital Generation, Wiley, 2005
- Jason Andress, Steve Winterfeld Cyber Warfare, Second Edition: Techniques, Tactics and Tools for Security Practitioners, Syngress, 2013
- Jeffrey Carr Inside Cyber Warfare: Mapping the Cyber Underworld (2nd Edition), O'Reilly Media, 2011
- Jonathan Clough Principles of Cybercrime, Cambridge University Press, 2010
- Julie E. Mehan Cyberwar, Cyberterror, Cybercrime and Cyberactivism (2nd Edition), ITGP, 2014
- Kevin D. Mitnick, William L. Simon The Art of Deception: Controlling the Human Element of Security, Wiley, 2003
- Kevin D. Mitnick, William L. Simon The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, Wiley, 2005
- Kevin Hogan, James Speakman Covert Persuasion: Psychological Tactics and Tricks to Win the Game, Wiley, 2006
- Kevin Mitnick, William L. Simon Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, Back Bay Books, 2012
- Kevin Poulsen Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground, Broadway Books, 2012
- Majid Yar Cybercrime and Society, 2nd Edition, SAGE Publications Ltd., 2013
- Mark Bowden Worm: The First Digital World War, Grove Press, 2012
- Martin C. Libicki Cyberdeterrence and Cyberwar, RAND Corporation, 2009
- Nicholas Capaldi The Art of Deception: An Introduction to Critical Thinking, Prometheus Books, 2007
- P.W. Singer, Allan Friedman Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014
- Parmy Olson We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, Back Bay Books, 2013
- Patrick D. Allen Information Operations Planning, Artech House Publishers, 2007
- Phil Lapsley Exploding the Phone, Grove Press, 2014
- Richard A. Clarke, Robert Knake Cyber War: The Next Threat to National Security and What to Do About It, Ecco, 2012
- Robert Moore Cybercrime, Second Edition: Investigating High-Technology Computer Crime, Anderson, 2006
- Ronald J. Deibert Black Code: Surveillance, Privacy, and the Dark Side of the Internet, Signal, 2013
- Thomad Rid Cyber War Will Not Take Place, Oxford University Press, 2013