

Curso Académico: ( 2021 / 2022 )

Fecha de revisión: 26/07/2020 17:20:46

Departamento asignado a la asignatura:

Coordinador/a: PASTRANA PORTILLO, SERGIO

Tipo: Optativa Créditos ECTS : 3.0

Curso : 1 Cuatrimestre : 2

**REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)**

Es recomendable, aunque no necesario, haber cursado previamente la asignatura "Técnicas y Protocolos Criptográficos" que se imparte en el primer cuatrimestre.

**OBJETIVOS**

Competencias básicas:

- 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 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:

- Capacidad para comprender y aplicar métodos y técnicas de investigación en el ámbito de la Ingeniería Informática.
- Capacidad para la aplicación de los conocimientos adquiridos y para resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, hasta ser capaces de integrar estos conocimientos.
- Saber transmitir de un modo claro y sin ambigüedades a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que se sustentan;

Competencias específicas:

- Capacidad de análisis crítico de documentos técnicos y científicos en el ámbito de la Ingeniería Informática.
- Conocer el significado de la investigación científica.
- Comprender y analizar los principios y métodos de protección de la información.
- Aplicar y evaluar los mecanismos de seguridad empleados en sistemas distribuidos y reconocer las tendencias en la seguridad en comunicaciones y sistemas distribuidos.

**DESCRIPCIÓN DE CONTENIDOS: PROGRAMA**

1. Introducción a la ciberseguridad
  - 1.1. Orígenes
  - 1.2. Ciberataques
  - 1.3. Breve historia del malware
  - 1.4. La economía sumergida
  - 1.5. Ciberamenazas 2013-2018
  - 1.6. Tendencias
2. Seguridad en dispositivos inteligentes
  - 2.1. Dispositivos inteligentes
  - 2.1. Modelos de seguridad
  - 2.2. Malware en dispositivos inteligentes
  - 2.3. Detección y análisis
  - 2.4. Problemas de seguridad abiertos
3. Ataques coordinados y de denegación de servicio
  - 3.1. Ataques coordinados
  - 3.2. Sistemas de detección de intrusiones colaborativos
  - 3.3. Clasificaciones existentes de CIDS
  - 3.4. Soluciones integradas para CIDS
4. Análisis de tráfico
  - 4.1. Introducción
  - 4.2. Raíces militares
  - 4.3. Análisis de tráfico civil
  - 4.4. Seguridad informática y de las comunicaciones
  - 4.5. Explotación de datos de la localización
  - 4.6. Contramedidas en Internet
  - 4.7. Retención de datos
5. Botnets
  - 5.1. Introducción
  - 5.2. Estructura y funciones
  - 5.3. Técnicas de detección
  - 5.4. Técnicas de defensa
  - 5.5. Nuevas tendencias y plataformas
  - 5.6. Retos

## ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Actividades formativas:

1. Clases teórico prácticas
2. Tutorías
3. Trabajo individual del estudiante (lectura crítica de artículos y participación en clase)

Metodología:

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

## SISTEMA DE EVALUACIÓN

|                                                    |    |
|----------------------------------------------------|----|
| <b>Peso porcentual del Examen/Prueba Final:</b>    | 80 |
| <b>Peso porcentual del resto de la evaluación:</b> | 20 |

(1) Asistencia y participación en clase

Se valorará con hasta un 20% de la nota final la asistencia a clase, lectura de los artículos recomendados por el profesor y participación en los sucesivos debates/actividades organizados.

(2) Entrega de trabajo final de asignatura

Cada alumno deberá realizar un trabajo final original sobre una temática previamente acordada con el profesor y exponerlo en clase en una fecha determinada.

Para la convocatoria extraordinaria, el alumno elegirá entre:

- a) Guardar la nota de la evaluación continua y realizar un examen escrito por valor del 80% restante; o
- b) Realizar un examen escrito por valor del 100% de la nota

#### BIBLIOGRAFÍA BÁSICA

- Matt Bishop Computer Security: Art & Science, Addison-Wesley Professional, 2015
- W. Stallings Cryptography and Network Security (7th Edition), Pearson, 2016

#### BIBLIOGRAFÍA COMPLEMENTARIA

- C. Sanders, J. Smith Applied Network Security Monitoring: Collection, Detection, and Analysis, Syngress, 2013
- Rebecca G. Bace Intrusion Detection, Sams Publishing, 2000
- Stephen Northcutt, Judy Novak Network Intrusion Detection (3rd Edition), Sams Publishing; 3 edition, 2002

#### RECURSOS ELECTRÓNICOS BÁSICOS

- Chenfeng Vincent Zhou, Christopher Leckie, Shanika Karunasekera . A survey of coordinated attacks and collaborative intrusion detection: <http://dx.doi.org/10.1016/j.cose.2009.06.008>
- G. Suarez-Tangil, J.E. Tapiador, P. Peris, A. Ribagorda. . Evolution, Detection and Analysis of Malware in Smart Devices: <http://dx.doi.org/10.1109/SURV.2013.101613.00077>
- George Danezis and Richard Clayton . Introducing Traffic Analysis: <https://www.cl.cam.ac.uk/~rnc1/TAIntro-book.pdf>
- Sérgio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto, Ronaldo M. Salles . Botnets: A survey: <http://dx.doi.org/10.1016/j.comnet.2012.07.021>