Programa de Asignatura

Unidad Académica Responsable: Departamento de Informática y Ciencias la Computación
Carrera a la que se imparte: Programas de postgrado y pregrado departamentales.

I.- IDENTIFICACIÓN

Nombre: Inteligencia Computacional aplicado a Ciberseguridad		
Código:	Créditos: 3	Créditos SCT: 6
Prerrequisitos: Licenciatura + 503356 (Inteligencia Artificial)		
Modalidad: presencial	Calidad: electivo	Duración: semestral
Semestre en el plan de estudios	10	
Trabajo Académico: 10		
Horas Teóricas: 2 Horas Prácticas: 2 Horas Laboratorio: 0 Horas de otras actividades: 6		

II.- DESCRIPCIÓN

Esta asignatura electiva está orientada a que los estudiantes conozcan distintas técnicas de inteligencia computacional y su aplicación a problemas de clasificación del dominio de la seguridad informática.

La asignatura aporta las siguientes competencias del perfil de egreso:

- Soluciona problemas complejos en el ámbito de la ingeniería informática, aplicando conocimientos de matemática, ciencias, ingeniería y computación; considerando criterios técnicos y sociales, dentro del contexto de trabajo colaborativo. **(ref Competencia 2).**
- Desarrolla investigaciones y estudios detallados de aspectos técnicos de la ingeniería informática, a través del diseño y conducción de experimentos y del análisis e interpretación de sus resultados. (**ref Competencia 3).**

III.-RESULTADOS DE APRENDIZAJE ESPERADOS

Al finalizar la asignatura, los alumnos serán capaces de:

R1. Comprender los problemas de clasificación propios del dominio de la seguridad de la información.
R2. Reconocer las fuentes de datos útiles para el análisis y solución del problema de detección de intrusos y *malware* en sistemas computacionales.
R3. Comprender aspectos básicos del diseño de sistemas de detección y prevención de intrusos en redes (IDS/IPS).
R4. Conocer y aplicar métricas de calidad a sistemas de detección de intrusos en redes, realizando experimentos para establecer evidencia válida para comparaciones entre algoritmos.
R5. Conocer técnicas de clasificación propias del dominio de la inteligencia computacional.
R6. Comprender el funcionamiento de algoritmos de clasificación basados en enjambre (*swarming*), y su aplicación al problema de detección de intrusiones.
R7. Comprender el funcionamiento de algoritmos de clasificación propios de Sistemas Inmunes Artificiales (AIS) y su aplicación al problema de detección de intrusiones.
R8. Aplicar a nivel de prueba de concepto y/o prototipado, técnicas de inteligencia computacional sobre el problema de detección de intrusos y/o de *malware* en redes computacionales.

IV.-CONTENIDOS

1. Vulnerabilidades en Sistemas Computacionales: *causas, catastros y herramientas de levantamiento y prospección.*
2. Caracterización de tipos de *malwares* y su funcionamiento: amenazas y principales desafíos.
3. Técnicas de detección de *malwares*: *detección estática, dinámica y heurística.*
4. Sistemas de Detección de Intrusiones (IDS/IPS): técnicas de detección de anomalía y de patrones, fuentes de datos (a*udit-trail*) utilizados en el análisis.
5. Conceptos básicos de Inteligencia computacional y sistemas clasificadores basados en aprendizaje de máquina.
6. Elementos de *swarming:* algoritmos de colonias hormigas utilizados para detección de intrusos (ANTIDS).
7. Sistemas Inmunes Artificiales (AIS): conceptos claves de Sistemas Inmunes Biológicos (BIS) y sus procesos de forma simplificada.
8. Algoritmos poblacionales y basados en red inmune aplicados a detección de *malware* e intrusos en sistemas computacionales. (Selección Negativa, Selección Clonal, Red de Jerne, Teoría del Peligro)
9. Variantes de Inmunidad según perspectiva de Varela, (Modelo EIA/AB)
10. Elementos básicos de modelamiento basado en agentes (ABM) usando NetLogo.

V.-METODOLOGÍA

La asignatura contempla sesiones expositivas, presentaciones por parte de invitados, y actividades de laboratorio orientadas a la exploración del funcionamiento y bondades de algoritmos clasificadores sobre problemas de seguridad, evaluados con significancia estadística.

VI.-EVALUACIÓN

La asignatura será evaluada en base a presentaciones de estudiantes, cómo también trabajo en desarrollo de un proyecto semestral evaluado en distintas etapas de desarrollo.

VII.BIBLIOGRAFÍA

Básicos:

- Tan Y. (2016). *Artificial Immune System Applications in Computer Security*, New Jersey: Wiley
- Bhuyan MH. (2017). *Network Traffic Anomaly Detection and Prevention*: Concepts, Techniques, and Tools, UK :Springer

Complementarios:

- Kruse R., Borgelt Ch. Braune Ch. Mostaghim S. Steinbrecher M. (2016) *Computational Intelligence A Methodological Introduction*, *Second Edition*, London, Springer.