FACULTAD DE INGENIERÍA DE SISTEMAS,
INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN
SEMINARIO PROFESIONAL I

Catedráticos Adrián Alberto Catalán Santis <adriancatalan@galileo.edu>
Victor Peñaloza <victorsergio@galileo.edu>
Pablo Barrera <pbarrera@gmail.com>
Kevin Hernández <hernandez.kevin@galileo.edu>

DESCRIPCIÓN

El curso tiene dos partes, Machine Learning y Seguridad Informática. El objetivo de la parte de Machine Learning es brindar al estudiante las herramientas necesarias para que pueda estar preparado a implementar las principales técnicas de Machine Learning y resolver problemas en investigación o en la industria. Durante el curso se revisarán diferentes modelos y algoritmos de ML en aprendizaje supervisado, sin supervisión y reforzado. La parte de Seguridad Informática busca proporcionar al estudiante los conocimientos necesarios para comprender a profundidad las principales áreas de seguridad de la información incluyendo risk assessment, criptografía, seguridad en redes, seguridad web y seguridad en sistemas operativos.

METODOLOGÍA

El curso tendrá presentaciones y clases magistrales para cubrir el contenido descrito y se evaluará a través de exámenes, laboratorios y un proyecto.

Exámenes

Los exámenes cubren contenido de clases magistrales, laboratorios, lecturas asignadas y todo el material visto hasta el momento.

Laboratorios

Semanalmente se trabajarán de 1 a 2 laboratorios sobre temas vistos en clase.

Proyecto

Se realizará un proyecto de curso en grupos a través del cuál se pondrán en práctica los conocimientos adquiridos durante el semestre.

COMPETENCIAS

- Conoce los principales algoritmos de Machine Learning para aprendizaje supervisado, sin supervisión y reforzado.
- Identifica qué aproximación y algoritmos utilizar para resolver distintos tipos de problema, utilizando Machine Learning
- Identifica las principales vulnerabilidades en seguridad para redes, sistemas operativos y web

- Conoce diferentes formas de mitigar las principales vulnerabilidades en seguridad para redes, sistemas operativos y web

CONTENIDO

PARTE 1: Machine Learning

- Introducción
    - Conceptos básicos
    - Clasificació
    - Trabajando con TensorFlow y Keras
- Redes Neuronales
    - Función de activación
    - Loss
    - Optimización
- Transfer learning en CV
    - Feature extraction
    - Fine Tuning
- CNNs y CV
    - Convoluciones
    - Filtros y pooling
    - Data Augmentation
- Secuencia
    - RNNs, LSTM y GRUs
    - Procesamiento de Lenguaje Natural
    - Series de Tiempo
- Generativo
    - GANs
    - Autoencoders
    - Style transfer
- Deployment de modelos de ML

PARTE 2: Seguridad Informática

- Introducción
    - Conceptos básicos de seguridad informática
    - Mecanismos de Seguridad

- Vulnerabilidades
    - Modelado de amenazas
    - Análisis de Vulnerabilidades
    - Administración de privilegios
- Cifrado
    - Algoritmos de cifrado
    - Funciones hash
    - Infraestructura de clave pública

- Seguridad a nivel de OS
    - Diferencias principales en sistemas Windows y *nix
    - Seguridad en dispositivos móviles Android y iOS
- Seguridad a nivel de red
    - Controles y dispositivos de seguridad
    - Seguridad en la nube
- Seguridad web
    - Estándares en aplicaciones web
    - Mejores prácticas al desarrollar software
- Manejo de incidentes

EVALUACIÓN

Exámenes	30 Pts.
Tareas	5 Pts.
Autoevaluación	5 Pts.
Prácticas de Laboratorio	30 Pts.
Proyectos	30 Pts.
Nota Final	**100 Pts.**

HORARIO DEL CURSO

El curso consta de 5 créditos académicos (CA)

REQUISITOS DE APROBACIÓN

Para aprobar el curso, además de obtener una nota mayor o igual a 61, el estudiante debe de cumplir con los siguientes requisitos:
Al menos 80% de asistencia a clase
Al menos 60% de nota de laboratorios

ENTREGAS TARDE

Las entregas tarde tendrán un punteo máximo de 50 por un día tarde y después de un día no se aceptará la entrega. Se le recomienda que no espere hasta el último momento para entregar su tarea, trate de calendarizar sus actividades de tal manera que entregue las asignaciones un día antes de la fecha final o con varias horas de anticipación a la hora de cierre. Todas las tareas y proyectos serán entregados únicamente a través del GES.