

SEMINARIO ALEATORIO 452

ADVERSARIAL CLASSIFICATION

RESUMEN:

In multiple domains such as malware detection, automated driving systems, or fraud detection, classification algorithms are susceptible to being attacked by malicious agents willing to perturb the value of instance covariates in search of certain goals. Such problems pertain to the field of adversarial machine learning and have been mainly dealt with, perhaps implicitly, through game-theoretic ideas with strong underlying common knowledge assumptions. These are not realistic in numerous application domains in relation to security. We present an alternative statistical framework that accounts for the lack of knowledge about the attacker's behaviour using adversarial risk analysis concepts.

Presentado por



FABRIZIO RUGGERI

**International Statistical Institute President
(2025-2027)**

**Senior Fellow, Italian National Research
Council (CNR IMATI, Milano)**


**Former President of European Network for
Business and Industrial Statistics (ENBIS),
International Society for Bayesian Analysis
(ISBA) and International Society for Business
and Industrial Statistics (ISBIS)**

ISI Vice President (2017-2021)

**Fellow of American Statistical Association
(ASA), ISBA and Institute of Mathematical
Statistics (IMS), ENBIS Honorary Member and
Zellner Medal recipient**

Detalles del evento:

 **Fecha:** Viernes 20 de marzo, 2026

 **Hora:** 13:00 (Hora Centro de México)

 **Ubicación:** Sala de Conferencias
ITAM Campus
Campus Río Hondo

Conexión Zoom:

ID reunión: 974 3744 1828

Código: 950511