Tutor: David Rios Insua (https://www.icmat.es/drios)

Tema: Adversarial Machine Learning

Descripción: Adversarial Machine Learning refers to robustifying Machine Learning algorithms against adversarial attacks with potentially catastrophic consequences. Many foundational, methodological and computational issues in the field are still open. Depending on the interests and skills of the candidate we shall explore one (or more) of such issues.