

# Position Offered: PREDOCTORAL RESEARCHER

Project: *SECURIA. SECURe artificial intelligence*

**Technological and scientific fields:** Artificial Intelligence and Cybersecurity

**Location:** Madrid, Comunidad de Madrid, ICMAT, <https://www.icmat.es>

**Research Group/PI:** DataLab, IP: David Ríos Insua. <https://datalab.icmat.es>

## PROJECT SUMMARY

Besides the benefits brought by artificial intelligence, a series of associated risks have been identified, focusing mainly on attacks against machine learning algorithms due to their potentially very negative impacts. Such threats are exacerbated by the massive adoption of these technologies, particularly since the rise of LLMs. From a regulatory and public policy perspective, the importance of this problem is well reflected in the EU AI Act. From a technical perspective, the growing importance of the field of adversarial machine learning is highlighted, primarily based on game theory methods under unrealistic common knowledge assumptions in the realm of security and cybersecurity.

Within the SECURIA project, this position will develop more rigorous methods and algorithms to strengthen machine learning algorithms against targeted attacks, which will converge into operational pipelines for their implementation in real-world AI-based systems. The methodology and software produced will be made available to the community to promote a more responsible and secure development of AI.

## PROFESSIONAL PROFILE

### Minimum requirements:

- Graduate or Bachelor's degree in Mathematics or Physics.
- Master in Statistics and Data Analysis.
- Knowledge of English and Spanish.

### Merits to be considered:

- Proficiency in Python programming language.
- Training in Bayesian analysis and machine learning techniques.
- Proven experience with research contracts.

## WHAT IS OFFERED

Cutting-edge training is offered in such current topics as Artificial Intelligence and Cybersecurity, aimed at pursuing a doctoral thesis in the area of Adversarial Machine Learning (AML), a fundamental pillar for developing a rigorous risk management framework in AI. The training program includes stays in leading AML laboratories such as Cagliari and Urbana Champaign, training in digital skills associated with the activities of the DataLab, as well as training in market transfer and dissemination of research within the activities of the aforementioned group integrated into the ICMAT, a reference center in mathematical research in Spain.

### Contract conditions:

Predoctoral Researcher contract of 4 years' duration. Gross annual salary of 23,871.33 €.

**Start of contract: before 31 December 2024**

## PRINCIPAL INVESTIGATOR CONTACT

Email: [marta.sanz@icmat.es](mailto:marta.sanz@icmat.es)

Phone: +34 91 29 99 743 / +34 607 40 77 00

[momentum@csic.es](https://momentum.csic.es/) | <https://momentum.csic.es/>