UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

# ANUNCIO DE CONFERENCIA

POSGRADO

# Do you trust your artificial intelligence system?

Robson de Oliveira Albuquerque
Universidad de Brasilia

Facultad de Informática
On-line https://meet.google.com/oha-igvo-gkz
jueves 2 de diciembre de 2021 - 17:30

**Resumen:**

This lecture will address issues of trust in computer systems, artificial intelligence and attacks on these types of systems with practical examples. Artificial Intelligence has gained ground in several areas with different applications scenarios, but in the perspective of this lecture, the fundamental point of the discussion is: what does an artificial intelligence system should do from a security perspective and how does an intelligence system provide results on a given subject? Few people are really concerned about the behavior of these types of systems from a security point of view. If you like machine learning and security, I believe this lecture will show you interesting security problems in artificial intelligence systems.

**Sobre Robson de Oliveira Albuquerque:**

Robson de Oliveira Albuquerque received his Doctorate Degree from UnB in 2008 and got a PhD from UCM in 2016. In 2020 he finished his postdoc in cybersecurity at UnB in association with the professional postgraduate program in electrical engineering. He has more than 25 years of experience in computer networks, information systems and network security. His field of study and research includes Information Systems, Computer Networks, Network Security, Information Security and Cybersecurity. His professional skills include IT consulting for private organisations and the Brazilian Federal Government. He is a member of the Professional PostGraduate Program in Electrical Engineering (PPEE) in the Electrical Engineering Department, at the University of Brasília. He contributes as a Researcher and Professor at the Brazilian National Science and Technology Institute on Cybersecurity (CyberSecurity INCT) - LATITUDE Laboratory. He is member of AQUARELA research group at University of Brasilia. He has more than 50 international publications in journals and conferences related to computer science, computer networks, information security and cybersecurity.