JNIC 2024: IX Jornadas Nacionales de Investigación en Ciberseguridad

Escuela Técnica Superior de Ingeniería Informática - Universidad de Sevilla

Sevilla, Spain, May 27-29, 2024

Conference website	https://2024.jnic.es/
Submission link	https://easychair.org/conferences/?conf=jnic2024
Deadline track de investigación	March 15, 2024
Submission deadline	March 15, 2024
Deadline track de formación y transferencia	March 22, 2024

The IX National Symposium on Cybersecurity Research (JNIC), organized jointly with INCIBE, serves as the scientific-technical forum for presenting relevant and recent contributions in all fields related to cybersecurity and its applications. Articles, in English or Spanish, are welcome in three tracks:

1.Cybersecurity Research. Scientific contributions in any area related to cybersecurity, especially in the following: cryptographic techniques, anonymity, and privacy; security and privacy of blockchain and its applications; forensic analysis of networks, systems, and documents; measures or systems for cyber attacks and defense; cryptography and quantum and post-quantum security; physical security and information theory for security; detection, prevention, and response to intrusions; detection, prevention, and mitigation of malware; security and privacy for big data and machine learning; protocols, standards, and measures for internet security; security in cyber-physical systems and OT environments; security and privacy in social networks, Metaverse, or AR/VR/MR environments; security and privacy assisted or based on artificial intelligence and machine learning; data protection and legal and economic aspects of cybersecurity. Contributions are sought in the form of:

- **Articles (up to 8 pages):** Original scientific papers with results or in development.
- **Extended abstracts (2 pages):** Scientific papers published during 2023. The title and publication reference must be indicated.

2. Education track: Contributions in the field of training and educational innovation in cybersecurity of various kinds, especially those related to:

- **Educational projects/actions or innovations in teaching** on cybersecurity to improve academic performance and personal development of students.
- **Actions or activities for talent acquisition in cybersecurity**, such as strategies or methodologies to attract qualified candidates and/or assess applications.
- **Innovative proposals for academic practices in cybersecurity**, indicating the subject, learning objectives, design or planning, criteria and methods of evaluation, as well as expected learning outcomes.

- **Works focused on the design, methodologies, tools, or experiences in training and education in cybersecurity,** at any educational level, especially those already implemented.

Contributions are requested in the form of articles (up to 8 pages).

3. Transfer track Contributions dedicated to highlighting and promoting interaction between the research field and the business/technological sector, emphasizing the impact and innovation in the transfer of knowledge and technology. Contributions are sought that not only reflect significant advances in terms of research and development but also demonstrate a tangible impact on industry or society. The thematic areas are those covered in the research track. Contributions must meet at least one of the following conditions:

- **R&D projects carried out with companies or end-users of technology:** The project must have been completed or reached a phase where effective knowledge or technology transfer is evident.
- **Cases of effective technology transfer:** Contributions describing the successful transfer of previously developed technology to companies or end-users.
- **Licensed patents:** Details of patents that have been effectively licensed, highlighting their application and relevance in the market or society
- **Established spin-offs:** Description of emerging companies (spin-offs) established from technological research or developments, emphasising their impact and innovation.

Contributions are requested in the form of articles (up to 8 pages), including references and acknowledgments. Each contribution will be evaluated based on its impact, relevance, originality, clarity, and compliance with specified contribution criteria.