2023 JNIC Cybersecurity Conference (JNIC'23)
Vigo (Spain), June 21 to 23, 2023
https://2023.jnic.es

The 2023 JNIC Cybersecurity Conference, organized jointly with INCIBE, is the scientific-technical forum for the presentation of relevant and recent contributions in all fields related to cybersecurity and its applications. Papers will be accepted, in English or Spanish, in three tracks (consult the Call For Flags):

1. **Research track**. Research contributions in any area related to cybersecurity, especially in these: Cryptographic, anonymity and privacy techniques; Security and privacy of blockchain and its applications; Network, system and document forensics; Cyber-attack and cyber-defense measures or systems; Quantum and post-quantum cryptography and security; Physical security and information theory for security; Intrusion detection, prevention and response; Malware detection, prevention and mitigation; 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 by or based on artificial intelligence and machine learning; Data protection and legal and economic aspects of cybersecurity. Contributions are requested in the form of: (1) Articles (max. 8 pages): original research works with proven results, or research work in progress; or (2) Extended abstracts (2 pages) of outstanding scientific papers published during 2022. The title and reference of the publication should be indicated.

2. **Technology transfer track:** Contributions that describe patents, prototypes, products, and more generally works transferred to the business sector or to society, highlighting their innovative nature. Also works carried out in collaboration with companies, either through a contract or funded by a public competitive call. The topics are those included in the research track. Contributions are requested in the form of Articles of up to 8 pages.

3. Educational track. Training. Contributions in the field of training and educational innovation in cybersecurity of various kinds and, especially the following: (i) educational or teaching innovation projects/actions in order to improve academic performance and personal development of the students; (ii) actions or activities to attract cybersecurity talent, for example, strategies or methodologies to attract qualified candidates and/or to assess that candidates; (iii) innovative proposals for academic lab assignments in cybersecurity, indicating the subject, learning objectives, design or planning, evaluation criteria and methods, as well as the expected learning outcomes; and (iv) in general, works oriented towards the design, methodologies, tools or experiences of training and education in cybersecurity, at any educational level. Contributions are requested in the form of Articles of up to 8 pages.

IDATES

	Research track	Technology Transfer and Educational tracks
Submission	31st of March	21st of April
Acceptance notification	30th of April	15th of May
Final submission	15th of May	30th of May

PAPER SUBMISSIONS

The submission of papers will be through EasyChair (this link). All the contributions (in Spanish or English) must respect the IEEEtrans conference template for JNIC, either in LaTeX format or in MS Word format (Templates and overleaf access).

PUBLICATION

Accepted papers will be submitted for inclusion into IEEE Xplore subject to meeting IEEE Xplore's scope and quality requirements. Extended versions of the top papers will be reviewed for possible publication in special issues of scientific journals like Wireless Networks (WINET) (Q2).

All contributions that are accepted and effectively presented at the Conference by their authors will be published in the Conference Proceedings. In addition, accepted scientific articles (Research Track) will be sent for publication in IEEEXplore in compliance with its quality criteria and thematic scope.

The articles with the best results in the review process may be invited to special issues of relevant magazines, such as Wireless Networks (WINET). In case of being invited, the authors will be required to provide a minimum extension of 30% with respect to the original, that it be written entirely in English and that it constitutes a substantial improvement. The invitation will follow an additional review process that will determine, where appropriate, acceptance in the special issue.

All participation in the JNIC 2023 will be subject to the acceptance of the rules and regulations. The authors of research, technology transfer, and educational contributions subscribe with them the commitment to present the accepted papers during the Conference.

AWARDS

The Conference will also host the RENIC Cybersecurity Research Awards, to which Master's theses and doctoral dissertations on cybersecurity may be submitted in accordance with these rules and dates.