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

Las **IX Jornadas Nacionales de Investigación en Ciberseguridad (JNIC)**, que se organizan de forma conjunta con INCIBE, son el foro científico-técnico de presentación de contribuciones relevantes y recientes en todos los campos relacionados con la ciberseguridad y sus aplicaciones. Se aceptarán artículos, en inglés o en español, en tres *tracks*:

1. Investigación en ciberseguridad. Contribuciones científicas en cualquier área relacionada con la ciberseguridad y, especialmente, en las siguientes: Técnicas criptográficas, de anonimato y de privacidad; Seguridad y privacidad de blockchain y sus aplicaciones; Análisis forense de redes, sistemas y documentos; Medidas o sistemas de ciberataque y ciberdefensa; Criptografía y seguridad cuántica y poscuántica; Seguridad física y teoría de información para seguridad; Detección, prevención y respuesta a intrusiones; Detección, prevención y mitigación de malware; Seguridad y privacidad para big data y machine learning; Protocolos, estándares y medidas para seguridad en Internet; Seguridad en sistemas ciberfísicos y entornos OT; Seguridad y privacidad en redes sociales, Metaverso o entornos AR/VR/MR; Seguridad y privacidad asistidas por o basadas en inteligencia artificial y machine learning; Protección de datos y aspectos legales y económicos de la ciberseguridad. Se solicitan contribuciones en forma de:

- **Artículos (Hasta 8 páginas):** Trabajos científicos originales con resultados o en desarrollo.
- **Resúmenes extendidos (2 páginas):** Trabajos científicos publicados durante 2023. Se ha de indicar el título y referencia de la publicación.

2. Formación en ciberseguridad. Contribuciones en el ámbito de la formación e innovación educativa en materia de ciberseguridad de diversa índole y, en especial las siguientes:

- **Proyectos/acciones educativos o de innovación docente** sobre ciberseguridad en aras de la mejora del rendimiento académico y el desarrollo personal de los estudiantes
- **Acciones o actividades de captación de talento en ciberseguridad**, por ejemplo, estrategias o metodología para atraer candidatos cualificados y/o para valorar las candidaturas

- **Propuestas innovadoras** para prácticas académicas en ciberseguridad, indicando la materia, los objetivos de aprendizaje, diseño o planificación, criterios y métodos de evaluación, así como los resultados de aprendizaje esperados
- **Trabajos orientados al diseño, metodologías, herramientas o experiencias de formación y educación en ciberseguridad**, en cualquier nivel educativo, especialmente las ya implantadas.

Se solicitan contribuciones en forma de artículos de hasta 8 páginas.

3. Transferencia en ciberseguridad. Contribuciones dedicadas a destacar y promover la interacción entre el ámbito investigador y el sector empresarial/tecnológico, subrayando el impacto y la innovación en la transferencia de conocimiento y tecnología. Se buscan contribuciones que no solo reflejen avances significativos en términos de investigación y desarrollo, sino que también demuestren un impacto tangible en la industria o en la sociedad. Las áreas temáticas son aquellas recogidas en el track de investigación. Las contribuciones deben cumplir al menos con una de las siguientes condiciones:

- **Proyectos de I+D realizados con empresas o usuarios finales de tecnología**: El proyecto debe haber finalizado o alcanzado una fase donde se evidencie una transferencia efectiva de conocimientos o tecnología.
- **Casos de transferencia de tecnología efectiva**: Contribuciones que describan la transferencia exitosa de tecnología previamente desarrollada a empresas o usuarios finales.
- **Patentes licenciadas**: Detalle de patentes que hayan sido efectivamente licenciadas, destacando su aplicación y relevancia en el mercado o sociedad.
- **Spin-offs constituidas**: Descripción de empresas emergentes (spin-offs) establecidas a partir de investigaciones o desarrollos tecnológicos, enfatizando su impacto e innovación.

Se solicitan contribuciones en forma de artículos de hasta 8 páginas incluyendo referencias y reconocimientos (Acknowledgements). Cada contribución será evaluada según su impacto, relevancia, originalidad, claridad, y el cumplimiento de los criterios de contribución especificados.