VIII Jornadas de Investigación en Ciberseguridad (JNIC'23)
Vigo, 21 a 23 de junio de 2023
Call For Papers

https://2023.jnic.es

Las VIII Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), que se organizan presencialmente 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* ***(CONSULTA LA LLAMADA Call For Flags AQUÍ)*****:**

1. Investigación. 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; Forensia 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: (1) Artículos (Hasta 8 páginas): trabajos científicos originales con resultados o en desarrollo; o (2) Resúmenes extendidos (2 páginas): trabajos científicos publicados durante 2022. Se ha de indicar el título y referencia de la publicación.

2. Transferencia: Contribuciones que describen solicitudes de patentes/patentes, prototipos, productos, y de forma más general trabajos transferidos al tejido empresarial o a la sociedad destacando su carácter innovador. También trabajos realizados en colaboración con empresas, ya sea mediante un contrato o financiado por una convocatoria pública de carácter competitivo. Las áreas temáticas son las recogidas en el track de investigación. Se solicitan contribuciones en forma de Artículos de hasta 8 páginas.

3. Formación. Contribuciones en el ámbito de la formación e innovación educativa en materia de ciberseguridad de diversa índole y, en especial las siguientes: (i) proyectos/acciones educativos o de innovación docente sobre ciberseguridad en aras de la mejora del rendimiento académico y el desarrollo personal de los estudiantes; (ii) acciones o actividades de captación de talento en ciberseguridad, por ejemplo, estrategias o metodología para atraer candidatos cualificados y/o para valorar las candidaturas; (iii) 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; y (iv) de forma general, 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.

FECHAS

	Track Investigación	Track Transferencia y Formación
Envío	~~31 de marzo~~ 16 de abril	~~21 de abril~~ 28 de abril
Notificación de aceptación	~~30 de abril~~ 5 de mayo	15 de mayo
Envío final de artículos	15 de mayo	30 de mayo

JNIC2023

ENVÍO DE TRABAJOS

El envío de todos los trabajos se realizará a través de la plataforma EasyChair en este enlace. Todas las contribuciones (que podrán ser en español o en inglés) seguirán el estilo IEEEtrans dispuesto para JNIC tanto en formato Latex como en formato MS WORD (Plantilla y Acceso overleaf).

PUBLICACIÓN

Todas las contribuciones que sean aceptadas y efectivamente presentados en las Jornadas por sus autores serán publicadas en un Libro de Actas de las Jornadas. Además, los artículos científicos aceptados (Track Investigación) se enviarán para publicación en IEEEXplore bajo cumplimiento de sus criterios de calidad y ámbito temático.

Los artículos con mejores resultados en el proceso de revisión podrán ser invitados a números especiales de revistas relevantes, como Wireless Networks (WINET). Caso de ser invitados, se requerirá que los autores aporten una extensión mínima del 30% con respecto al original, que sea escrito íntegramente en inglés y que dicha extensión constituya una mejora sustancial. La invitación seguirá naturalmente un proceso adicional de revisión que determinará, en su caso, la aceptación en el número especial.

Toda participación en las JNIC 2023 estará sujeta a la aceptación de las bases reguladoras. Los/as autores/as de contribuciones de investigación y de formación e innovación educativa suscriben con ellas el compromiso de presentar los trabajos aceptados durante las Jornadas.

PREMIOS

Las Jornadas albergan además el fallo de los Premios RENIC de Investigación en Ciberseguridad, a los que se podrán presentar trabajos de fin de máster y tesis doctorales sobre ciberseguridad de acuerdo con estas bases y fechas.

gradiant

atlanTTic

Universidade Vigo

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD