Conf-IRM 2027 Bogota, Colombia, 31 May – 2 June, 2027

Conference Theme: **Intelligent & Fragile Infrastructures: Governing Complexity in Information Systems**

Track Number	5
Track Name	Cybersecurity, Privacy & Digital Infrastructure Resilience
Track Co-Chairs	**Sandra Rueda** (Uniandes, Colombia), sarueda@uniandes.edu.co **Anita Neumannova** (WU Vienna, Austria), anita.neumannova@wu.ac.at **Barbara Krumay** (Johannes Kepler Universität Linz, Austria), barbara.krumay@jku.at
Track Description	In an increasingly digital world, organizations face growing challenges in protecting sensitive information and maintaining the stability of critical infrastructure against major threats (i.e., cyber incidents, geopolitical tensions, natural disasters, or supply chain risks). Additionally, the rise of artificial intelligence has transformed the threat landscape, enabling more advanced, automated, and adaptive attacks that require equally innovative defense strategies and are reshaping the regulatory landscape. The aim of this track is to delve deeper into the strategies and governance mechanisms essential for building secure, trustworthy, and resilient organizations. The key themes examine how organizations can instill robust security practices while addressing the complex interplay between safeguarding digital assets and ensuring continuous, reliable operation in a rapidly evolving landscape. This track invites contributions to strengthen the security and resilience of existing systems from a management perspective, bridging technical insights and strategic business concerns. Topics include, but are not limited to: 1. **Security Frameworks, Regulatory Compliance, and Governance:** Examining how organizations can develop robust security frameworks that align with business strategies, including risk management practices, regulatory compliance, and governance models. 2. **Digital (Infrastructure) Resilience and Business Continuity:** Detailing the technical measures, alongside strategies for ensuring business continuity and digital resilience, organizations can employ to safeguard against major threats (i.e., cyber incidents, geopolitical tensions, natural disasters, or supply chain risks). 3. **Human Factors in Security:** Exploring the critical role of human behaviour and organizational culture in security, including training, awareness programs, and the psychology behind security breaches and incident responses. 4. **Emerging Threats and AI-driven Security:** Assessing the evolving landscape of security threats and the role of artificial intelligence (i.e., machine learning, natural language processing) in predicting and mitigating cyber-attacks. 5. **Data Privacy and Protection:** Addressing the challenges and strategies related to data privacy and protection in an increasingly digital world, including regulatory compliance and ethical considerations. 6. **IoT cybersecurity-related issues:** Addressing the challenges of an increasingly connected world, and the consequent larger attack surface, with IoT-enabled solutions as a key component of Industry 4.0 and Smart X environments.