International Forum

Crisis and Emergency Management in Light of Combating Cyber Intrusions and Attacks: The "Spanish model"

29 June - 2 July, 2026

Madrid, Spain

Jesus Castellanos

International IT security consultant, Relational Tools S.L.

Director of Product and Design of Cybersecurity Services

ICA Sistemas y Seguridad

Adrià Arribas

P.Chief Operating Officer ,Apolo Cybersecurity

Chief Information Security Officer, Light Eyes Spain

Dr. Ammar A. Abu. Obaid

Former. MIS Officer
State Department, USA, Cyber Spe
Microsoft. Certified. Systems Engineer.
PMI, Certified
ICT Professional Project. Manager

Tel: +965 90939008 Fax: +965 22455728 Cell/WhatsApp: +965 90939008 P.O. Box 2277 Safat 13023, Kuwait
Email: marketing@consulenzakw.com Web: www.consulenzakw.com/Conferences

1.1 Forum Description

1.1 Introduction

The accelerating pace of digital transformation has significantly increased the dependence of governments, critical infrastructure operators, businesses, and public institutions on interconnected digital systems. While these advancements have enhanced efficiency and innovation, they have also expanded the landscape of cyber threats, exposing organizations to increasingly sophisticated cyber intrusions and information, ransomware attacks, data breaches, and disruptions to essential services.

In this evolving environment, effective crisis and emergency management has become a strategic necessity for ensuring national resilience, protecting critical assets, and maintaining public trust. Cyber incidents now possess the potential to escalate rapidly into large-scale crises affecting economic stability, public safety, national security, and the continuity of essential operations.

Spain has emerged as a leading example in the development of integrated cybersecurity governance, crisis response frameworks, and public-private cooperation mechanisms. The Spanish model combines advanced cybersecurity capabilities, institutional coordination, emergency preparedness, and resilience-building strategies that offer valuable lessons for governments, organizations, and professionals worldwide.

This conference aims to examine contemporary cyber threats and explore best practices in crisis and emergency management through the lens of the Spanish experience. It seeks to provide participants with practical knowledge, strategic insights, and collaborative opportunities to strengthen preparedness, response, recovery, and resilience in the face of cyber emergencies and digital crises, we expect from the attendees and senior officials that they understand the information security in working and thinking levels, some insight into management systems and basic knowledge of the new GDPR legislation would be desirable. Some technical knowledge of networks, systems and applications is an advantage, and genral fram for Cyber Security Governance.

1.2 Forum Topics

- *The Evolving Cyber Threat Landscape and Information systems.*
* Emerging cyber risks and attack trends
* State-sponsored cyber operations
* Cybercrime and organized cyber threats
- *Cybersecurity and National Crisis Management*
* *Integrating cybersecurity into national emergency plans*
* Strategic governance and decision-making during cyber crises
* Protection of national critical infrastructure
- *The Spanish Model for Cyber Crisis Response*
* *Spain's cybersecurity governance framework*
* Roles of national cybersecurity institutions
* Lessons learned from major cyber incidents
- *Incident Response and Emergency Coordination*
* Cyber incident response frameworks
* Multi-agency coordination during emergencies
* Crisis communication and stakeholder management
- *Critical Infrastructure Protection*
* Energy, transportation, healthcare, and telecommunications sectors
* Risk assessment and vulnerability management
* Business continuity and operational resilience
- *Artificial Intelligence and Cybersecurity*
* AI-driven threat detection and response
* Risks associated with AI-enabled cyberattacks
* Future trends in cyber defense
- Public-Private Partnerships in Cyber Resilience
* Information sharing and collaboration mechanisms

* Building resilient digital ecosystems
* International cooperation and cross-border response
- *Cyber Crisis Simulation and Preparedness*
* Tabletop exercises and cyber drills
* Developing organizational readiness
* Training leadership teams for cyber emergencies
- *Legal, Regulatory, and Policy Frameworks*
* Data protection and privacy considerations
* International standards and best practices
- *Recovery and Organizational Resilience*
* Post-incident recovery strategies
* Lessons-learned frameworks
* Building long-term cyber resilience

1.3 Forum Topics schedule

Time: 9:am to 2:00 pm

Day 1: 29 June, 2026

- The Evolving Cyber Threat Landscape and Information systems.
- Cybersecurity and National Crisis Management
- The Spanish Model for Cyber Crisis Response
- Risk management
- Spanich experience

Day 2: 30 June, 2026

- Incident Response and Emergency Coordination
- Critical Infrastructure Protection
- Privacy issues within organizations
- Artificial Intelligence and Cyber Security
- Security Incident and incident response

Day 3: 1 July, 2026

- Public-Private Partnerships in Cyber Resilience
- Cyber Crisis Simulation and Preparedness
- Legal, Regulatory, and Policy Frameworks
- Recovery and Organizational Resilience

Day 4: 2 July, 2026

- General Discussion
- Questions and Inquiries
- Attendance Certificates

Target Audience:

VIPs - Senior and Middle Management Office Staff - Information Systems Center Staff - Risk Management Staff - Cybersecurity and Information Security Staff

Tel: +965 90939008 Fax: +965 22455728 Cell/WhatsApp: +965 90939008 P.O. Box 2277 Safat 13023, Kuwait
Email: marketing@consulenzakw.com Web: www.consulenzakw.com