International Forum

Information security and combating cyber intrusions: The Spanish experience"

28 June -1 July, 2026

H.Regency Hotel, Madried, 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

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

1.1 Forum Description

Nowadays, more and more Inistitutions suffer many damage because hackers from various origins abuse vulnerabilities in a process, system, network, application or infrastructure. These are Nation state actors, hackers commissioned by companies to steal Intellectual property, Hackers who use an environment as a test object, crackers who do damage to get ransom or just script kiddies who find something. But even hackers who get hacked again can pose a risk.
In addition, Cyber security, privacy and Governance are often seen as separate disciplines for which different people are also responsible for in a Inistitutions (Chief Information Security Officer (CISO), Computer Emergency Response Team (CERT) or Data Protection Officer (DPO)). However, these disciplines can all be well integrated based on risk management and information security management systems, like Cobit 5 and ISO27001. During this training you will receive concrete information about what is (legal, technical and organizational) expected of you with regard to Cyber security and how you can get started with this in practice. The trainers draw up an effective (cyber) security and privacy approach with you that integrates people, processes and technology. Together with you, they look for the balance where privacy and security reinforce each other instead of opposing them. During the training you work on cases and assignments where the theory is linked to your daily practice.

1.2 Prior Knowledge

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.

1.3 Trainer

Your highly experienced and leading trainers are experts in the field of cybersecurity and privacy and work together with several universities worldwide. Next to that they are able to assist you with advice and many tips and practical examples.

1.4 Forum Topics

- Introduction
- Information security and Cyber Security
- The role of a baseline measurement, audit, control or review.
- ASSIGNMENT: SCOPING
- Human aspects around information security.
- Goverance and Standards and frameworks for Cyber Security.
- Risk management, Information Security Management System.
- Privacy aspects of information security.
- The risk of interfacing systems and data.
- Data breach reporting obligations.
- Privacy issues within organizations.
- Security Incident and incident response.
- Privacy and Governance.
- Business Continuity , Audits and results.
- Security Scans, - DEMO: How to hack a user account.
- Penetration testing and Red Team / Blue Team testing.
- Spanich experinace.

1.5 Forum Topics schedule

Time: 9:am to 2:00 pm

Day 1: 28 June, 2026

- Information security and Cyber Security
- Human aspects around information security
- Standards and frameworks for Cyber Security
- Risk management
- Spanich experinace
- Goverance and Standards and frameworks for Cyber Security.

Day 2: 29 June, 2026

- CyberSecurity Privacy
- Data Data breach reporting obligation
- Privacy issues within organizations
- Financial transfers and secure payment systems
- Security Incident and incident response
- CyberSecurity Governance

Day 3: 30 June, 2026

- KPIs for ensuring privacy
- Audits and results , Security Scans
- Penetration testing and Red Team / Blue Team testing
- Access control (Identity Management & Access Control / IAM)

Day 4: 1 July, 2026

- General Discussion
- Questions and Inquiries
- Attendance Certificates