

#CSBC2026

# Cybersecurity Summer Bootcamp



LEÓN - 2026

**July 13 to 23, 2026**  
Leon, Spain

Organized by:



With the collaboration of:



## GENERAL INFORMATION

### CSBC Objectives:

- ◊ To train and educate participants in the latest techniques for combating cybercrime, incident management, and legal aspects of cybersecurity.
- ◊ To improve coordination in the management of incidents and cybercrime.
- ◊ To promote international collaboration and the creation of expert networks.
- ◊ To foster cooperation among law enforcement agencies, regulators, judges, and prosecutors in the field of cybersecurity through a practical format.

### Languages of Instruction:

- ◊ **Spanish:** all tracks.
- ◊ **Inglés:** CSIRT/CERT (basic and advanced levels) and *Policy Makers*.

### Difficulty Level:

- ◊ Law Enforcement Agencies (LEAs) and CSIRT/CERT: basic and advanced.

### Key Features:

- ◊ International and free event.
- ◊ Exclusive, high-quality training.
- ◊ Innovative topics and the latest trends in cybercrime detection.
- ◊ Practical workshops delivered by leading professionals.
- ◊ High-level networking opportunities.

### Target Audience:

- ◊ **Law Enforcement Agencies (LEAs):** members of operational cybersecurity units.
- ◊ **CSIRT/CERT:** technical staff from security incident response teams.
- ◊ **Prosecutors:** legal professionals specializing in cybercrime.
- ◊ **Judges and magistrates:** legal professionals in cybercrime and cybersecurity.
- ◊ **Policy Makers:** political actors, regulators, and cybersecurity policymakers.



**More information:**  
[www.incibe.es/en/events/summer-bootcamp](http://www.incibe.es/en/events/summer-bootcamp)

## EVENT FEATURES

**International training program specialized in cybersecurity.**

**Distributed across 5 tracks**

**220 instructional hours**

- ♦ Law Enforcement Agencies (LEAs): 40 hours.
- ♦ CSIRT/CERT in Spanish: 40 hours.
- ♦ CSIRT/CERT in English: 40 hours.
- ♦ Judicial Track (judges and prosecutors): 20 hours per track.
- ♦ Policy Makers (in English): 40 hours.

**\*Indicative hours subject to change.**

**Specialized workshops:** delivered by leading experts for each track.

## TRAINING PROGRAMS

The Cybersecurity Summer BootCamp 2026 offers an intensive academic program structured into specialized learning pathways, with a strongly practical approach based on active methodologies, advanced simulations, and real-case analysis.

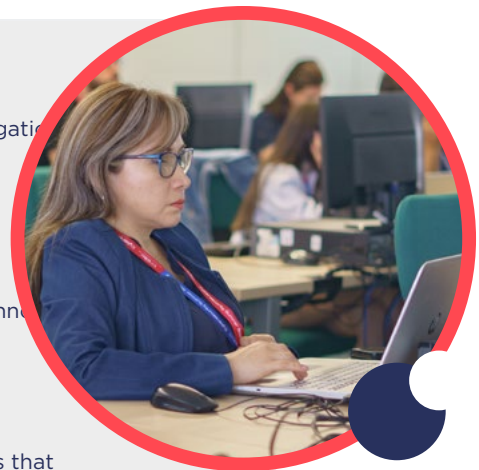
### Law Enforcement Investigation (LEAs):

Program aimed at operational units specialized in technological investigation and cybercrime.

**Key areas:**

- ♦ OSINT applied to criminal investigations.
- ♦ Digital forensics and electronic evidence management.
- ♦ Investigation of crimes involving cryptocurrencies and blockchain technology.
- ♦ Deepfakes and digital manipulation as emerging threats.
- ♦ Cyberterrorism and online radicalization.
- ♦ Protection and response to attacks on critical infrastructures.

The approach is highly practical, with simulations and real-case analysis that strengthen operational capabilities and inter-agency coordination.



### CSIRT/CERT Operations

Designed for technical professionals responsible for incident detection and response.

**Main topics:**

- ♦ End-to-end incident and cyber crisis management
- ♦ Threat hunting and proactive analysis
- ♦ Malware analysis.
- ♦ Cloud security.
- ♦ Detection of advanced persistent threats (APT).
- ♦ Collaborative Red vs Blue Team exercises.

The program concludes with a practical Core NetWars-type exercise, enabling participants to test acquired competencies in a realistic environment.

# TRAINING PROGRAMS

## Judges Program

A track designed to strengthen judicial capacity in addressing cybercrime.

**Topics covered:**

- Emerging types of digital crime.
- Admissibility and evaluation of electronic evidence.
- International judicial cooperation.
- Protection of fundamental rights in technological investigations.

The program combines practical case analysis with interdisciplinary discussions involving technical experts.



## Prosecutors Program:

Focused on the strategic direction of criminal investigations in the digital environment.

**Includes:**

- Prosecution strategies in technology-related crimes.
- Coordination with technical and law enforcement units.
- Investigation of cyber-enabled financial crimes.
- International cooperation instruments.

The program is delivered through practical dynamics and collaborative development of complex case scenarios.

## Policy Makers Program

Designed for public officials and regulators involved in cybersecurity policy design.

**Core areas:**

- Governance and national cybersecurity strategy.
- European and international regulation.
- Digital diplomacy and multilateral cooperation.
- Crisis management at the institutional level.
- Development of regulatory frameworks adapted to emerging technologies.

The approach combines strategic analysis with decision-making exercises in simulated scenarios.



## OTHER ACTIVITIES

### CSBC 2026 complements technical training with opportunities for strategic interaction and international cooperation.

#### High-Level Networking

- Meetings between international delegations.
- Spaces for exchanging best practices.
- Connection between technical, operational, and legal profiles.
- Promotion of long-term collaborative networks.

#### Multidisciplinary Simulations

Practical exercises integrating law enforcement, technical, and legal profiles to manage:

- Cybersecurity crises.
- Attacks on critical infrastructures.
- Scenarios with institutional and media impact.
- Coordination among national and international bodies.

#### Strategic Forums and Dialogues

Discussion spaces focused on:

- Digital diplomacy.
- International cooperation.
- Cybersecurity talent.
- Governance and digital rights.

#### Cultural Activities and León Experience

- Guided tours of León's historical heritage.
- Official CSBC cultural event.
- Social activities designed to strengthen professional relationships.



## RESULTS OF THE 2025 EDITION

**Record Participation: 507** professionals from **27** countries.  
Participants: Law Enforcement Agencies (LEAs), CSIRT/CERT, judges, prosecutors, and Policy Makers.

### 10th Edition Overview:

- 200 hours of advanced training across 5 thematic tracks.
- Workshops and lectures: 104 experts + 5 international keynote speakers.

**Bilingual training:** Spanish and English.

### Highlighted Activities:

- Collaborative role-plays: 238 professionals.
- Global Dialogue on Cybersecurity focused on digital diplomacy.
- Cybersecurity Talent Summit: discussion on employment and capacity building.
- Institutional event “Democracy, Progress and Cybersecurity” with Trinidad Jiménez.
- Cultural activities: concert “Film Music in León” performed by the JOCSMAB Orchestra.

### Address by the Minister for Digital Transformation and Public Service, Óscar López:

- Highlighted the Cybersecurity Summer BootCamp as an international benchmark in cybersecurity.
- Nearly 5,000 individuals trained over 10 years, with 32% female participation.
- Institutional support to strengthen international partnerships and professional excellence.

### Participant Feedback:

**100%** would recommend the training program.

**100%** reported an excellent level of satisfaction.

**90%** found the content highly relevant and useful.



#CSBC2026

# Cybersecurity Summer Bootcamp



LEÓN - 2026

More Information

[www.incibe.es/en/events/summer-bootcamp](http://www.incibe.es/en/events/summer-bootcamp)



Organized by:



With the collaboration of:

