#CyberSBC2022



5 to 15 July 2022 León, Spain

incibe.es/summer-bootcamp

Organizadores



DEL GOBERNO DEL GOBERNO O DE DIGITALIZACIÓN E DOS ECONÓMICOS INTELGENCIA ARTIFICI ORMACIÓN DIGITAL











 AYUNTAMIENTO DE LEÓN





universidad deleón

GENERAL INFORMATION

Objectives:

- To provide training and coaching on the latest techniques in the fight against cybercrime, management of cybersecurity incidents and legislative aspects to be taken into account in relation to same.
- + To improve coordination in incident and cybercrime management.

100% face-to-face format:

- Languages: Spanish and English
- International event, free of charge.
- Certificate with 6 ECTS from the **University of León**.
- Exclusive cutting edge training of the highest quality.
- Novel issues and the most recent trends in detecting cybercrimes.
- Practical workshops given by the best professionals.
- + Highest level networking opportunity with the attendees.

Target Audience:

- State Security Forces and Agencies: Members of Law Enforcement Agencies that work in operational units related to cybersecurity.
- CSIRT o CERT: Technical personnel who work in Incident Response Centres.
- Prosecutors, judges and magistrates: active personnel from judicial or tax authorities, magistrates and State's attorneys who work on cybercrime or cybersecurity cases.
- PM: policy makers, political, regulatory or legislative actors: personnel working in areas regarding legal and regulatory aspects of cybersecurity, policy makers, cybersecurity strategies and diplomacy.

CHARACTERISTICS OF THE EVENT

4 tracks | 114 teaching hours

 35-hour programme aimed at members of Security Forces and Agencies working in operational units related to cybersecurity (FCS).



- **35-hour** programme aimed at **technical staff working in Security Incident Response Centres** (CSIRT).
- 22-hour programme aimed at active personnel belonging to the judicial or prosecutorial careers, state attorneys, civil servants in the Justice Administration (Public Prosecutor's Office, judges and prosecutors).
- A **22-hour** programme aimed at staff from regulatory or legislative bodies working in areas related to the legal and regulatory aspects of cybersecurity (*policy makers*).

WORKSHOPS GIVEN

By leading experts on relevant and current issues for each of the 4 specialisations.

Police investigation (FCS):

| Торіс | Duration |
|--|-----------|
| Criminal investigation in technological environments | 10 hours |
| Digital Forensics and Incident Response (DFIR) | 7,5 hours |
| Digital Forensics in the cloud | 2,5 hours |
| Open Source Intelligence (OSINT) | 5 hours |
| Intelligence in police investigations | 2,5 hours |
| Cryptocurrencies and bank fraud | 2,5 hours |
| Blockchain | 2,5 hours |
| Introduction to <i>deepweb</i> | 2,5 hours |



CSIRT operations:

| Торіс | Duration |
|---|-----------|
| Pentesting / Ethical Hacking | 7,5 hours |
| Forensic analysis | 7,5 hours |
| Cybersecurity incident management | 5 hours |
| Malware analysis | 5 hours |
| Cybersecurity Intelligence for CERT/CSIRT | 5 hours |
| Security warnings | 2,5 hours |
| Legal and Cooperation Aspects | 2,5 hours |

Legislation and regulatory framework:



| Торіс | Duration |
|---|----------|
| Chain of custody and electronic evidence: Practical problems of digital evidence. Random findings. Rights and Freedoms in a digital world. New challenges in criminal procedure. Practical problems of technological investigation proceedings. Ex. Tracking of virtual currencies. | 7 hours |
| Technological research and jurisprudence: Investigation in open sources. Technological innovation as a tool for the FCS Practical fundamentals of technology research. Technological Research in the Case Law of the Supreme Court. | 10 hours |
| Regulation of privacy, data protection and the right to honour: Illegal content on the Internet: special reference to hate crimes. The removal of contents from the Internet: collaboration with private operators | 5 hours |

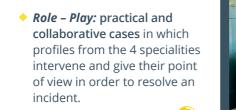
Policy makers:

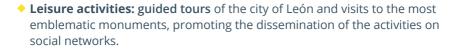
| Торіс | Duration |
|--|-----------|
| Regulations: Impact of privacy and data protection regulation. The removal of contents from the Internet: collaboration with private operators | 5 hours |
| Creation of a Cybersecurity Strategy: The importance of institutional management of cybersecurity: Cybersecurity Governance in Spain and LATAM. Implementation and monitoring of cybersecurity strategies. | 7 hours |
| Options for sustainability and fund building in cybersecurity. | 2,5 hours |
| The role of cyber diplomacy in cyber crisis management. | 1 hours |
| Role of the CSIRT - international CSIRT system. | 1 hours |
| International law applicable to cyberspace. Regulatory developments. | 3,5 hours |
| Legal and Cooperation Aspects. | 2 hours |



OTHER ACTIVITIES

Activities to promote *networking* among attendees and the need for collaboration among them.





 Expert talks on different current topics, ongoing research and new tools related to cybersecurity and other areas.



RESULTS OF THE EVENT IN 2021 Virtual format with 785 participants from 38 countries 4 hours of keynotes and master-classes 54 hours of specific training **30 international** keynotes and speakers **Participants'** feedback: 93% 9,2 9,4 People Remarkable level The contents are of great would recommend of satisfaction interest and usefulness (out of 10) the event (out of 10) 7



#CyberSBC2022

5 to 15 July 2022 León, Spain

incibe.es/summer-bootcamp

















