GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

CALL FOR PAPERS

General conditions of contract for participation
Cybersecurity Summer BootCamp 2022

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

INDEX

1. PURPOSE 3
2. CANDIDATES 3
3. DATES OF THE PROCESS 4
4. PROPOSALS 5
4.1. TYPES OF PROPOSALS 5
4.2. TOPICS OF INTEREST 5
5. PROCEDURE FOR THE SUBMISSION OF PROPOSALS 7
5.1. DEADLINE 7
5.2. SUBMISSION OF PROPOSALS 7
6. ASSESSMENT OF PROPOSALS 7
6.1. WORKSHOPS FOR FCSE AND CSIRTS 7
6.2. LEGISLATION, REGULATORY FRAMEWORK AND POLICY MAKERS 8
7. PROCEDURE FOR THE SELECTION OF PROPOSALS 9
APPLICABLE LAW AND JURISDICTION 9
CONFIDENTIALITY 10
INTELLECTUAL PROPERTY PROTECTION 10
TRANSFER OF IMAGE RIGHTS 10
PERSONAL DATA PROTECTION 11
INVOICING 12
CONTACT 13

INDEX OF TABLES

Table 1. Dates of the process 4
Table 2. FCS Themes 5
Table 3. CSIRT Contents 6
Table 4. Legislation and Regulatory Framework Contents 6
Table 5. Policy maker Contents 7

1. PURPOSE

The purpose of these rules is to regulate the participation and recruitment of **speakers** for the next edition of the Cybersecurity Summer BootCamp event, organised by S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE) together with the Organization of American States (OAS) and in collaboration with the University of León, between 5 and 15 July 2022.

2. CANDIDATES

Any natural or legal person (the candidate) may submit a proposal, although the proposed speaker must be a natural person **over 18 years of age** who is not an INCIBE employee or a student on a scholarship at INCIBE.

In order to participate, candidates must comply with the requirements set out in these rules and send their participation proposal in due time and form following the instructions below.

By means of this call, the minimum number of proposals that guarantee the correct development for each of the four training programmes of the *Cybersecurity Summer BootCamp and* its variants in English version will be selected, of which they will be:

- A programme aimed at members of Security Forces and Agencies working in operational units related to cybersecurity (FCS).
- A programme aimed at technical staff working in Security Incident Response Centres (CSIRTs).
- A 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 programme aimed at staff from regulatory or legislative bodies working in areas related to the legal and regulatory aspects of cybersecurity (Policy Makers).

It is possible that additional workshop needs may arise in the agenda of the event. To address this scenario, the following will be developed:

a) **Ranking of selected proposals**: This list will correspond to the best proposals taking into account the academic programmes of the typologies indicated above and will be selected as the best proposals applying the evaluation criteria set out in these rules.
b) **Classification of proposals in reserve:** The selection will follow the ranking of the proposals submitted from highest to lowest score for each typology starting from the proposals not selected in the previous ranking.

3. DATES OF THE PROCESS

DATES (2022)	ACTION
04 May	Opening of the call for papers
23 May	Closing of the call for papers
23 May	Start of the assessment of the call for papers
30 May	End of assessment
31 May	Notification of accepted call for papers
1 June	Public announcement of selected proposals on the website https://www.incibe.es/summer-bootcamp

Table 1. Dates of the process

4. PROPOSALS

4.1. TYPES OF PROPOSALS

All proposed workshops should focus on **cybersecurity:**

- **Duration:** The minimum duration of each workshop is established according to the subject matter in the section TOPICS OF INTEREST
- **Target audience:** Technical profiles and/or professional experts in cybersecurity.
- **Price**: €250,00 per hour, taxes and deductions not included.
- **Types of proposed formats:**
  - Technical master classes.
  - Live or pre-recorded demonstrations of technologies or techniques.

4.2. TOPICS OF INTEREST

The following is a non-exhaustive, indicative list of topics of interest for the Cybersecurity Summer BootCamp programme:

- **Police investigation (FSC):**

Topic	Estimated 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 DeepWeb	2.5 hours
Full syllabus	**35 hours**

Table 2. FCS Themes

- **CSIRTs operations:**

Topic	Estimated duration
Pentesting / Ethical Hacking	7.5 hours
Forensic analysis	7.5 hours
Cybersecurity incident management	5 hours
Malware analysis	5 hours

Cybersecurity Intelligence for CERTs/CSIRTs	5 hours
Security warnings	2.5 hours
Legal and Cooperation Aspects	2.5 hours
Full syllabus	**35 hours**

Table 3. CSIRT Contents

- **Legislation and regulatory framework:**

Topic	Estimated 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 CSCDF ▪ 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
Full syllabus	**22 hours**

Table 4. Legislation and Regulatory Framework Contents

- **Policy makers:**

Topic	Estimated 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
Full syllabus	**22 hours**

Table 5. Policy maker Contents

5. PROCEDURE FOR THE SUBMISSION OF PROPOSALS

5.1. DEADLINE

The deadline for receipt of proposals to participate in the Cybersecurity Summer BootCamp 2022 is **23:59h (CET) on 23 May 2022**.

5.2. SUBMISSION OF PROPOSALS

In order to submit the proposal, the model document available in the *call for papers* section of the Cybersecurity Summer BootCamp website must be submitted and the required fields must be filled in correctly.

Once the form has been filled-in, it should be sent to the address contacto_SummerBC@incibe.es within the established deadline, indicating the reference in the subject line: «**CFP Cybersecurity Summer BootCamp 2022**».

If deemed necessary by the applicant, additional complementary information on the proposal may be attached.

6. ASSESSMENT OF PROPOSALS

Each proposal will be scored from 0 to 100 on the basis of the following criteria:

*Proposals the main purpose of which is to advertise solutions for commercial purposes will not be accepted.

6.1. WORKSHOPS FOR FCSE AND CSIRTS

- **Topic.** 0 to 20 points.

The proposed topic is included in the list of topics that are presumed to be of interest, providing an innovative approach to it.

- **Expository Clarity.** 0 to 10 points.
  The appropriateness of the structure and outline of the presentation will be assessed, as well as the suitability of the presentation for the target audience and the subject matter presented.

- **Practical Approach.** 0 to 40 points.
  - **0 to 20 points.** The practical approach presented in such a way that the target audience acquires practical knowledge in their own fields of action and is easy to implement within the attendee's field of action will be assessed.
  - **0 to 20 points.** The degree of adequacy and appropriateness of the practical aspects presented in the proposal will be assessed, such as:
    - Techniques for recognition and defence against threats.
    - The exposure and/or discovery of new cybersecurity vulnerabilities, whether our own or those of third parties.
    - Presentation of new tools or systems developed in cybersecurity, whether developed in-house or by third parties.
    - Public distribution of the tools presented.
    - New cybersecurity defence systems.
    - New lines of cybersecurity research.

- **Demonstration.** 0 to 20 points.
  It will be appreciated if the workshop includes demonstrations, case studies, examples of studies, laboratories.

- **Resources.** Points awarded: 0 to 10 points.
  The inclusion and adaptation of means and material resources such as virtual machines, tool repository, or any other downloadable resource that allows the workshop to be reproduced offline by the attendee will be valued.

6.2. LEGISLATION, REGULATORY FRAMEWORK AND POLICY MAKERS

- **Topic.** 0 to 25 points.
  - **0 to 10 points.** The proposed topic is included in the list of topics that are presumed to be of interest, providing an innovative approach to it.
  - **0 to 15 points.** It will be assessed whether the proposed theme offers an in-depth treatment of any of the aspects identified within the proposed themes.

- **Expository Clarity.** 0 to 5 points.
  The appropriateness of the structure and outline of the presentation will be assessed, as well as the suitability of the presentation for the target audience and the subject matter presented.

- **Practical Approach.** 0 to 30 points.

The practical approach presented in such a way that the target audience acquires practical knowledge in their own fields of action and is easy to implement within the attendee's field of action will be assessed.

- **Educational Value.** 0 to 20 points.
  It shall be assessed whether the workshop's approach and didactic focus guarantees its success and whether the knowledge to be transmitted is useful and instructive.

- **Testimonial Value.** 0 to 10 points.
  It shall be assessed whether the subject matter is based on the speaker's personal experiences or evidence of appropriate success stories.

- **Resources.** Points awarded: 0 to 10 points.
  The inclusion and suitability of material or conceptual means and resources to support the exhibition in order to facilitate its comprehension will be assessed.

7. PROCEDURE FOR THE SELECTION OF PROPOSALS

The selection of the proposals submitted to this Call for Papers will be carried out by a jury made up of staff from the University of León, INCIBE and the OAS. The decision of this jury will be final.

The assessment process will be as follows:

- It will be verified that the topic is related to **cybersecurity and** is one of the **topics of interest** described in this call. Proposals not complying with this requirement will be excluded.
- **Proposals will be assessed** by using the criteria indicated in the previous section. A list will be drawn up for each type of proposal. Proposals will be ranked in order from highest to lowest.

  The Ranking of selected and reserve proposals will be drawn up as long as those proposals exceed the threshold of **60 points**.

  In the event of a tie:

  - In both categories, the jury will give priority in the ranking to the proposal that scores highest on the practical approach criterion.

- **Publicising the results**

  - Notification of the selection of the Call for Papers will be made via the same e-mail address given in the application form.
  - A list will be published for each typology for those proposals that have been selected.
  - A list will be published with the proposals that are in reserve for each modality, provided that the proposals exceed the threshold of **60 points**.

APPLICABLE LAW AND JURISDICTION

These terms are guided by Spanish law. Any conflict arising from the application or interpretation of these terms will be submitted to the courts and tribunals of the city of León,

with the express waiver of the parties to their own jurisdiction, if different. The decisions taken by Judges regarding activities are binding from the moment they are made public and are not subject to appeal and will be decided according to the sole criterion of the organisation of the event, which must comply with the provisions of the general and specific terms.

CONFIDENTIALITY

INCIBE guarantees the confidentiality and secrecy of any data it may learn in connection with the call, especially personal and technical data, which may not be copied or used for any purpose other than that stated in the call.

Any information, with particular attention to issues related to technology, products, procedures, processes or know-how of participants in the call shall be considered as confidential information.

Information which is disclosed by applicants, which is required to be disclosed in accordance with these rules, the contract, the law, a court decision or an act of competent authority, or which must be made public in accordance with this call, is excluded from the category of confidential information.

The duration of the confidentiality will be indefinite as long as it remains confidential, and will remain in force after the end of the event, without prejudice to INCIBE's obligation to ensure that the grants are adequately publicised.

INTELLECTUAL PROPERTY PROTECTION

The candidate and/or the speaker knows and accepts that the seminar/workshop subject to the contract may be disseminated, in whole or in part, by INCIBE both in written media on physical media and on the Internet through the portal https://www.incibe.es/summer-bootcamp as well as the social networks of the event.

The speaker will retain the legal ownership and copyright of the content presented or developed during his/her participation in the Cybersecurity Summer BootCamp.

The speaker/s authorise INCIBE to use, communicate and disseminate free of charge and without time or territorial restrictions, any image, sound, or any other content presented, solely for the purpose of including them in dissemination, publicity and advertising activities of the activity and/or of the event or future INCIBE events.

The speaker gives permission for his or her speech to be recorded and broadcast to the students of the Cybersecurity Summer BootCamp. Please note that the communication, dissemination and/or reproduction of your intervention will be carried out in any channel, whether traditional or online.

TRANSFER OF IMAGE RIGHTS

The selected speakers expressly, exclusively and free of charge grant INCIBE the use, free of charge, of any image that might be captured of them during participation in the event, without any limitation or restriction whatsoever. In particular, speakers irrevocably and freely authorise INCIBE to use their image and/or names in any notice or communication sent using any written or audiovisual means, worldwide and during the legally permitted time,

and they promise to subscribe to those documents or authorisation which might be necessary to use said image and/or name.

INCIBE will act in strict compliance with its obligations under Organic Law 1/1982 on the Civil Protection of the Right to Honour, to Personal and Family Privacy and to one's own image

PERSONAL DATA PROTECTION

The speakers are obliged to comply with the current regulations on personal data protection.

Legal Basis	GDPR: 6.1.a) Processing where the data subject has given consent for one or more specific purposes. Law 1/1982 on civil protection of the right to honour, personal and family privacy and self-image. Law 34/2002 of 11 July 2002 on information society services and electronic commerce. Law 3/2018, on the Protection of Personal Data and Guarantee of Digital Rights (LOPGDD). Article 19 LOPGDD. Processing of contact data of individual entrepreneurs and liberal professionals. **1.** In the absence of evidence to the contrary, the processing of contact data and, where applicable, data relating to the function or position held by natural persons providing services in a legal person shall be presumed to be covered by Article 6(1)(f) of Regulation (EU) 2016/679 provided that the following requirements are met: a) The processing relates solely to the data necessary for their professional location. b) The purpose of the processing is solely to maintain relations of any kind with the legal person in which the data subject provides their services. **2.** The same presumption shall apply to the processing of data relating to sole proprietors and liberal professionals, where it relates to them solely in that capacity and is not processed for the purpose of establishing a relationship with them as natural persons. **3.** The data controllers or processors referred to in Article 77.1 of this Organic Law may also process the data mentioned in the two preceding paragraphs when this arises from a legal obligation or is necessary for the exercise of their powers.
Purposes of Processing	Registration and control of participation in the event, as well as to comply with the rest of the obligations applicable to INCIBE. Sending of notices related to the event. Managing activity and participation Recording and transmission of the lecture
Collective	Participants in the CFP to be eligible to be a speaker at the event.
Data Categories	• Details of the participants (name, surname, e-mail address and contact telephone number) for the purposes of their participation in the call, resolution of doubts and management of their participation, in the case of being selected. • Image and voice of the speaker, if selected.

Category Recipients	Service contractor for the event. Exceptionally, communications to public authorities and bodies in order to comply with a legal obligation required of INCIBE.
International Transfer	N/A
Time limit for deletion	They shall be kept for the time necessary to fulfil the purpose for which they were collected and to determine the possible responsibilities that may arise from this purpose and from the processing of the data and for sending information of interest to the recipients, until the recipients unsubscribe. The mandatory minimum data collected in the registration form shall be kept for one year after the end of the event.
Security measures	The security measures implemented correspond to those provided for in the National Security Scheme.
Rights	Access, Rectification, Deletion, Limitation, Portability and Opposition. You can exercise your rights in the mailbox dpd@incibe.es For any complaint you can go to the Spanish Data Protection Agency
Responsible Entity	S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE), bearing CIF A24530735.
Data Protection Officer	dpd@incibe.es
Additional information	Additional and detailed information on Data Protection can be found on our website at https://www.incibe.es/registro-actividad/ https://www.incibe.es/proteccion-datos-personales https://www.incibe.es/aviso-legal Information about cookies can be found on the website https://www.incibe.es/politica-cookies

INVOICING

The processing of the fee collection will be managed by the University of León as a partner of the training programme within the framework of the agreement *"Convenio marco entre la Universidad de León y la Sociedad Mercantil Estatal Instituto Nacional de Ciberseguridad para la colaboración conjunta en materia de ciberseguridad" (Framework agreement between the University of León and the Sociedad Mercantil Estatal Instituto Nacional de Ciberseguridad for joint collaboration in cybersecurity matters)*.

The remuneration set out in these terms and conditions is €250.00 per hour excluding taxes and deductions.

CONTACT

For any questions about the process, please contact the Cybersecurity Summer BootCamp organisation at contacto_SummerBC@incibe.es

Leon, 4 May 2022