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

Acta Valoración CFP - FCS

Cybersecurity Summer BootCamp 2022

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD

8 de junio de 2022

ACTA DE CALIFICACIÓN PARA LA CONTRATACIÓN DE PONENTES CALL FOR PAPERS CYBERSECURITY SUMMER BOOTCAMP, EDICIÓN 2022.

Siendo las 17:00 horas del miércoles 8 de junio de 2022, queda constituido el Jurado regulado en el apartado 7 de las Bases de participación, para la contratación de Ponentes CFP, del programa de capacitación *Cybersecurity Summer BootCamp*, para proceder a la calificación y propuesta de contratación para la impartición de talleres. El jurado formado por personal de INCIBE, Universidad de León y la OEA, cuya decisión será inapelable, queda constituido del siguiente modo:

- Secretario: INCIBE
- Jurado: Universidad de León
- Jurado: OEA

ANTECEDENTES

Primero.- El día 4 de mayo de 2022, se publicaron las Bases de participación CALL FOR PAPERS, para regular la participación y contratación de ponentes en la próxima edición del programa de capacitación *Cybersecurity Summer BootCamp*, organizado por el S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE), junto con la Organización de los Estados Americanos (OEA), entre el 5 y el 15 de julio de 2022.

Segundo.- El 1 de junio de 2022 a las 23: 59 (CET), se cierra el plazo para la entrega de propuestas.

Tercero.- Durante el periodo de recepción se reciben en el buzón contacto_SummerBC@incibe.es, por orden de recepción las siguientes:

- 01_06/05/2022, LMR_ DFIR en Windows.
- 02_09/05/2022, DEM_ Introducción a la Deepweb.
- 03_16/05/2022, JLVN_ VoIP: Hacking y fraude telefónico.
- 04_16/05/2022, CCA_ Descripción y monitorización de grupos de ransomware en darknets.
- 05_16/05/2022, CS_ Inteligencia de fuentes abiertas (OSINT) enfocadas en la investigación policial.
- 06_17/05/2022, MOS_ Ciberterrorismo, captación, radicalización y acciones, (desde lo virtual a lo presencial a unos clicks).
- 07_20/05/2022, RGB_ EL Agente Encubierto Digital. La automatización y profesionalización de la investigación Penal en entornos digitales.
- 08_20/05/2022, RJR_ Extracción de indicadores de compromiso de malware en forense de memoria.
- 09_23/05/2022, SR_ OSINT: herramientas, técnicas de búsqueda y análisis de información.
- 10_23/05/2022, DVC_ Técnicas de Web Scraping con Python.

- 11_24/05/2022, JRRR_ Identificación, recolección y preservación de Evidencias Digitales en entornos Windows, Linux y MacOs.
- 12_24/05/2022, EOR_ Taller Teórico-práctico para el análisis e investigación del Cibercrimen en las Tecnologías Emergentes.
- 13_24/05/2022, ESJ – GC_ Análisis técnico en investigación de accesos indebidos a sistemas de información críticos – caso real de estudio.
- 14_25/05/2022, GDP_ Taller de recolección de evidencia digital.
- 15_26/05/2022, WAGR_ Investigación de organizaciones dedicadas al hurto a celulares.
- 16_25/05/2022, SDA_ Sistema de Geolocalización celular.
- 17_27/05/2022, JDPA_ Caza de amenazas: Análisis de familias ransomware con leaks en hidden sites de TOR.
- 18_28/05/2022, ACO_ Técnicas OSINT e ingeniería social para la obtención de información a través de la emulación de geolocalizaciones.
- 19_28/05/2022, SDA_ IMSI Catcher y Directional Finder.
- 20_30/05/2022, DODL_ Blockchain: Construcción de una Aplicación Distribuida (DApp) desde cero - Blockchain: Building a Distributed App (DApp) from zero.
- 21_30/05/2022, DODL_ Descubriendo cibercrimenes utilizando OSINT y analítica de datos – Discovering cybercrimes using OSINT and Data Analytics.
- 22_30/05/2022, MAMA_ Python y técnicas de Scrapping para Investigaciones basadas en datos de fuentes abiertas (OSINT).
- 23_30/05/2022, SDA_ Sistema de geolocalización celular.
- 24_31/05/2022, MCM_ Técnicas de ciber engaño y contrainteligencia.
- 25_31/05/2022, CLM_ Aprendiendo de cero con Threat Hunting Policial.
- 26_31/05/2022, SGC_ Métodos para identificar y geolocalizar cibercriminales.
- 27_01/06/2022, FJRM_ Mas allá del Internet Convencional. Introducción a la DeepWeb, DarkWeb y Darknets.
- 28_01/06/2022, JECS_ Digital Forensics in the cloud Nuevos Retos en análisis forense.
- 29_01/06/2022, HRSS_ Criptomomendas y detección de fraude bancario y online.
- 30_01/06/2022, FJRM_ Investigación criminal en entornos tecnológicos: acciones orientadas al reconocimiento e identificación de infraestructuras vinculadas a actividad delictiva en Surface Web y Deep Web y análisis de la superficie de ataque de las entidades objetivo.
- 31_01/06/2022, JECV_ Investigación de aplicaciones Loan.
- 32_01/06/2022, APV_ Aproximación técnico-legal a blockchain.
- 33_01/06/2022, MG – AJM_ Introducción a la blockchain y el ecosistema de los criptoactivos.
- 34_01/06/2022, MG – AJM_ Análisis Forense de Drones
- 35_01/06/2022, MG – AJM_ Trazabilidad, incautación y recupero de criptoactivos.
- 36_01/06/2022, HA - MG – AJM_ Workshop intensivo sobre investigación criminal de casos vinculados con criptoactivos.

Cuarto.- Candidatos. Las características de candidatos y propuestas son las reguladas en el apartado segundo de las bases y se reflejan en los apartados siguientes**.**

Podrá presentar una propuesta cualquier persona física o jurídica (el candidato) si bien el ponente propuesto deberá ser persona física mayor de 18 años. Podrá presentarse como

ponente personal laboral de INCIBE o personas que se encuentren cursando una beca en INCIBE.

Se seleccionarán un mínimo de propuestas que garanticen el correcto desarrollo para cada uno de los cuatro programas formativos del *Cybersecurity Summer BootCamp* y sus variantes en versión inglesa, de las cuales serán:

- Programa dirigido a miembros de Fuerzas y Cuerpos de Seguridad que trabajen en unidades operativas relacionadas con la ciberseguridad (FCS).
- Programa dirigido a personal técnico que trabaje en Centros de Respuesta a Incidentes de Seguridad (CSIRTs).
- Programa dirigido a personal en activo perteneciente a las carreras judicial o fiscal, abogacía del Estado, funcionario de la Administración de Justicia (Ministerio Fiscal, jueces y fiscales).
- Programa dirigido a personal de organismos reguladores o legislativos que trabajen en áreas relacionadas con los aspectos jurídicos y normativos de la ciberseguridad (*Policy Makers*).

Ante la posibilidad de que puedan surgir necesidades adicionales de ponencias, talleres o charlas en la agenda del programa de capacitación. Para atender este supuesto, se elaborará:

a) **Clasificación de propuestas seleccionadas:** Esta lista corresponderá con las mejores propuestas teniendo en cuenta los programas académicos de las tipologías indicados anteriormente y serán seleccionadas por ser las mejores propuestas aplicados los criterios de valoración previstas en las presentes bases.

b) **Clasificación de propuestas en reserva:** Para la selección se seguirá la clasificación de las propuestas presentadas de mayor a menor puntuación por cada tipología empezando a contar a partir de las propuestas no seleccionadas en la clasificación anterior.

Quinto.- Propuestas.

Todos los talleres propuestos deberán girar en torno a la ciberseguridad:

- Duración: La duración mínima de cada taller se establece en función de la temática en el apartado La duración mínima de cada taller se establece en función de la temática en el apartado 4.2 TEMÁTICAS DE INTERÉS que figura en las bases.
- Público objetivo: Perfiles técnicos y/o expertos profesionales en Ciberseguridad.
- Precio: 250,00€ por hora impuestos y retenciones no incluidos.
- Tipos de formatos propuestos:
  - Clases magistrales de carácter técnico.
  - Demostraciones de tecnologías o técnicas en directo o pregrabadas

Sexto.- El proceso de valoración es el regulado en las bases:

1. Se comprueba que la temática gira en torno a la ciberseguridad y es de una de las temáticas de interés descritas en la presente convocatoria. Las propuestas que no cumplan este requisito son excluidas.
2. Se valoran las propuestas aplicando los criterios indicados en el apartado 6 de las bases. Cada propuesta se valorada con una puntuación de 0 a 100, en base a los criterios siguientes:

- Temática. De 0 a 20 puntos.
- Claridad expositiva. De 0 a 10 puntos.
- Enfoque práctico. De 0 a 40 puntos.
  - Enfoque práctico. De 0 a 20 puntos.
  - Grado de adecuación e idoneidad. De 0 a 20 puntos.
- Demostración. De 0 a 20 puntos.
- Recursos. Puntos asignados: de 0 a 10 puntos.

3. Se elabora una lista para cada tipología de propuesta. La clasificación de las propuestas será ordenada de mayor a menor.
4. Se elabora la Clasificación de propuestas seleccionadas y de reserva siempre y cuando aquellas propuestas superen el umbral de **60 puntos**.

ACUERDOS

PRIMERO.- Que finalizado el plazo de presentación de propuestas, han presentado toda la documentación exigida siguiendo los requisitos establecidos en las Bases de participación CALL FOR PAPERS, parar regular la participación y contratación de ponentes, del programa de capacitación Cybersecurity Summer BootCamp 2022, FCS:

- 01_LMR
- 02_DEM
- 03_JLVN
- 04_CCA
- 05_CS
- 06_MOS
- 07_RGB
- 08_RJR
- 09_SR
- 10_DVC
- 11_JRRR
- 12_EOR
- 13_ESJ – GC
- 14_GDP
- 15_WAGR
- 16_ SDA
- 17_JDPA
- 18_ACO
- 19_SDA
- 20_DODL
- 21_DODL_
- 22_MAMA
- 23_SDA
- 24_MCM
- 25_CLM
- 26_SGC
- 27_FJRM
- 28_JECS
- 29_HRSS

- 30_FJRM
- 31_JECV
- 32_APV
- 33_MG – AJM
- 34_MG – AJM
- 35_MG – AJM
- 36_HA - MG – AJM

SEGUNDO.- Según establece el apartado 7 del procedimiento de selección la decisión de este jurado será inapelable. La valoración y clasificación de propuestas en orden de mayor a menor, según los criterios establecidos en las Bases:

ID	Puntuación	Posición ranking
01_LMR	93,0	1
35_MG – AJM	91	2
36_HA - MG – AJM	91	3
08_RJR	90,0	4
09_SR	88,5	5
18_ACO	86,1	6
30_FJRM	85	7
04_CCA	84,5	8
03_JLVN	84,0	9
22_MAMA	82,9	10
02_DEM	82,5	11
07_RGB	82,0	12
27_FJRM	81,5	13
28_JECS	81,3	14
05_CS	81,0	15
21_DODL_	79,8	16
29_HRSS	79,1	17
11_JRRR	79,0	18
17_JDPA	78,3	19
10_DVC	78,0	20
33_MG – AJM	70,8	21
20_DODL	70,5	22
12_EOR	68,5	23
26_SGC	68,1	24
34_MG – AJM	66,4	25
25_CLM	66,1	26
32_APV	64,6	27
16_SDA	61,5	28
31_JECV	60	RESERVA
19_SDA	60	RESERVA
13_ESJ – GC	60	RESERVA

24_MCM	60	RESERVA
14_GDP	60	RESERVA
23_SDA	60	RESERVA
06_MOS	60	RESERVA
15_WAGR	60	RESERVA

TERCERO.- Notificación mediante correo electrónico a los aceptados en el plazo y forma establecida de la selección del Call for Papers, esta se hará a través de la misma dirección de correo electrónico que conste en el modelo de solicitud.

CUARTO.- Que se publique en anuncio público las propuestas seleccionadas en la web https://www.incibe.es/summer-bootcamp , según establecen las bases, en su apartado tercero.

QUINTO.- Finalmente, siendo las 17:00 horas se dio por terminada la reunión.

INCIBE