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 - CSIRTs

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_19/05/2022, OEL_ (CTI) Análisis y Automatización.
- 03_ 20/05/2022, RJR_ Extracción de indicadores de compromiso de malware en forense de memoria.
- 04_21/05/2022, PCR_ Matemáticas 101: aplicación práctica de empleo de MBA's (Expresiones mixtas aritméticas y booleanas) con OC's (Constantes Opacas) para la ofuscación de código para evadir Reglas/AV's/EDR's/XDR's y su posible detección.
- 05_22/05/2022, PGP_ Pentesting Training: Linux Environments & Windows Post-Exploitation.
- 06_23/05/2022, OA_ Análisis de malware, desofuscando payloads ocultos.
- 07_23/05/2022, RJR_Técnicas avanzadas de análisis de aplicaciones dañinas.
- 08_23/05/2022, SR, Smartphone Pentesting.
- 09_23/05/2022, DMC_ Construcción de un dispositivo IoT desechable para Pentesting de redes.
- 10_23/05/2022, DMP_OSINT enfocado a ejercicios de Red Team.

- 11_24/05/2022, GJLC_ Técnicas de Red Team para Evasión de Sistemas de Seguridad y Soluciones Antivirus (EDR, XDR, etc.)
- 12_26/05/2022, AMM_ Análisis de amenazas basadas en stegomalware. Detección y anulación.
- 13_26/05/2022, LFC_ Herramientas de todos los días para un análisis de compromiso inicial.
- 14_26/05/2022, OMPH_ PENTESTING en entornos empresariales Microsoft Windows.
- 15_27/05/2022, JMRV_ Detección de APT´s aplicando minería de datos y sistemas de aprendizaje automático.
- 16_27/05/2022, JDPA_ Anatomía de un ataque web: Hacker de Sombrero Gris.
- 17_28/05/2022, JJCM_ Introducción a los libros de jugadas (Playbooks). Más allá de la continuidad del negocio.
- 18_29/05/2022, CS_ Inteligencia de fuentes abiertas (OSINT) como elemento proactivo en Ciberseguridad.
- 19_30/05/2022, AGB_ Facing a company-wide compromise: lessons learned from ransomware attacks.
- 20_30/05/2022, MAMA_ Seguridad para DevOps y pentesting de APIs y Microservicios.
- 21_30/05/2022, SGV_ Análisis de amenazas industriales en SloMo.
- 22_31/05/2022, JP | FS_ Introducción al Ethical Hacking.
- 23_31/05/2022, OA_ Inteligencia en Ciberseguridad para CERTs/CSIRTs.
- 24_01/06/2022, MD_ Automatización en el procesamiento de incidentes utilizando IntelMQ.
- 25_01/06/2022, MD_ Búsqueda de vulnerabilidades a gran escala.
- 26_01/06/2022, PSEL_ Exploits, Malware & Frida.
- 27_01/06/2022, GAC_ Gestión de incidentes de ciberseguridad: se juega como se entrena.
- 28_01/06/2022, GAC_ Aspectos legales y cooperación para técnicos de CSIRT.
- 29_01/06/2022, GHAP_ Auditoría estática y dinámica de una app infectada con Pegasus.
- 30_01/06/2022, NJDM_ Análisis Técnico de Malware para la Respuesta a Incidentes Informáticos en Infraestructuras Críticas.
- 31_01/06/2022, EPM_ Cómo mejorar la estrategia de ciberseguridad.
- 32_01/06/2022, IPNM_ Metodología de investigación sobre ciberamenazas, actores y emulación de sus TTPs.
- 33_01/06/2022, APV_ Coordinación técnico-legal en un CSIRT y su importancia en la respuesta ante incidentes.
- 34_01/06/2022, ES_ Cyber Operations - Análisis, detección y respuesta de Malware.
- 35_01/06/2022, JSNA_ Creando Ciberseguridad defensiva: más allá del SIEM.
- 36_01/06/2022, EA_ CISA Presents "Benefits of becoming a CNA".
- 37_01/06/2022, MD_ Proyecto colaborativo de capacitación en CSIRTs utilizando CTFs.
- 38_01/06/2022, HRSS_ Ciencia de datos aplicada a la detección de ciberincidentes.
- 39_01/06/2022, HJA_ La regulación Internacional de la investigación de los crímenes cibernéticos – Temas actuales.
- 40_01/06/2022, JFF_ Zero Trust SDN - Defensa del Datacenter.

- 41_01/06/2022, DETD_ Clasificación de tráfico en red de Internet Industrial de las Cosas (IIoT) utilizando redes neuronales convolucionales 1D.

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, CSIRTS:

- 01_LMR
- 02_OEL
- 03_ RJR
- 04_PCR
- 05_PGP
- 06_OA
- 07_RJR
- 08_SR
- 09_DMC
- 10_DMP
- 11_GJLC
- 12_ AMM
- 13_LFC
- 14_ OMPH
- 15_JMRV
- 16_JDPA
- 17_JJCM
- 18_CS
- 19_AGB
- 20_MAMA
- 21_SGV
- 22_JP | FS

- 23_ OA
- 24_MD
- 25_MD
- 26_PSEL
- 27_GAC
- 28_ GAC
- 29_GHAP
- 30_NJDM
- 31_EPM
- 32_IPNM
- 33_APV
- 34_ES
- 35_JSNA
- 36_EA
- 37_MD
- 38_ HRSS
- 39_HJA
- 40_JFF
- 41_DETD

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 en el ranking
03_ RJR	94	1
24_MD	91,5	2
34_ES	91,5	3
07_RJR	90,5	4
12_AMM	89	5
19_AGB	89	6
11_GJLC	89	7
32_IPNM	87,5	8
05_PGP	85,5	9
36_EA	85	10
29_GHAP	84	11
38_HRSS	83,5	12
01_LMR	81,5	13
14_OMPH	81,5	14
21_SGV	81,5	15
15_JMRV	81	16
25_MD	81	17
26_PSEL	81	18
02_OEL	79,5	19
10_DMP	79	20
20_MAMA	78,5	21

08_SR	78	22
13_LFC	78	23
18_CS	78	24
16_JDPA	76	25
35_JSNA	75	26
06_OA	74,5	27
40_JFF	74	28
37_MD	73,5	29
04_PCR	73	30
33_APV	73	31
30_NJDM	72	32
17_JJCM	70	33
09_DMC	68	34
27_GAC	68	35
39_HJA	68	36
22_JP | FS	65,5	37
41_DETD	65,5	38
31_EPM	60	RESERVA
28_GAC	60	RESERVA
23_OA	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