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

Bases de participación Cybersecurity Summer BootCamp 2022

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

ÍNDICE

ÍNDICE DE FIGURAS

No se encuentran elementos de tabla de ilustraciones.

ÍNDICE DE TABLAS

1. OBJETO

El objeto de las presentes bases es el de regular la participación y contratación de **ponentes**, en la próxima edición del evento 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) y en colaboración con la Universidad de León, entre el 5 y el 15 de julio de 2022.

2. CANDIDATOS

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.

Para poder participar, el candidato deberá cumplir con los requisitos establecidos en las presentes bases y enviar en tiempo y en forma su propuesta de participación siguiendo las instrucciones que vienen recogidas a continuación.

Por la presente convocatoria, se seleccionarán el 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*).

Es posible que puedan surgir necesidades adicionales de talleres en la agenda del evento. 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.

3. FECHAS DEL PROCESO

FECHAS (2022)	ACCIÓN
04 de mayo	Apertura del *call for papers*
23 de mayo	Cierre del *call for papers*
23 de mayo	Inicio de la valoración de los *call for papers* recibidos
30 de mayo	Fin de valoración
31 de mayo	Notificación de los *call for papers* aceptados
1 de junio	Anuncio público de las propuestas seleccionadas en la web https://www.incibe.es/summer-bootcamp

Tabla 1. Fechas del proceso

4. PROPUESTAS

4.1. TIPOLOGÍAS DE PROPUESTAS

Todos los talleres propuestos deberán girar en torno a **la ciberseguridad[1]:**

- **Duración**: La duración mínima de cada taller se establece en función de la temática en el apartado TEMÁTICAS DE INTERÉS
- **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.

4.2. TEMÁTICAS DE INTERÉS

A continuación se muestra un listado meramente indicativo, con carácter no exhaustivo, sobre temáticas de interés para el programa del Cybersecurity Summer BootCamp:

- **Investigación policial (FCS):**

Temática	Duración estimada
Investigación criminal en entornos tecnológicos	10 horas
Digital Forensics and Incident Response (DFIR)	7,5 horas
Digital Forensics in the cloud	2,5 horas
Inteligencia de fuentes abiertas (OSINT)	5 horas
Inteligencia en investigaciones policiales	2,5 horas
Criptomonedas y fraude bancario	2,5 horas
Blockchain	2,5 horas
Introducción a la Deepweb	2,5 horas
Temario completo	**35 horas**

Tabla 2. Temáticas FCS

- **Operaciones CSIRTs:**

Temática	Duración estimada
Pentesting / Ethical Hacking	7,5 horas

[1] Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan [O.M. 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas]

Análisis forense	7,5 horas
Gestión de Incidentes de ciberseguridad	5 horas
Análisis de amenazas (malware)	5 horas
Inteligencia en Ciberseguridad para CERTs/CSIRTs	5 horas
Avisos de seguridad	2,5 hora
Aspectos legales y cooperación	2,5 horas
Temario completo	**35 horas**

Tabla 3. Temáticas CSIRTs

- **Legislación y marco normativo:**

Temática	Duración estimada
Cadena de custodia y evidencia electrónica: ▪ Problemática práctica de la prueba digital. Hallazgos casuales. Derechos y Libertades en un mundo digital. Nuevos retos del proceso penal. ▪ Problemática práctica de las diligencias de investigación tecnológica. Ej. Seguimiento de monedas virtuales.	7 horas
Investigación tecnológica y jurisprudencia: ▪ La investigación en fuentes abiertas. La innovación tecnológica como herramienta de las FFCCS ▪ Fundamentos prácticos de la investigación tecnológica. ▪ La investigación tecnológica en la Jurisprudencia del Tribunal Supremo.	10 horas
Regulación privacidad, protección de datos y derecho al honor: ▪ Los contenidos ilícitos en la red: especial referencia a los delitos de odio. ▪ La retirada de contenidos en Internet: la colaboración con los operadores privados.	5 horas
Temario completo	**22 horas**

Tabla 4. Temáticas Legislación y Marco normativo

- **Formuladores de políticas:**

Temática	Duración estimada
Normativa:	5 horas

▪ Impacto de la regulación de la privacidad y protección de datos. ▪ La retirada de contenidos en Internet: la colaboración con los operadores privados.	
Creación de Estrategia de ciberseguridad: ▪ La importancia de la ordenación institucional de la Ciberseguridad: Gobernanza de la Ciberseguridad en España y LATAM. ▪ Implementación y seguimiento de Estrategias de ciberseguridad.	7 horas
Opciones de sostenibilidad y creación de fondos en ciberseguridad.	2,5 horas
El rol de la ciberdiplomacia en la gestión de crisis cibernéticas.	1 hora
Rol del CSIRT - sistema de CSIRTs internacional.	1 hora
Derecho internacional aplicable al ciberespacio. Novedades regulatorias.	3,5 horas
Aspectos legales y cooperación.	2 horas
Temario completo	**22 horas**

Tabla 5. Temario Formuladores de políticas

5. PROCEDIMIENTO DE PRESENTACIÓN DE PROPUESTAS

5.1. PLAZO

El Plazo de recepción de propuestas para participar en el Cybersecurity Summer BootCamp 2022 finaliza a las **23:59h (CET) del 23 de mayo de 2022**.

5.2. ENVÍO DE PROPUESTAS

Para el envío de la propuesta se deberá de presentar el modelo de documento disponible en la sección *call for papers* del portal web del Cybersecurity Summer BootCamp y completar correctamente los campos requeridos.

Una vez cumplimentado el formulario, se deberá remitir a la dirección contacto_SummerBC@incibe.es dentro del plazo establecido, indicando, en el asunto del mismo, la referencia: «**CFP Cybersecurity Summer BootCamp 2022**».

Si se considera necesario por parte del candidato, podrá adjuntarse información adicional complementaria sobre la propuesta.

6. VALORACIÓN DE PROPUESTAS

Cada propuesta será valorada con una puntuación de 0 a 100, en base a los criterios siguientes:

*No se aceptarán propuestas cuyo fin principal sea publicitar soluciones con fines comerciales.

6.1. TALLERES PARA FCSE Y CSIRTS

- **Temática.** De 0 a 20 puntos.

  La temática propuesta se encuentra dentro del listado de temas que se presumen de interés aportando un enfoque innovador sobre el mismo.

- **Claridad Expositiva**. De 0 a 10 puntos.
  Se valorará la idoneidad de la estructura y el esquema de la presentación es adecuado para el público objetivo y la temática presentada.

- **Enfoque práctico.** De 0 a 40 puntos.
  - **De 0 - 20 puntos.** Se valorará el enfoque práctico presentado de modo que el público objetivo adquiera conocimiento de carácter práctico en sus propios ámbitos de actuación y tenga una implantación sencilla dentro del ámbito de actuación del asistente.
  - **De 0 - 20 puntos.** Se valorará el grado de adecuación e idoneidad de los aspectos prácticos presentados en la propuesta, tales como:
    - Técnicas para el reconocimiento y defensa contra amenazas.
    - La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros.
    - Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad, bien si son desarrollos propios o de terceros.
    - Distribución pública de las herramientas presentadas.
    - Nuevos sistemas de defensa de ciberseguridad.
    - Nuevas líneas de investigación de ciberseguridad.

- **Demostración.** De 0 a 20 puntos.
  Se valorará si el taller incluye demostraciones, casos prácticos, ejemplos de estudios, laboratorios.

- **Recursos**. Puntos asignados: de 0 a 10 puntos.
  Se valorará la inclusión y adecuación de medios y recursos materiales tales como máquinas virtuales, repositorio de herramientas, o cualquier otro recurso descargable que permita reproducir el taller por parte del asistente de manera offline.

6.2. LEGISLACIÓN, MARCO NORMATIVO Y *POLICY MAKERS*

- **Temática.** De 0 a 25 puntos.
  - **De 0 - 10 puntos.** La temática propuesta se encuentra dentro del listado de temas que se presumen de interés aportando un enfoque innovador sobre el mismo.
  - **De 0 - 15 puntos.** Se valorará si la temática propuesta ofrece un tratamiento profundo de alguno de los aspectos identificados dentro de las temáticas propuestas.

- **Claridad Expositiva.** De 0 a 5 puntos.
  Se valorará la idoneidad de la estructura y el esquema de la presentación es adecuado para el público objetivo y la temática presentada.

- **Enfoque práctico.** De 0 a 30 puntos.

  Se valorará el enfoque práctico presentado de modo que el público objetivo adquiera conocimiento de carácter práctico en sus propios ámbitos de actuación y tenga una implantación sencilla dentro del ámbito de actuación del asistente.

- **Valor didáctico.** De 0 a 20 puntos.
  Se valorará si el planteamiento que hace del taller y su enfoque didáctico garantiza el éxito del mismo y el conocimiento a trasmitir es útil e instructivo.

- **Valor testimonial.** De 0 a 10 puntos.
  Se valorará si la temática cuenta con experiencias personales del ponente o evidencia casos de éxito adecuadas.

- **Recursos**. Puntos asignados: de 0 a 10 puntos.
  Se valorará la inclusión y adecuación de medios y recursos materiales o conceptuales como apoyo a la exposición con la finalidad de facilitar su comprensión.

7. PROCEDIMIENTO DE SELECCIÓN DE PROPUESTAS

La selección de las propuestas presentadas a este *Call for Papers* se llevará a cabo por un jurado formado por personal de la Universidad de León, INCIBE y la OEA. La decisión de este jurado será inapelable.

El proceso de valoración será el siguiente:

- Se comprobará 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 serán excluidas.
- **Se valorarán las propuestas** aplicando los criterios indicados en el apartado anterior. Se elaborará una lista para cada tipología de propuesta. La clasificación de las propuestas será ordenada de mayor a menor.

  Se elaborará la Clasificación de propuestas seleccionadas y de reserva siempre y cuando aquellas propuestas superen el umbral de **60 puntos**.

  En caso de empate:

  - En ambas categorías, el jurado dará prioridad en la clasificación a la propuesta que tenga mejor puntuación en el criterio del enfoque práctico.
- **Publicidad de los resultados**

  - La notificación de la selección del *Call for Papers* se hará a través de la misma dirección de correo electrónico que conste en el modelo de solicitud.
  - Se publicará un listado, para cada tipología para aquellas propuestas que hayan sido seleccionadas.

- Se publicará un listado con las propuestas que se encuentren en reserva para cada modalidad, siempre que las propuestas superen el umbral de **60 puntos**.

LEGISLACION Y FUERO APLICABLE

Las presentes Bases se rigen por la legislación española. Cualquier conflicto derivado de la aplicación o interpretación de las presentes Bases se someterá a los juzgados y tribunales de la ciudad de León, con renuncia expresa de las partes a su fuero propio si éste fuera otro. Las decisiones adoptadas por los Jurados respecto de las actividades tienen carácter firme desde que se hagan públicas y no serán recurribles y se decidirán según el criterio único de la Organización del evento que deberá ajustarse a lo previstos en las bases generales y particulares.

CONFIDENCIALIDAD

INCIBE garantiza la confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión de la convocatoria, especialmente los de carácter personal y de carácter técnico que no podrá copiar o utilizar con fin distinto al que figura en la convocatoria.

Se considerará información confidencial cualquier información, con especial atención a los temas relacionados con la tecnología, productos, procedimientos, procesos o know-how de los participantes en la convocatoria.

Se excluye de la categoría de información confidencial toda aquella información que sea divulgada por los solicitantes, aquella que haya de ser revelada de acuerdo con las presentes bases, el contratos, las leyes o con una resolución judicial o acto de autoridad competente o que deba hacerse pública conforme a la presente convocatoria.

La duración de la confidencialidad será indefinida mientras la misma ostente tal carácter, manteniéndose en vigor con posterioridad a la finalización del evento, sin perjuicio de la obligación de INCIBE de garantizar una adecuada publicidad de las ayudas.

PROTECCIÓN DE PROPIEDAD INTELECTUAL

El candidato y/o el ponente conocen y aceptan que el seminario/taller objeto del contrato podrá ser divulgada, en todo o en parte, por INCIBE tanto en medios de comunicación escritos en soporte físico, como en Internet a través del portal https://www.incibe.es/summer-bootcamp así como las redes sociales del evento.

El ponente mantendrá la titularidad y los derechos de autor que legalmente le correspondan sobre los contenidos presentados o desarrollados durante su participación en el Cybersecurity Summer BootCamp.

El ponente/s, autoriza/n a INCIBE a que utilice, comunique y difunda gratuitamente y sin restricciones temporales ni territoriales, cualquier imagen, sonido, o cualquier otro contenido presentado, únicamente con el fin de incluirlos en actividades de difusión, publicidad y propaganda de la actividad y/o del evento o futuros eventos de INCIBE.

El conferenciante da permiso para que su intervención sea grabada y transmitida en diferido a los alumnos del Cybersecurity Summer BootCamp. Nótese que la comunicación, difusión y/o reproducción de su intervención se realizará en cualquier canal ya sea tradicional u online.

CESIÓN DE DERECHOS DE IMAGEN

Los ponentes seleccionados ceden de forma expresa, en exclusiva y de forma gratuita a INCIBE el uso de su imagen personal, que pudiera ser captada durante su participación o asistencia al evento, sin limitación ni restricción de ninguna clase. En particular, los ponentes autorizan de forma irrevocable y gratuita a INCIBE para hacer uso de su imagen y/o sus nombres en cualquier aviso o comunicación que se realice a través de cualquier medio escrito o audiovisual, en todo el mundo y durante todo el tiempo permitido legalmente y se comprometen a suscribir cualesquiera documentos o autorizaciones que pudieren ser necesarios para el uso de dicha imagen y/o nombre.

INCIBE actuará con estricta sujeción a las obligaciones que para ella se deriven de la Ley Orgánica 1/1982 de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen.

PROTECCIÓN DE DATOS PERSONALES

Los ponentes quedan obligados al cumplimiento de la normativa vigente en materia de protección de datos personales.

Base Jurídica	RGPD: 6.1.a) Tratamiento en el que el interesado dio su consentimiento para uno o varios fines específicos. Ley 1/1982 de protección civil del derecho al honor, intimidad personal y familiar y a la propia imagen. Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Ley 3/2018, de Protección de datos personales y garantía de los derechos digitales (LOPGDD). Artículo 19 LOPGDD. Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales. 1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos: a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional. b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios. 2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas. 3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.
Fines del Tratamiento	Registro y control de participación en el evento, así como para cumplir con el resto de obligaciones aplicables a INCIBE.

	Envío de avisos relacionados con el evento. Gestionar la actividad y la participación Grabación y transmisión de la ponencia
Colectivo	Participantes en el CFP para optar a ser ponente del evento.
Categorías de Datos	• Datos del participante (nombre , apellidos,dirección de correo electrónico y teléfono de contacto) a efectos de su participación en la convocatoria, resolución de dudas y gestión de su participación, en el caso de ser seleccionado. • Imagen y voz del ponente, en caso de ser seleccionado.
Categoría Destinatarios	Contratista del servicio para el evento. Excepcionalmente, comunicaciones a autoridades y organismos públicos para el cumplimiento de una obligación legal requerida a INCIBE.
Transferencia Internacional	N/A
Plazo de Supresión	Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos y para el envío de información de interés para los destinatarios, hasta que estos se den de baja. Los datos mínimos obligatorios recogidos en el formulario de inscripción se conservarán durante el año siguiente a la finalización del evento.
Medidas de Seguridad	Las medidas de seguridad implantadas se corresponden con las previstas en el Esquema Nacional de Seguridad.
Derechos	Acceso, Rectificación, Supresión, Limitación, Portabilidad y Oposición. Puede ejercer sus derechos en el buzón dpd@incibe.es Para cualquier reclamación puede acudir a la Agencia Española de Protección de Datos
Entidad Responsable	S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE) con CIF A24530735.
Delegado de Protección de Datos	dpd@incibe.es
Información adicional	Puede consultar la información adicional y detallada sobre Protección de Datos en nuestra página web en: https://www.incibe.es/registro-actividad/ https://www.incibe.es/proteccion-datos-personales https://www.incibe.es/aviso-legal

En relación a las cookies puede obtener la información en la página web: https://www.incibe.es/politica-cookies

FACTURACIÓN

La tramitación del cobro en concepto de honorarios será gestionada por la Universidad de León como colaborador del programa de capacitación en el marco del convenio *"Convenio marco entre la Universidad de León y la Sociedad Mercantil Estatal Instituto Nacional de Ciberseguridad para la colaboración conjunta en materia de ciberseguridad"*.

La remuneración establecida en las presentes bases es de 250,00€ por hora impuestos y retenciones no incluidos.

CONTACTO

Para cualquier duda acerca del proceso, puede ponerse en contacto con la organización de Cybersecurity Summer BootCamp a través del correo contacto_SummerBC@incibe.es

León, 4 de mayo de 2022