

CALL FOR PAPERS

Bases de participación CyberCamp 2019



OBJETO

El objeto de las presentes bases es el de regular la participación y contratación de **ponentes**, en la próxima edición del evento CyberCamp, organizado por el S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (INCIBE), los próximos días 27 al 30 de noviembre de 2019 en el Palacio de Congresos de Valencia.

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** que no sea personal laboral de INCIBE o se encuentre 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 forma su propuesta de participación siguiendo las instrucciones que vienen recogidas a continuación.

Por la presente convocatoria, se seleccionarán un mínimo de **19 propuestas**, para el programa de CyberCamp, de las cuales serán:

- **Entre 6 y 12 ponencias magistrales**
- **Entre 6 y 10 talleres técnicos**
- **Entre 2 y 4 talleres técnicos de iniciación**
- **Entre 2 y 3 charlas inspiracionales y de promoción del talento**
- **Entre 3 y 5 charlas de concienciación**

Es posible que puedan surgir necesidades adicionales de ponencias, talleres o charlas en la agenda del evento. Para atender este supuesto, se elaborará:

- a) **Clasificación de propuestas seleccionadas por tipología.** Esta lista corresponderá a las mejores propuestas teniendo en cuenta los límites indicados anteriormente y puntuadas a través de los criterios de valoración previstos en las presentes bases.
- b) **Clasificación de propuestas en reserva por tipología.** Para la selección se seguirá la clasificación de las propuestas presentadas de mayor a menor puntuación empezando a contar a partir de las propuestas no seleccionadas en la clasificación anterior.

FECHAS DEL PROCESO

| FECHAS | ACCIÓN |
|---|--|
| 19 de septiembre | Apertura del <i>call for papers</i> |
| 9 de octubre | Cierre del <i>call for papers</i> |
| 20 de octubre | Fin de valoración y notificación de las propuestas aceptadas |
| 21 de octubre | Anuncio público de ponencias seleccionadas. |
| Desde el 22 de octubre hasta el 22 de noviembre | Formalización de los contratos |

| FECHAS | ACCIÓN |
|---|---|
| Desde el día 2 diciembre hasta el 16 de diciembre de 2019 | Recepción de facturas que serán abonadas, previa conformidad con la misma, en el plazo máximo de 30 días desde la fecha de recepción en el buzón de contabilidad@incibe.es Están exceptuados de la presentación de factura, las personas físicas que conforme a ley no estén obligadas a ello. |

PROPUESTAS

TIPOLOGÍAS

Todas las propuestas deberán girar en torno a **la ciberseguridad¹** y **podrán ser de los siguientes tipos:**

- **Ponencias magistrales**
 - Duración: 50 minutos.
 - Público objetivo: Público en general interesado por la Ciberseguridad y perfiles técnicos y/o expertos en ciberseguridad.
 - Precio: 750,00 € impuestos y retenciones no incluidos².
 - Recursos disponibles para los asistentes: los asistentes no cuentan con equipamiento informático.
- **Talleres técnicos**
 - Duración: 110 minutos.
 - Público objetivo: Perfiles técnicos y/o expertos en Ciberseguridad.
 - Precio: 1.500,00€ impuestos y retenciones no incluidos².
 - Tipos de formatos propuestos:
 - Clases magistrales de carácter técnico.
 - Demostraciones de tecnologías o técnicas en directo o pregrabadas.
 - Recursos disponibles para los asistentes: los asistentes pueden llevar su equipamiento informático para seguir el taller técnico.
- **Talleres técnicos de iniciación**
 - Duración: 90 minutos.
 - Público objetivo: Perfiles técnicos de iniciación en Ciberseguridad.
 - Precio: 900,00€ impuestos y retenciones no incluidos².
 - Recursos disponibles para los asistentes: los asistentes pueden llevar su equipamiento informático o, en algunos casos, en función de la ubicación del taller la organización los pondrá a su disposición.

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]

² En el caso de que el candidato sea una persona física, a esa cantidad se le debe restar la retención del IRPF en vigor correspondiente. En el caso de persona jurídica a esa cantidad se le debe añadir el IVA.

■ **Charlas inspiracionales y de promoción del talento.**

- Duración: 50 minutos.
- Público objetivo: jóvenes con interés potencial en dedicarse profesionalmente a la ciberseguridad.
- Precio: 750,00 € impuestos y retenciones no incluidos².
- Recursos disponibles para los asistentes: los asistentes no cuentan con equipamiento informático.

■ **Charlas de concienciación**

- Duración: 30 minutos.
- Público objetivo: ciudadanos y familias.
- Precio: 450,00 € impuestos y retenciones no incluidos².
- Recursos disponibles para los asistentes: los asistentes no cuentan con equipamiento informático.

TEMÁTICAS DE INTERÉS

A continuación se muestra un listado meramente indicativo, con carácter no exhaustivo, sobre temáticas de interés para CyberCamp 2019, para cada tipología de propuesta:

■ **Ponencias magistrales y Talleres técnicos:**

- Pentesting, hacking ético, exploiting.
- Gestión de incidentes, análisis forense/anti-forense.
- Threat intelligence, intercambio de información, inteligencia artificial, machine learning aplicado a Ciberseguridad, APT.
- Ingeniería inversa.
- Hardware hacking, seguridad en sistemas embebidos, biometría, IoT.
- Seguridad de las redes anónimas.
- Protección de infraestructuras críticas, SCADA.
- Seguridad en entornos virtualizados, servicios en la nube, big data.
- Desarrollo seguro y análisis de código, devops.
- Seguridad en las comunicaciones.
- Criptografía/criptoanálisis, esteganografía.
- Seguridad en Blockchain.

■ **Talleres técnicos de iniciación**

- Pentesting, hacking ético, exploiting.
- Gestión de incidentes, análisis forense/anti-forense.
- Threat intelligence, intercambio de información, inteligencia artificial, machine learning aplicado a Ciberseguridad, APT.
- Ingeniería inversa.
- Hardware hacking, seguridad en sistemas embebidos, biometría, IoT.
- Seguridad de las redes anónimas.
- Protección de infraestructuras críticas, SCADA.
- Seguridad en entornos virtualizados, servicios en la nube, big data.
- Desarrollo seguro y análisis de código, devops.
- Seguridad en las comunicaciones.
- Criptografía/criptoanálisis, esteganografía.
- Seguridad en Blockchain.

- **Charlas inspiracionales y de promoción del talento:**
 - Inspiración y consejos para convertirse en un profesional de la ciberseguridad. Perfiles y salidas profesionales dentro del sector de ciberseguridad.
 - Empleabilidad y emprendimiento en ciberseguridad. Consejos y herramientas para la búsqueda de empleo y para el autoempleo en ciberseguridad.
 - Valores y competencias del profesional de la ciberseguridad más allá de las habilidades técnicas: ética, liderazgo, comunicación, trabajo en equipo, compartición de conocimiento, visión.
- **Charlas de concienciación:** Estas charlas pueden estar destinadas tanto a padres, madres y educadores como a jóvenes.
 - Uso seguro y responsable de Internet por parte de los menores: riesgos, prevención, iniciativas y tendencias en la materia.
 - Privacidad.
 - Sexting.
 - Grooming.
 - Ciberacoso.
 - Contenidos inapropiados.
 - Comunidades peligrosas.
 - Uso excesivo de las TIC.
 - Mediación parental.
 - Alfabetización mediática.

PROCEDIMIENTO DE PRESENTACIÓN DE PROPUESTAS

PLAZO

El plazo de recepción de propuestas para participar en CyberCamp 2019 es **desde el 19 de septiembre de 2019** a las 16:00h UTC+02:00 **hasta** las 23:59h UTC+02:00 del **9 de octubre de 2019**.

ENVÍO DE PROPUESTAS

En el portal <https://cybercamp.es> se encuentran todos los formularios de solicitud y presentación de propuestas.

Para el envío de la propuesta se deberá realizar el procedimiento siguiente:

1. Envío del documento de solicitud de participación en el CFP al buzón cfp@cybercamp.es dentro del plazo establecido, indicando, en el asunto del mismo, la referencia: «**CFP CyberCamp 2019**».
2. Envío del formulario de la propuesta a la plataforma <https://easychair.org/my/conference?conf=cybercamp19>

Existe un formulario para cada tipo:

- Ponencias magistrales.
- Talleres técnicos.
- Talleres técnicos de iniciación.
- Charlas inspiracionales y de promoción del talento.
- Charlas de concienciación.

Cada aspirante sólo podrá enviar 1 propuesta por tipología y un máximo de 2 propuestas en total, en caso de enviar más de una por cada tipo, sólo se tendrá en cuenta la recibida en primer lugar. Si se envían propuestas a más de dos tipologías se tomarán en consideración las recibidas en primer lugar, el resto serán descartadas.

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 expertos en ciberseguridad nombrado por INCIBE. La decisión de este jurado será inapelable. No pueden ser parte del jurado personas o entidades que presenten propuestas.

El proceso de selección 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.
- **Cada propuesta será valorada por al menos, 2 miembros del Jurado** 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 por tipología siempre y cuando aquellas propuestas superen el umbral de **60 puntos**.

En caso de empate:

- Para las categorías de ponencias magistrales, talleres técnicos, y talleres técnicos de iniciación el jurado dará prioridad en la clasificación a la propuesta que tenga mejor puntuación en el criterio del enfoque práctico.
- Para la categoría de charlas inspiracionales y de promoción del talento, en caso de empate el jurado dará prioridad en la clasificación a la propuesta que tenga mejor puntuación en el criterio de valor motivacional.
- Para la categoría de charlas de concienciación, en caso de empate el jurado dará prioridad en la clasificación a la propuesta que tenga mejor puntuación en el criterio carácter divulgativo.
- **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 en la herramienta de gestión del CFP y en la web, para cada tipología con un identificador 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**.

CRITERIOS DE VALORACIÓN

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

a) PONENCIAS MAGISTRALES

■ Enfoque práctico de la propuesta. Puntos asignados: de 0 a 35 puntos

Se establecen los siguientes sub-criterios de valoración:

| Puntuación | Índice de valoración |
|---------------|---|
| 0 – 30 puntos | <p>La ponencia tiene en cuenta aspectos particulares como:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Técnicas para el reconocimiento y defensa contra amenazas de seguridad. <input type="checkbox"/> La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros. <input type="checkbox"/> Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad. <input type="checkbox"/> Distribución pública de las herramientas presentadas. <input type="checkbox"/> Nuevos sistemas de defensa de ciberseguridad. <input type="checkbox"/> Nuevas líneas de investigación de ciberseguridad. |
| 0 – 5 puntos | <p>La propuesta plantea un enfoque práctico para 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.</p> |

Temática. Puntos asignados: de 0 a 30 puntos

Se establecen los siguientes sub-criterios de valoración:

| Puntuación | Índice de valoración |
|---------------|--|
| 0 – 15 puntos | <p>La temática propuesta aporta un enfoque diferenciador en el ámbito de la ciberseguridad, favoreciendo progresos científicos o tecnológicos.</p> |
| 0 – 10 puntos | <p>La temática propuesta se encuentra dentro del listado de temas que se presumen de interés aportando un enfoque innovador sobre el mismo.</p> |
| 0 – 5 puntos | <p>El esquema de la presentación es adecuado para el público objetivo y la temática presentada.</p> |

■ Valor didáctico:

Puntos asignados: de 0 a 20 puntos

| Puntuación | Índice de valoración |
|---------------|--|
| 0 – 10 puntos | <p>El conocimiento a transmitir al público objetivo es útil e instructivo</p> |
| 0 – 10 puntos | <p>El planteamiento que hace de la ponencia y su enfoque didáctico garantiza el éxito de la misma.</p> |

■ Que no haya sido difundida previamente en otros eventos.

Puntos asignados: de 0 a 15 puntos

Puntuación = 15 – nº congresos³ en los que se ha presentado anteriormente la propuesta presentada

³ Se entiende por congreso cualquier evento de ciberseguridad presencial de al menos una jornada de duración.

b) TALLERES TÉCNICOS

- **Enfoque práctico de la propuesta.** Puntos asignados: de 0 a 40 puntos

Se establecen los siguientes sub-criterios de valoración:

| Puntuación | Índice de valoración |
|---------------|---|
| | El taller tiene en cuenta aspectos particulares como: <ul style="list-style-type: none"> <input type="checkbox"/> Técnicas para el reconocimiento y defensa contra amenazas de seguridad. <input type="checkbox"/> La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros. <input type="checkbox"/> Divulgación responsable de exploits 0-day, propios o de terceros. <input type="checkbox"/> Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad, bien si son desarrollos propios o de terceros. <input type="checkbox"/> Distribución pública de las herramientas presentadas. <input type="checkbox"/> Nuevos sistemas de defensa de ciberseguridad. <input type="checkbox"/> Nuevas líneas de investigación de ciberseguridad. |
| 0 – 30 puntos | |
| 0 – 10 puntos | El taller plantea un enfoque práctico para 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. |

Temática. Puntos asignados: de 0 a 30 puntos

Se establecen los siguientes sub-criterios de valoración:

| Puntuación | Índice de valoración |
|---------------|---|
| 0 – 15 puntos | La temática propuesta aporta un enfoque diferenciador en el ámbito de la ciberseguridad, favoreciendo progresos científicos o tecnológicos. |
| 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. |
| 0 – 5 puntos | El esquema de la presentación es adecuado para el público objetivo y la temática presentada. |

- **Demostración práctica** Se valorará si el taller incluye demostraciones y los minutos estimados que conllevará esta parte práctica.

Puntos asignados: de 0 a 20 puntos

$$\text{Puntuación} = (20 * \text{minutos demostración}) / 60$$

Siendo 60 los minutos máximos de demostración propuestos

- **Que no haya sido difundida previamente en otros eventos.**

Puntos asignados: de 0 a 10 puntos

$$\text{Puntuación} = 10 - n^{\circ} \text{ congresos}^4 \text{ en los que se ha presentado anteriormente la propuesta presentada.}$$

c) TALLERES TÉCNICOS DE INICIACIÓN

⁴ Se entiende por congreso cualquier evento de ciberseguridad presencial de al menos una jornada de duración.

■ **Enfoque práctico de la propuesta.** Puntos asignados: de 0 a 40 puntos

Se establecen los siguientes sub-criterios de valoración:

| Puntuación | Índice de valoración |
|---------------|---|
| | El taller tiene en cuenta aspectos particulares como: |
| 0 – 30 puntos | <input type="checkbox"/> Técnicas para el reconocimiento y defensa contra amenazas de seguridad. <input type="checkbox"/> La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros. <input type="checkbox"/> Nuevos sistemas de defensa de ciberseguridad. <input type="checkbox"/> Nuevas líneas de investigación de ciberseguridad. <input type="checkbox"/> Identificación de herramientas prácticas |
| 0 – 10 puntos | El taller plantea un enfoque práctico para que el público objetivo adquiera los conocimientos de manera sencilla y adaptable a sus propias necesidades formativas. |

Temática. Puntos asignados: de 0 a 30 puntos

Se establecen los siguientes sub-criterios de valoración:

| Puntuación | Índice de valoración |
|---------------|---|
| 0 – 15 puntos | La temática propuesta aporta un enfoque diferenciador en el ámbito de la ciberseguridad, favoreciendo progresos científicos o tecnológicos. |
| 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. |
| 0 – 5 puntos | El esquema de la presentación es adecuado para el público objetivo y la temática presentada. |

■ **Demostración** Se valorará si el taller incluye demostraciones y los minutos estimados que conllevará esta parte práctica.

Puntos asignados: de 0 a 20 puntos

$$\text{Puntuación} = (20 * \text{minutos demostración}) / 90$$

Siendo 90 los minutos máximos de demostración propuestos

■ **Recursos didácticos.** 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.

D) CHARLAS INSPIRACIONALES Y DE PROMOCIÓN DEL TALENTO

■ **Valor motivacional.** Puntos asignados: de 0 a 45 puntos (sub-criterios no incrementales).

| Puntuación | Índice de valoración |
|---------------|--|
| 0 a 15 puntos | Valor testimonial: La propuesta incluye experiencias personales del ponente o evidencia casos de éxito adecuados. |
| 0 a 15 puntos | Mensaje: Se valorará la inclusión y adecuación de los mensajes y propuestas de acción claras y accionables. |

| Puntuación | Índice de valoración |
|---------------|---|
| 0 a 15 puntos | Carácter divulgativo de la charla. La charla es de fácil comprensión y el ponente utiliza un vocabulario estándar. |

- **Temática.** Puntos asignados: de 0 a 45 puntos (sub-criterios no incrementales).

| Puntuación | Índice de valoración |
|---------------|--|
| 0 a 15 puntos | Innovación y diferenciación. La temática propuesta aporta un enfoque diferenciador en el ámbito de la promoción del talento en ciberseguridad |
| 0 a 15 puntos | Concreción y profundidad de tratamiento. La temática propuesta ofrece un tratamiento profundo de alguno de los aspectos identificados dentro de las temáticas propuestas. |
| 0 a 15 puntos | Claridad expositiva. La estructura de la propuesta es adecuada y favorece la asimilación por parte de los asistentes. |

- **Carácter inédito.** Puntos asignados: de 0 a 10 puntos (sub-criterios incrementales).

Puntuación = 10 – nº congresos en los que se ha presentado anteriormente la propuesta presentada.

E) CHARLAS DE CONCIENCIACIÓN

- **Carácter divulgativo.** Puntos asignados: de 0 a 50 puntos.

| Puntuación | Índice de valoración |
|---------------|--|
| 0 a 25 puntos | Información clara y objetiva. La charla propuesta incluye información clara que permita dar a conocer al público el tema de concienciación abordado por el ponente. |
| 0 a 25 puntos | Adecuación al público objetivo. La charla es de fácil comprensión, y el ponente utiliza un vocabulario estándar para referirse a un tema de interés general. |

- **Recursos didácticos.** Puntos asignados: de 0 a 20 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.

- **Temática.** Puntos asignados: de 0 a 30 puntos (sub-criterios no incrementales).

| Puntuación | Índice de valoración |
|---------------|--|
| 0 a 15 puntos | Innovación y diferenciación. La temática propuesta aporta un enfoque diferenciador. |
| 0 a 15 puntos | Concreción y profundidad de tratamiento. La temática propuesta ofrece un tratamiento profundo de alguno de los aspectos identificados dentro de las temáticas propuestas. |

FORMALIZACIÓN DE LOS CONTRATOS

Las presentes bases servirán a efectos de publicidad, concurrencia, transparencia e igualdad de trato de los contratos menores que posteriormente se tramiten.

Conforme a lo previsto en las presentes bases si el candidato (persona que presenta una ponencia) es:

- Persona jurídica: se formalizarán contratos menores de acuerdo con lo previsto en el art. 118 de la Ley 9/2017 de Contratos del Sector Público.
- Persona física será de aplicación lo previsto en el artículo 310 de la Ley 9/2017 de Contratos del Sector Público en relación al Régimen de contratación que supone que las disposiciones de esta Ley no serán de aplicación a la preparación y adjudicación del contrato.

En cualquier caso por unificar el tratamiento y la formalización de las contrataciones con los candidatos seleccionados, tanto si es persona física como si es persona jurídica se procederá a la firma del modelo de contrato del **anexo I**.

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 previsto 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 contrato, 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 la ponencia/talleres/charla 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://cybercamp.es> 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 CyberCamp. No obstante, autoriza a INCIBE a que eventualmente utilice gratuitamente y sin restricciones, 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.

En particular, autoriza de forma irrevocable y gratuita a INCIBE para hacer uso, difusión y comunicación de su obra 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 en referencia al evento y su participación en el mismo.

PROTECCIÓN DE DATOS PERSONALES

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

Todos los datos personales que INCIBE, como responsable del tratamiento, deba tratar para la gestión de la tramitación de las presentes bases y formalización del contrato así como para enviar avisos sobre convocatorias relacionadas con el evento, serán incluidos en el registro de actividad de INCIBE «Eventos» cuya titularidad es de INCIBE, y cuya finalidad es la organización de eventos de ciberseguridad para transmitir, divulgar, formar en conocimientos y buenas prácticas en esta materia.

Los ponentes 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.

Asimismo, se podrán ejercitar los derechos de acceso, rectificación, limitación del tratamiento, supresión, portabilidad y oposición previstos en la normativa de protección de datos personales mediante carta a INCIBE, Avenida José Aguado nº 41 de León o por correo electrónico a dpd@incibe.es.

La base jurídica del tratamiento es su consentimiento y el tratamiento necesario para el cumplimiento derivado del contrato que van a suscribir las partes.

No están previstas cesiones internacionales de datos.

Es posible que sus datos deban comunicarse al encargado del tratamiento de INCIBE para la gestión del evento, que será la empresa que resulte contratista del expediente de contratación pública 016/19 en proceso de licitación.

Los datos que nos facilite a los efectos de este acuerdo 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.

En el aviso legal de la web de INCIBE www.incibe.es puedes encontrar más información sobre el tratamiento y ejercicio de tus derechos.

Para más información puedes acudir a la AEPD, que es la autoridad de control en materia de protección de datos.

CONTACTO

Para cualquier duda acerca del proceso, puede ponerse en contacto con la organización de CyberCamp a través del correo cfp@cybercamp.es

León, 19 de septiembre de 2019

Director General.

Alberto Hernández Moreno

ANEXO I.- CONTRATO PONENTES CYBERCAMP 2019

ACUERDO ENTRE _____ Y LA S.M.E. INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA M.P., S.A. PARA LA CONTRATACIÓN DE UN SERVICIO DE PONENCIA

En León a... de..... de 2019

REUNIDOS

De una parte, DON ALBERTO HERNÁNDEZ MORENO, mayor de edad, en su calidad de Director General de la S.M.E. Instituto Nacional de Ciberseguridad de España, M.P., S.A. (en adelante, "INCIBE"), con domicilio en 24005-León, Edificio INCIBE, Avda. José Aguado, 41 y C.I.F. A-24530735, facultado para este acto conforme consta en la escritura pública con número de protocolo 2233, otorgada el 24 de mayo de 2017 por la Notaria del Ilustre Colegio de Madrid, D^a. Ana López-Monís Gallego.

De otra parte, _____, mayor de edad, con domicilio a estos efectos en _____, en representación de la _____ en su calidad de _____, con capacidad legal para contratar según escrituras otorgadas el día _____ ante el notario de _____ D. _____, con número de protocolo _____.

INCIBE y _____ (en adelante, podrán ser denominadas, individualmente, "la Parte" y, conjuntamente, "las Partes"), reconociéndose mutuamente capacidad jurídica y de obrar suficiente para la celebración del presente contrato.

EXPONEN

Primero.- Que INCIBE es una sociedad dependiente del Ministerio de Economía y Empresa, siendo la entidad de referencia para el desarrollo, refuerzo y protección de la privacidad, ciberseguridad y de la confianza digital de ciudadanos y empresas, especialmente en el sector de las tecnologías de la información y de la comunicación, así como para sectores estratégicos en general.

Segundo.- Que CyberCamp es un evento organizado por el S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) y su próxima edición se celebrará entre el 27 y el 30 de noviembre de 2019 en el Palacio de Congresos de Valencia.

Tercero.- Que INCIBE promovió una convocatoria pública para la contratación de ponentes para el evento.

Cuarto.- Que la propuesta de _____ fue una de las seleccionadas tras la aplicación de los criterios de valoración recogidos en las bases de participación del Call for papers CyberCamp2019.

De conformidad con lo anterior, ambas Partes suscriben el presente contrato con las siguientes

ESTIPULACIONES

Primera.- Objeto

El presente contrato regla las condiciones para la impartición de un taller/ponencia durante el evento CyberCamp 2019, que se celebrará los próximos días 27 al 30 de noviembre de 2019 en el Palacio de Congresos de Valencia.

El candidato se compromete a realizar:

- La ponencia magistral cuya denominación es _____ y tiene una duración de 50 minutos el día _____
- El taller técnico cuya denominación es _____ y tiene una duración de 110 minutos el día _____
- El taller técnico de iniciación cuya denominación es _____ y tiene una duración de 90 minutos el día _____
- La charla inspiracional y de promoción del talento cuya denominación es _____ y tiene una duración de 50 minutos el día _____
- La charla de concienciación cuya denominación es _____ y tiene una duración de 30 minutos el día _____

El ponente es _____.

Tanto el ponente como el candidato manifiestan que el ponente es mayor de edad y que ninguno de ellos está incurso en ninguna de las causas de incompatibilidad o incapacidad fijadas por la legislación para contratar.

Segunda.- Duración.

La ponencia/taller o charla tendrá lugar en el sitio y día indicados en el apartado anterior.

En relación a la posibilidad de uso de la grabación realizada durante el evento tiene carácter ilimitado en los términos regulados en el presente contrato.

Tercera.- Obligaciones de las partes

INCIBE se obliga a:

- Poner a disposición del ponente la plantilla oficial de presentaciones de CyberCamp que será facilitada por la organización.
- Abonar el precio en las condiciones previstas en la cláusula cuarta.
- Poner a disposición del ponente un equipamiento técnico mínimo para la visualización de la presentación.
- Poner a disposición del ponente un contacto para dudas, aclaraciones y otras gestiones para su participación.

El candidato y/o ponente se obligan a:

- Crear una presentación profesional innovadora, tratando de evitar presentaciones que ya se hayan utilizado en otros eventos.
- Usar la plantilla oficial de presentaciones de CyberCamp que será facilitada por la organización.

- No incluir publicidad de ningún tipo en la presentación (marcas, empresas, productos, servicios, etc.)
- No atentar de ninguna forma contra la imagen ni prestigio de ninguna persona física o jurídica ni marca.
- No divulgar públicamente riesgos de seguridad de entidades públicas o privadas. Si existiera tal riesgo, deberán anonimizarse los contenidos que fueran necesarios.
- Enviar la presentación a la organización de CyberCamp con, al menos, 15 días de antelación al evento, para que pueda ser validada (concordancia con el trabajo presentado en el CFP y no inclusión de información inadecuada).
- Tratar de acomodar las modificaciones sobre la presentación que la organización pudiera sugerir, tras su revisión.
- Personarse en el evento con una antelación mínima de 2 horas antes de su participación, llevando todo lo necesario para impartir la ponencia y asegurándose de que la misma podrá desarrollarse sin contratiempos.
- Hacerse cargo de la gestión y de los gastos para su participación en el evento como por ejemplo desplazamientos, alojamiento, manutención etc., así como de cualquier otro gasto adicional que fuera necesario para la realización de la ponencia.
- Asumir las directrices que se especifiquen desde la organización, así como las normas recogidas en las [Bases Generales del Evento](#).
- Registrarse debidamente en la web del evento como asistente al mismo.
- Cumplir con lo dispuesto en las presentes Bases Generales del evento y en las bases particulares que regulen la actividad o actividades concretas en las que el participante intervenga o se inscriba.
- Atender y respetar las indicaciones de la Organización del evento, en todo momento.
- Respetar las instalaciones y material utilizado para el desarrollo del evento y actividades, manteniendo su buen estado de conservación y absteniéndose de llevar a cabo actuación alguna que pueda dañar, deteriorar o menoscabar el buen estado de aquellas.
- Actuar de buena fe, y comportarse con respeto y decoro hacia el resto de participantes y asistentes.

Cuarta.-Precio

El precio del contrato es de _____, impuestos y retenciones no incluidos.

Quinta.- Forma de pago

Este pago se realizará tras la participación en el evento por INCIBE previa presentación y conformidad de la factura o, en su defecto, emisión del certificado de ejecución del servicio por INCIBE.

Sexta.- Penalizaciones

En el caso de que el ponente no se presente a la especificada en el presente contrato, el candidato no recibirá el precio del contrato, con derecho a la indemnización de daños y perjuicios causados.

En el caso de que la intervención del ponente sea de duración inferior a 35 minutos en el caso de las ponencias o charlas de 50 minutos, o de 95 minutos en el caso de los talleres de 110 minutos, o de 75 minutos en el caso de los talleres de 90 minutos, se le abonará la cuantía restada de manera porcentual la duración no impartida.

Si INCIBE prescindiese de los servicios del conferenciante en los 15 días previos al evento, deberá abonar, en concepto de indemnización, la mitad de los honorarios pactados.

En caso de que por causa de fuerza mayor INCIBE no pudiera realizar el evento quedará liberado de sus obligaciones, cuando quede probada la ausencia de culpa o negligencia por su parte.

Séptima.- Publicidad de la obra y derechos de autor, confidencialidad, y privacidad

El candidato y/o el ponente conocen y aceptan que la ponencia/talleres/charla objeto del contrato podrá ser divulgada por INCIBE tanto en medios de comunicación escritos en soporte físico, como en Internet a través del portal <https://cybercamp.es> así como las redes sociales del evento.

El ponente mantendrá la titularidad y los derechos de autor que legalmente le correspondan sobre los contenidos, imágenes, documentación de cualquier clase presentada o desarrollada durante su participación en CyberCamp. Los candidatos y/o ponentes garantizan que son los autores y que ostentan la titularidad en exclusiva, libre de toda carga o limitación, de todos los derechos de propiedad intelectual e industrial sobre las propuestas, proyectos, contenidos y/o sus distintos componentes, presentados al evento, de conformidad con la legislación española sobre propiedad intelectual e industrial. Además, 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 ponente, cede de forma gratuita a INCIBE el uso de su imagen personal y su obra, que pudiera ser captada durante el evento, sin limitación ni restricción de ninguna clase. En particular, autoriza de forma irrevocable y gratuita a INCIBE para hacer uso de su imagen y/o su nombre, obra 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 en referencia al evento y su participación en el mismo.

El conferenciante da permiso para que su intervención sea grabada y transmitida en videostreaming en directo y publicada la misma en el canal de YouTube y en la web de CyberCamp. Nótese que la comunicación, difusión y/o reproducción de su intervención se realizará en cualquier canal ya sea tradicional u online.

Octava.- Propiedad intelectual

El candidato y/o el ponente conocen y aceptan que la ponencia/talleres/charla objeto del contrato podrá ser divulgada por INCIBE tanto en medios de comunicación escritos en soporte físico, como en Internet a través del portal <https://cybercamp.es> 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 CyberCamp. No obstante, autoriza a INCIBE a que eventualmente utilice gratuitamente y sin restricciones, 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 ponente, cede de forma gratuita a INCIBE el uso de su obra, que pudiera ser captada durante el evento, sin limitación ni restricción de ninguna clase. En particular, autoriza de forma irrevocable y gratuita a INCIBE para hacer uso de su obra 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 en referencia al evento y su participación en el mismo.

Novena.- Protección de datos de carácter personal

En cumplimiento de la normativa vigente en materia de protección de datos de carácter personal, INCIBE se compromete a no ceder a terceros ningún dato de carácter personal del conferenciante.

El conferenciante autoriza a INCIBE a la utilización de sus datos personales para la difusión y realización del evento (incluida la página web y las redes sociales y distintos medios de comunicación de CyberCamp).

Los ponentes ceden 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 ganadores 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 tomará las medidas oportunas para la protección de los datos y ficheros, frente a la destrucción, pérdida, alteraciones indebidas, cesiones y accesos no autorizados.

Todos los datos personales que INCIBE, como responsable del tratamiento, deba tratar para la gestión de la tramitación de las presentes bases y formalización del contrato así como para enviar avisos sobre convocatorias relacionadas con el evento, serán incluidos en el registro de actividad de INCIBE «Eventos» cuya titularidad es de INCIBE, y cuya finalidad es la organización de eventos de ciberseguridad para transmitir, divulgar, formar en conocimientos y buenas prácticas en esta materia.

Se podrán ejercitar los derechos de acceso, rectificación, limitación del tratamiento, supresión, portabilidad y oposición previstos en la normativa de protección de datos personales mediante carta a INCIBE, Avenida José Aguado nº 41 de León o por correo electrónico a dpd@incibe.es.

La base jurídica del tratamiento es su consentimiento y el tratamiento necesario para el cumplimiento derivado del contrato que van a suscribir las partes.

No se tienen previstas cesiones internacionales de datos.

El candidato y/o el ponente autoriza que los datos deban comunicarse al encargado del tratamiento de INCIBE para la gestión del evento que será la empresa que resulte contratista del expediente de contratación pública 016/19 Servicios CyberCamp 2019 - LOTE 1: Servicio de Gestión de Contenidos y Programa. En los pliegos que rigen dicha licitación se recogen las obligaciones específicas que en la materia se le imponen al contratista.

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.

En el aviso legal de la web de INCIBE www.incibe.es puedes encontrar más información sobre el tratamiento y ejercicio de tus derechos.

Para más información puedes acudir a la AEPD, que es la autoridad de control en materia de protección de datos.

Décima.- Resolución

Son causas por las que INCIBE puede acordar la resolución del Contrato:

- La muerte o incapacidad sobrevenida del contratista individual o la extinción de la personalidad jurídica de la sociedad contratista. En los casos de fusión de empresas en los que participe la sociedad contratista, continuará el contrato vigente con la entidad absorbente o con la resultante de la fusión, que quedará subrogada en todos los derechos y obligaciones dimanantes del mismo. Igualmente, en los supuestos de escisión, aportación o transmisión de empresas o ramas de actividad de las mismas, continuará el contrato con la entidad resultante o beneficiaria, que quedará subrogada en los derechos y obligaciones dimanantes del mismo, siempre que tenga la solvencia exigida al acordarse la adjudicación.
- La declaración de concurso conforme al procedimiento establecido en la ley concursal o la declaración de insolvencia en cualquier otro procedimiento.
- El mutuo acuerdo entre las partes.
- La no formalización del contrato en plazo.
- La demora en el cumplimiento de los plazos por parte del contratista, y el incumplimiento de los plazos o las obligaciones esenciales establecidas en el contrato. Y no alcanzar los objetivos por causas imputables a _____ . Cualquier tipo de incumplimiento después del tercer apercibimiento.
- La falta de capacidad o solvencia sobrevenidas o estar incurso, con posterioridad a la adjudicación, en alguna de las prohibiciones de contratar.
- Las demás establecidas expresamente en el contrato.

En caso de resolución del contrato _____, a solicitud de INCIBE, deberá cesar de inmediato en todos los trabajos contratados. Asimismo, se procederá a efectuar la liquidación definitiva de los trabajos realizados hasta la fecha que se consideren útiles para INCIBE, quien abonará los trabajos realizados en las condiciones establecidas en el Contrato hasta dicha fecha. En todo caso, INCIBE deducirá de la cantidad que resulte de la liquidación el importe correspondiente a indemnizaciones y demás conceptos que procedan.

Se considera obligación contractual esencial:

Cualquiera de las propuestas de _____ que se haya tenido en cuenta en la valoración.

En su caso, las obligaciones del contratista en relación con la subcontratación.

La resolución del contrato se acordará por el órgano de contratación.

Y en prueba de conformidad las Partes firman el presente Contrato, en LEÓN en la fecha señalada en el encabezado.

INCIBE

(Empresa)

Conformidad de la
ponencia / taller

Director General

Apoderado

DATOS FISCALES PARA FACTURACIÓN⁵

PERSONA FÍSICA:

- D./Dña.:
- NIF:
- Dirección:
- CP:
- Provincia:
- Número de cuenta (IBAN):

PERSONA JURÍDICA:

- Nombre de la empresa:
- CIF:
- Dirección:
- CP:
- Provincia:
- Número de cuenta (IBAN):

⁵ Indicar lo que corresponda persona física o jurídica.