GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

CALL FOR PAPERS

Bases de participación CyberCamp 2017

INSTITUTO NACIONAL DE CIBERSEGURIDAD

OBJETO

El objeto de las presentes bases es el de regular la participación de ponentes o formadores, en la próxima edición del evento CyberCamp, organizado por el Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE), los próximos días 30 de noviembre, 1, 2 y 3 de diciembre de 2017 en Santander.

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

Todas las propuestas deberán girar en torno a **la ciberseguridad[1] y estarán enfocadas a un perfil técnico**. Podrán ser de dos tipologías:

- **Ponencias** de ciberseguridad de 50 minutos de duración.
- **Talleres técnicos prácticos** a modo de clase magistral de 110 minutos de duración. Dentro de los talleres podrán considerarse aquellas propuestas que incluyan demostraciones en directo (tiempo real o pre-grabada) de ciberseguridad.

Por la presente convocatoria, se seleccionarán un mínimo de 3 propuestas de ponencias y 3 talleres técnicos prácticos para impartir en CyberCamp. Cada autor solo podrá enviar una propuesta para cada tipo, en caso de enviar más de una solo se tendrá en cuenta la recibida en primer lugar.

No obstante, a medida que se acerquen las fechas de celebración del evento, podrían surgir nuevas vacantes de ponencia o talleres en la agenda. En tal caso, podrían llegar a seleccionarse un número superior de propuestas presentadas a través de este *call for papers.* Para la selección se seguirá la clasificación de las propuestas presentadas de mayor a menor puntuación.

Conforme al artículo 304 del Texto Refundido de la Ley de Contratos del Sector Público las disposiciones de esta Ley no serán de aplicación a la preparación y adjudicación de los contratos que tengan por objeto la prestación de actividades docentes en centros del sector público desarrolladas en forma de conferencias o cualquier otro tipo similar de actividad, siempre que dichas actividades sean realizadas por personas físicas.

PLAZO

El plazo para la presentación de solicitudes de ponencias y talleres técnicos para participar en CyberCamp 2017 finaliza el próximo 26 de septiembre de 2017, a las 00:00h UTC+02:00

CANDIDATOS

Podrá **participar** cualquier persona **mayor de 18 años** que no sea personal laboral de INCIBE o se encuentre cursando una beca en INCIBE.

[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]

PROCEDIMIENTO DE PRESENTACIÓN DE PROPUESTAS

A continuación se muestra un listado meramente indicativo, con carácter no exhaustivo, sobre temáticas que se presumen de interés para CyberCamp 2017:

- Pentesting, Hacking ético, Exploiting.
- Gestión de incidentes, Análisis forense/anti-forense.
- Ciberinteligencia e intercambio de información, inteligencia artificial, machine learning.
- Ingeniería Inversa, esteganografía, criptomonedas, APT.
- Hardware hacking, seguridad en sistemas embebidos, biometría, IoT.
- Seguridad de las redes anónimas: TOR, Freenet, I2P, etc.
- 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: 3G/4G/WIMAX, GSM, VOIP, Satélite, WiFi, NFC, GPS, RFID.

ENVIO DE PROPUESTAS

Para el envío de la propuesta se deberá de presentar el modelo de documento adjunto en la sección *call for papers* del portal web de CyberCamp y completar correctamente los campos requeridos. Una vez cumplimentado, se deberá remitir a la dirección cfp@cybercamp.es dentro del plazo establecido, indicando, en el asunto del mismo, la referencia: «CFP CyberCamp 2017».

El máximo de propuestas en la que podrá participar un ponente será una por tipología de propuesta.

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

CRITERIOS PARA LA VALORACIÓN DE LAS PROPUESTAS

Se valorarán los siguientes aspectos de la propuesta:

a) Talleres:

- **Enfoque práctico de la propuesta**.

  Puntos asignados: de 0 a 40 puntos

  Se establecen los siguiente sub-criterios de valoración:

Puntuación	Indice de valoración
0 – 30 puntos	El taller tiene en cuenta aspectos particulares como: □ Técnicas para el reconocimiento y defensa contra amenazas de seguridad. □ La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros. □ Divulgación responsable de exploits 0-day, propios o de terceros. □ Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad, bien si son desarrollos propios o de terceros. □ Distribución publica de las herramientas presentadas. □ Nuevos sistemas de defensa de ciberseguridad. □ Nuevas líneas de investigación de ciberseguridad.
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	Indice 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 de 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

  Puntos asignados: de 0 a 20 puntos

Puntuación	Indice de valoración
20 puntos	Para aquellas propuestas de talleres que incluyan una demostración con una duración de más del 57% del tiempo asignado
16 – 19 puntos	Para aquellas propuestas de talleres que incluyan una demostración con una duración superior al-48% e igual o inferior al 57 % del tiempo asignado

Puntuación	Indice de valoración
11 – 15 puntos	Para aquellas propuestas de talleres que incluyan una demostración con una duración superior al 33% e igual o inferior al 48% del tiempo asignado
4 – 10 puntos	Para aquellas propuestas de talleres que incluyan una demostración con una duración aproximada superior al 12% e igual o inferior 33% del tiempo asignado
1 – 3 puntos	Para aquellas propuestas de talleres que incluyan una demostración con una duración menor al 9% del tiempo asignado
0 puntos	Para aquellas propuestas de talleres que no incluyan ningún tipo de demostración

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

  Puntos asignados: de 0 a 10 puntos

Puntuación	Indice de valoración
10 puntos	Para aquellas propuestas de talleres que no hayan sido presentados en ningún evento anteriormente
3 puntos	Para aquellas propuestas de talleres que ya hayan sido presentadas 1 o 2 eventos en su totalidad o parcialmente
0 puntos	Para aquellas propuestas de talleres que ya hayan sido presentadas en 3 o más eventos en su totalidad.

b) Ponencias

- **Enfoque práctico de la propuesta.**

  Puntos asignados: de 0 a 40 puntos

  Se establecen los siguiente sub-criterios de valoración:

Puntuación	Indice de valoración
0 – 30 puntos	El taller tiene en cuenta aspectos particulares como: ◻ Técnicas para el reconocimiento y defensa contra amenazas de seguridad. ◻ La exposición y/o descubrimiento de nuevas vulnerabilidades de ciberseguridad, propias o de terceros. ◻ Divulgación responsable de exploits 0-day, propios o de terceros. ◻ Presentación de nuevas herramientas o sistemas desarrollados en ciberseguridad, bien si son desarrollos propios o de terceros. ◻ Distribución publica de las herramientas presentadas. ◻ Nuevos sistemas de defensa de ciberseguridad.

Puntuación	Indice de valoración
	▫ Nuevas líneas de investigación de ciberseguridad.
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	Indice 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 de 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.

- **Valor didáctico:**

  Puntos asignados: de 0 a 20 puntos

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

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

  Puntos asignados: de 0 a 10 puntos

Puntuación	Indice de valoración
10 puntos	Para aquellas propuestas de talleres que no hayan sido presentados en ningún evento anteriormente
7 puntos	Para aquellas propuestas de talleres que ya hayan sido presentadas parcialmente
3 puntos	Para aquellas propuestas de talleres que ya hayan sido presentadas en menos de 3 eventos en su totalidad.
0 puntos	Para aquellas propuestas de ponencias que ya hayan sido presentadas en más de 4 eventos en su totalidad.

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 INCIBE. La decisión de este jurado será inapelable.

El proceso de valoración será el siguiente:

- Se comprobará que la temática versa sobre ciberseguridad. Las propuestas que no cumplan este requisito serán excluidas.
- Se valorarán las propuestas aplicando los criterios indicados. Se elaborará una lista para cada tipología de propuesta. La clasificación de las propuestas será ordenada de mayor a menor.
- Se seleccionarán atendiendo al orden de clasificación.
- En caso de empate, el jurado seleccionará la propuesta que tenga mejor puntuación en el criterio del enfoque práctico.

FECHAS DEL PROCESO

FECHAS (2017)	ACCIÓN
18 de julio	Apertura del *call for papers*
25 de septiembre	Cierre del *call for papers*
27 de septiembre	Inicio de la valoración de los *call for papers* recibidos
04 de octubre	Fin de valoración
11 de octubre	Notificación de los *call for papers* aceptados
18 de octubre	Anuncio público de ponencias seleccionadas en la web https://cybercamp.es

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.

Además, se publicará un listado tanto para talleres como para ponencias con un identificador para aquellas que hayan sido seleccionadas y para que las tres primeras que se encuentren en reserva para cada modalidad.

IMPORTE A PERCIBIR POR LOS PONENTES

Los ponentes cuyas propuestas sean seleccionadas recibirán una cantidad de 750€ a la que habrá que deducir las retenciones del IRPF correspondientes. Dicha cantidad será abonada tras su participación en el evento como ponente. Este pago se realizará previa presentación de factura o, en su defecto, emisión de certificado de retenciones practicadas.

La gestión de las contrataciones y/o pagos se realizará por el contratista de INCIBE del contrato de servicios de logística integral y organización del evento CyberCamp 2017 (expediente 016/17).

COMPROMISOS ASUMIDOS POR EL PONENTE

La mera participación en este *call for papers* implica la aceptación de los siguientes compromisos por parte del ponente:

- Creación de una presentación profesional innovadora, tratando de evitar presentaciones que ya se hayan utilizado en otros eventos.
- Uso de la plantilla oficial de presentaciones de CyberCamp que será facilitada por la organización.
- No inclusión de 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.
- Envío de 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.

PUBLICIDAD DE LA OBRA Y DERECHOS DE AUTOR, CONFIDENCIALIDAD, Y PRIVACIDAD

A efectos de la participación en este *call for papers* únicamente se requerirá la entrega o depósito del material aportado por el participante con el fin realizar la valoración de su propuesta tomando como criterio las presentes bases.

Las propuestas seleccionadas sin embargo podrán ser objeto de divulgación por INCIBE, en las comunicaciones que realice de carácter informativo o divulgativo, y tanto en medios de comunicación escritos en soporte físico, como en Internet.

INCIBE se compromete a mantener la confidencialidad sobre aquellas propuestas que no resulten seleccionadas. Sus datos personales serán cancelados una vez se haya procedido a comunicar la no aceptación de la propuesta.

Los participantes mantendrán en todo caso la titularidad y los derechos de autor que legalmente les correspondan sobre los contenidos presentados o desarrollados durante su participación en CyberCamp. No obstante, autorizan a INCIBE a que eventualmente utilice

gratuitamente y sin restricciones, cualquier imagen, sonido, o cualquier otro contenido presentados por los participantes, 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.

Mediante la aceptación de estas Bases, ceden en exclusiva y 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, los ponentes seleccionados autorizan de forma irrevocable y gratuita a INCIBE para hacer uso de su imagen y/o sus nombres, 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. La comunicación, difusión y/o reproducción de su intervención podrá realizarse en cualquier canal ya sea tradicional u online.

Asimismo, el participante consiente que la organización almacene sus datos personales y los use para la comunicación pública de su elección como propuesta seleccionada

En cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y del R.D. 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de desarrollo, le informamos que la información recabada se almacenará en un fichero, cuyo titular es INCIBE. El fichero se denomina Eventos y tiene como finalidad el registro y control de asistencia en eventos promovidos por la sociedad y el desarrollo de las actividades en él contenidas.

El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se deberá llevar a cabo mediante comunicación por escrito y con la referencia “Protección de Datos”, a la sede de INCIBE, sita en Avda. José Aguado nº 41, 24005 León, en los términos previstos en la normativa anteriormente citada o mediante correo electrónico a calidad@incibe.es. Puede tener información en https://www.incibe.es/aviso-legal

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.

CONTACTO

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