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

Invitación pública para la colaboración en la promoción de la cultura de la ciberseguridad mediante la organización de eventos CyberCamp en España

INCIBE 2021

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017 TU AYUDA EN CIBERSEGURIDAD

ÍNDICE

1. INTRODUCCIÓN 3
2. OBJETO 4
3. destinatarios 4
4. DOTACIÓN PRESUPUESTARIA 4
4.1. COSTES ELEGIBLES 5
5. VENTAJAS Y COMPROMISOS 7
6. OBLIGACIONES DE LAS PARTES 9
6.1. INCIBE 9
6.2. Colaborador 10
7. MEMORIA DE CIERRE 11
8. SOLICITUD de PARTICIPACIÓN 12
9. PUBLICIDAD 14
10. RÉGIMEN JURÍDICO 15
10.1. Órgano competente 15
10.2. Propiedad intelectual 15
10.3. Confidencialidad 16
10.4. Protección de datos de carácter personal 17
10.4.1. De las organizaciones que participen en la Invitación Pública 17
10.4.2. De los participantes en las actuaciones formativas 18
10.5. Naturaleza jurídica de los Convenios 20
10.6. Jurisdicción y resolución de controversias 20
10.7. Publicidad y notificaciones 20
ANEXO I. FORMULARIO DE SOLICITUD 21
ANEXO II. MEMORIA 22

1. INTRODUCCIÓN

La ciberseguridad y la confianza digital son hoy dos de los retos más importantes a los que se enfrentan gobiernos, empresas y ciudadanos. Se trata de aspectos de crucial importancia en un contexto global, interconectado y dependiente de la tecnología como es el actual, e imprescindible para alcanzar la necesaria confianza en el ámbito digital.

La Estrategia Nacional de Ciberseguridad, dentro de su "*Objetivo IV: Cultura y compromiso con la Ciberseguridad y potenciación de las capacidades humanas y tecnológicas*", desarrolla a través de una serie de medidas incluidas en la "***Línea de Acción 7: Desarrollar una cultura de Ciberseguridad***", centrada en **contribuir a la consolidación de la confianza digital para ciudadanos y empresas**. En este contexto, la Agenda España Digital 2025, como parte del ***Plan de recuperación, transformación y resiliencia*** de España y en el contexto global del plan europeo "NextGenerationEU", constituye el marco global estratégico y el motor acelerador de la transformación digital del país, y especifica que es imprescindible el desarrollo de las capacidades de ciberseguridad de ciudadanía, empresas y Administraciones Públicas, así como la generación de confianza a través de una cultura de ciberseguridad que llegue a todas las capas de la sociedad.

INCIBE, como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y las empresas, tiene como misión desarrollar actuaciones y medidas que contribuyan a alcanzar los objetivos anteriores, particularmente la organización de **eventos y actividades dirigidas a la elevación de la cultura y concienciación en ciberseguridad**, dirigidos a ciudadanos, menores de edad y sus familias, padres y educadores, estudiantes de universidades, centros de formación, centros tecnológicos e instituciones de investigación y profesionales y empresarios, dirigidos a impulsar las capacidades en ciberseguridad de la sociedad y la economía en general. Eventos como *CyberCamp* o *Summer BootCamp* se han convertido en una referencia nacional e internacional que aglutina cada año a una importante comunidad de personas, jóvenes y familias interesadas en mejorar sus conocimientos en este ámbito.

Englobado en la promoción y generación de la cultura en ciberseguridad se lanza la presente Invitación de colaboración (en adelante, la **Invitación**), destinada a apoyar la organización de eventos CyberCamp en el ámbito de la ciberseguridad promovidos por **universidades públicas** legalmente constituidas en España.

A esta Invitación Pública y los convenios que se firmen, les será aplicable lo dispuesto en la normativa europea y nacional sobre el Mecanismo de Recuperación y Resiliencia y el Plan de Recuperación, y en especial el Reglamento (UE) n.º 2020/2094 del Consejo, de 14 de diciembre de 2020, por el que se establece un Instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis de la COVID; el Reglamento (UE) n.º 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, y el Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia, así como la normativa de desarrollo europea y nacional.

2. OBJETO

INCIBE lanza la presente invitación destinada a universidades y fundaciones universitarias de carácter público legalmente constituidas a la fecha de esta convocatoria con el objeto de promocionar el desarrollo del conocimiento y capacidades de personas y organizaciones en el ámbito de la ciberseguridad mediante el apoyo a la organización conjunta con INCIBE de eventos CyberCamp.

INCIBE apoyará en régimen de colaboración, mediante la firma de Convenios de colaboración, la organización de eventos bajo la marca CyberCamp por Universidades y Fundaciones universitarias públicas españolas, que cumplan los requisitos de esta Invitación y sean seleccionados por INCIBE.

Se seleccionarán propuestas de colaboración en orden a facilitar el desarrollo de un evento bajo la marca Cybercamp en cada una de las Comunidades Autónomas españolas, como criterio general, si bien, en las de mayor población podrán seleccionarse dos. En el caso de recibir propuestas de más de una universidad para la realización de la actividad en un mismo marco autonómico, se atenderá al criterio de preferencia de mayor número de actividades propuestas en la candidatura. Asimismo, INCIBE podrá proponer la realización de acuerdos de colaboración entre dos o más universidades en una misma Comunidad que faciliten el desarrollo de los eventos.

En aquellas comunidades o ciudades autónomas que tengan cobertura de distrito universitario se podrá facilitar el desarrollo de eventos por universidades con sede en territorios autonómicos limítrofes.

En cualquier caso, no se restringirá el límite territorial de las actividades a los residentes a una única comunidad autonómica, siendo este un criterio orientativo que facilite el alcance de los eventos Cybercamp a todos los ámbitos territoriales. De este modo cualquier persona u organización deberá poder participar en las actividades programadas independientemente de su lugar de residencia o procedencia. Las universidades públicas UNED y la UIMP podrán proponer asimismo programas circunscritos a una o varias Comunidades autónomas.

3. DESTINATARIOS

Podrán solicitar la participación en esta Invitación Pública universidades públicas y fundaciones sin ánimo de lucro vinculadas a universidades públicas a la fecha de esta convocatoria, debiendo, en todo caso, desarrollar sus actividades y tener sede en el ámbito territorial de España.

4. DOTACIÓN PRESUPUESTARIA

La dotación presupuestaria global para esta Invitación asciende a 3.450.000€ (impuestos indirectos no incluidos) durante el periodo comprendido desde la fecha de publicación hasta el 31 de diciembre de 2023, repartidos de la siguiente forma (impuestos indirectos no incluidos):

- 1.200.000€ primera convocatoria (cuarto trimestre 2021).
- 750.000€ segunda convocatoria (2022).
- 750.000€ tercera convocatoria (2022).
- 750.000€ cuarta convocatoria (2023).

La justificación presupuestaria se corresponde con las siguientes líneas y componentes incluidos en el Plan de Recuperación Transformación y Resiliencia, concretamente:

- Línea directriz del plan: Transformación digital
- Componente 15: "Conectividad Digital, impulso de la ciberseguridad y despliegue del 5G"
- Inversión 7: "Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, PYMEs y profesionales; e Impulso del ecosistema del sector" como una de las actuaciones concretas orientadas a desarrollar las capacidades de ciberseguridad tanto de ciudadanos como empresas y al impulso del ecosistema de ciberseguridad español en el marco de la estrategia de soberanía digital europea.
- Eje 1: "Fortalecimiento de las Capacidades", Pilar (2): Capacitación en Ciberseguridad (desarrollo de Recursos Específicos, incorporación de las competencias digitales en ciberseguridad en todos los niveles educativos, etc.)"

Más información en el siguiente enlace: https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/05052021-Componente15.pdf .

El límite de la aportación económica por parte de INCIBE será de 150.000 euros por beneficiario y convocatoria.

De conformidad con el artículo 9 del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, los proyectos que se financien con cargo al Mecanismo de Recuperación y Resiliencia solo podrán recibir ayuda de otros programas e instrumentos de la Unión siempre que dicha ayuda no cubra el mismo coste.

INCIBE aportará un máximo del 60% de los costes elegibles de las actuaciones que cumplan los requisitos de esta Invitación.

El abono de estas aportaciones de INCIBE se realizará de la siguiente forma: un 50% del compromiso se abonará anticipadamente con la firma del Convenio, y otro 50% a la finalización de la actuación, con la presentación y aprobación de la justificación de los gastos y la Memoria final. Corresponderá a la Comisión de Seguimiento del convenio de colaboración aprobar el plan de gastos y sus correspondientes justificaciones, recabando cuanta información justificativa complementaria necesaria que permita conocer el impacto de las actuaciones desarrolladas y su correcta ejecución y, elevando la preceptiva propuesta de abono a INCIBE.

4.1. COSTES ELEGIBLES

Los importes de la cofinanciación aportada por INCIBE en concepto de las diferentes acciones se incluirán en el convenio específico que se suscriba con la entidad beneficiaria y no serán excluyentes entre sí, pudiendo acumularse.

Las Universidades y fundaciones universitarias deberán colaborar mediante la organización de eventos bajo la marca CyberCamp, que conlleven aportaciones en especie y/o gastos de los siguientes tipos:

- Costes de dirección y coordinación de las actuaciones.
- Costes de personal propio o subcontratado para la impartición y ejecución de las diferentes actividades, en función del porcentaje de dedicación al proyecto. No se consideran elegibles los costes de personal propio de INCIBE ni del colaborador durante las fases de diseño, pero sí durante el evento.

Estos gastos se justificarán mediante la presentación de las nóminas, seguros sociales y sus respectivos justificantes de pago, así como una certificación firmada por el responsable legal indicando el porcentaje de dedicación asumido por cada uno de los trabajadores imputados al proyecto, que acredite que estos no son gastos recurrentes de la entidad. En el caso de trabajadores imputados al 100% al proyecto, se debe presentar también su contrato laboral

- Costes para la contratación de servicios externos y personal para el desarrollo de actividades. que siendo necesarios para la ejecución del proyecto la Universidad o Fundación Universitaria no pueda realizar por sí misma.
  Se podrán realizar subcontrataciones siempre que el porcentaje subcontratado no exceda del 50% del importe total del proyecto. Se entiende que la entidad subcontrata cuando concierta con terceros la ejecución total o parcial de la actividad que constituye el objeto del Convenio o de aquellas actividades que pudiendo ser realizadas por la entidad beneficiaria se externalizan. Queda fuera de este concepto la contratación de aquellos gastos en que tenga que incurrir el beneficiario para la realización por sí mismo de la actividad objeto del Convenio.
  En estas contrataciones de servicios externos se aplicarán, en la medida de lo posible, criterios de sostenibilidad, concurrencia y aquellos necesarios para favorecer la igualdad entre hombres y mujeres.
  Deberán justificarse mediante la presentación de la correspondiente factura o documento acreditativo del gasto y su respectivo justificante de pago.
- Coste de amortización de los bienes inventariables de logística del evento: dotación de medios, equipamiento y recursos de acondicionamiento de los espacios, plataformas de teleformación o de retos y costes de infraestructura del evento.
  La amortización de material inventariable durante el periodo de ejecución del proyecto, incluida la adquisición de software o aplicación informáticas, se justificará mediante la correspondiente factura o documento acreditativo y su respectivo justificante de pago, siempre que tengan relación directa con la ejecución de las actividades, no exista otra financiación para las mismas y la amortización correspondiente esté debidamente contabilizada por la entidad en el ejercicio de ejecución de la actuación.
- Costes por el uso de aulas y espacios de la Universidad o Fundación universitaria.
  Se consideran costes de retención por tratarse de gastos causados a dicha universidad por la utilización de instalaciones, equipamientos y servicios generales. Su justificación se realizará mediante certificado emitido por el Gerente de la Universidad al término del periodo de duración del Convenio. Dichos costes no podrán exceder de las tasas aprobadas por los órganos de gobierno de la administración universitaria en cada caso.
  En el caso de que los costes de retención no incluyan costes indirectos como los gastos relativos al suministro de agua, electricidad, seguridad, gestoría, calefacción y limpieza, correo, telefonía e internet, material y suministros de oficina y gastos de alquiler de locales o sede social de la entidad, así como otras contrataciones o servicios que, no estando directamente vinculados con el objeto de la ayuda, son necesarios para el correcto funcionamiento de la Universidad, podrá incrementarse el porcentaje de retención, previa justificación, y con la aprobación de INCIBE.
  En todo caso estos costes indirectos se justificarán mediante tanto alzado sobre los gastos directos, hasta un máximo de 4%. La justificación de estos gastos consistirá en una certificación firmada por el Gerente de la Universidad.

- Costes de difusión y marketing relativo a las acciones a desarrollar enmarcadas en el convenio. Se incluyen en esta categoría los costes de adquisición de material publicitario, premios y regalos.
- También serán financiables otros costes no contemplados en los anteriores apartados que se deriven de la actuación y que sean necesarios para su ejecución, siempre que sean acordados por ambas partes e incluidos como tales en el Convenio de colaboración

Como regla general, el Mecanismo para la Recuperación y Resiliencia solo financiará gastos no recurrentes que supongan un cambio estructural y tengan un impacto duradero sobre la resiliencia económica y social, la sostenibilidad, la competitividad a largo plazo y el empleo.
Se considerarán gastos elegibles aquellos que, de manera indubitada, estén relacionados con la actividad objeto del Convenio, sean necesarios para su ejecución, hayan sido contraídos durante el periodo de ejecución aprobado para cada proyecto y se encuentren efectivamente pagados con anterioridad a la finalización del período de justificación. Los gastos deberán estar sujetos a precios de mercado. Los gastos deberán estar a nombre de las Universidades y/o fundaciones universitarias. No serán admisibles los gastos contraídos antes del inicio del cronograma de la actividad objeto del Convenio, a excepción los correspondientes a amortización de material inventariable previamente adquirido y que a fecha de inicio del proyecto no esté completamente amortizado.

5. VENTAJAS Y COMPROMISOS

Las universidades públicas, a través de la presente Invitación, tienen la oportunidad de contribuir **a la consolidación de la confianza digital para ciudadanos y empresas**, de la mano de INCIBE.

INCIBE apoyará en régimen de cofinanciación la organización de eventos bajo la marca CyberCamp, de carácter híbrido (combinando actividades virtuales y presenciales). Las aportaciones de INCIBE pueden ser otorgadas a eventos que cumplan los siguientes requisitos:

- El evento deberá realizarse en España.
- El evento deberá ser presencial y virtual como regla general, teniendo preferencia sobre los eventos exclusivamente presenciales o exclusivamente *on line*.
- El evento debe versar sobre ciberseguridad.
- Se entiende por evento CyberCamp un programa de actividades que incluya, de modo no exhaustivo, actividades tales como congresos, convenciones, reuniones de expertos, competiciones, cursos, talleres, charlas magistrales y similares, con una programación definida y documentada, que tiene un público y alcance determinados, que tienen lugar de modo virtual o presencial en una o varias ubicaciones concretas, y que tienen un lema u objetivo concreto diferenciable de otros eventos y/o ediciones anteriores
- Todas las actividades deberán integrar la marca o nombre CyberCamp haciendo expresa referencia a la colaboración con INCIBE, así como las referencias a procedencia de los fondos presupuestarios nacionales y/o europeos, como por ejemplo el Plan de Recuperación Transformación y Resiliencia.

- El evento debe incluir alguna de las siguientes actividades u otras que tengan un alcance similar a propuesta de las universidades sumando un mínimo de 100 horas para eventos 100% online, al menos 2 jornadas para eventos con formato presencial y, al menos un objetivo de participación de 200 personas:
  - **Para público general:**
    - Talleres de concienciación
    - Talleres de iniciación en tecnologías de ciberseguridad
    - Talleres de competencias digitales
    - Espacio expositivo de soluciones / proyectos de ciberseguridad locales
    - Talleres de aprendizaje en aspectos concretos a nivel técnico de la ciberseguridad.
  - **Para públicos familiares:**
    - Itinerarios educativos para menores por rango de edad (6 – 8, 9 – 13, +14).
    - Talleres para menores “Uso seguro de Internet” + acciones gamificación.
    - Actividades programadas con centros educativos
    - Aplicativos digitales gamificados.
    - Actividades tipo gymkanas, scape rooms, juegos de pregunta-respuesta, competiciones, teatro, etc.
    - Talleres formativos sobre uso seguro de Internet que adopten metodologías educativas innovadoras y colaborativas (análisis de casos, juegos de roles).
    - Programación de los itinerarios para menores con los centros educativos locales.
    - Talleres familias: mediación parental en Internet.
    - Talleres para educadores sobre competencias digitales de ciberseguridad para trabajar con alumnos y para fomentar el teletrabajo seguro.
    - Talleres para familias sobre estrategias de mediación parental en Internet.
    - Espacios informativos y de asesoramiento (por ejemplo, el Stand Ciberseguridad 017 de INCIBE).
  - **Para públicos profesionales y empresariales:**
    - Talleres de Concienciación para profesionales y empresas
    - Talleres de implantación de ciberseguridad en la empresa
    - Charlas inspiracionales de profesionales y empresas de ciberseguridad.
    - Talleres y simulaciones “role-play” de ciberseguridad
    - Talleres de gestión de riesgos e implementación de un Plan Director de Seguridad y planes de continuidad de negocio y similares.
    - Concursos de conocimientos en ciberseguridad
    - Talleres y charlas sobre Tecnologías de Ciberseguridad.
    - Espacio expositivo de soluciones de ciberseguridad de empresa.

- **Para públicos interesados en desarrollo de talento, empleabilidad y emprendimiento:**
  - Talleres de concienciación para estudiantes y academia
  - Talleres de especialización en tecnologías de ciberseguridad
  - Talleres específicos de investigación en ciberseguridad
  - Ferias de empleo y orientación curricular:
  - Charlas técnicas.
  - Charlas inspiracionales.
  - Ponencias de soft-skills y relacionadas con la preparación de la contratación (head-hunters, profesionales de RRHH, etc.) que ayuden a preparar la entrevista, el CV y aspectos a tener en cuenta para incrementar la contratación laboral en materia de ciberseguridad
  - Charlas o talleres generales sobre los profesionales de la Ciberseguridad.
  - Entrenamientos y competiciones de hacking ético.
  - Charlas generalistas de oportunidades y salidas profesionales en ciberseguridad.
  - Ferias de empleo: con al menos 5-10 empresas virtual o presencial que ofrezcan empleos relacionados con la Ciberseguridad.
  - Talleres y charlas sobre Emprendimiento en ciberseguridad
    - Talleres de ideación y creación de ideas de negocio
    - Talleres sobre modelo de negocio (Business Model Canvas)
    - Jornadas inspiracionales.
    - Servicios vs. Desarrollo de tecnología
    - Talleres de creación de empresas
    - Talleres de soft skills
    - Talleres de creación de empresas ciber: Financiación y ayudas

Seleccionada la entidad, y conforme a la solicitud realizada se formalizará el correspondiente convenio de colaboración entre las partes recogiendo los derechos y obligaciones a los que INCIBE y la entidad se comprometen.

6. OBLIGACIONES DE LAS PARTES

6.1. INCIBE

INCIBE se compromete a:

- Realizar una aportación económica para la realización del programa conforme a lo estipulado en esta Invitación.
- Aportar personal propio o subcontratado para la definición, planificación, ejecución y seguimiento del programa.
- Prestar apoyo técnico, documental o equivalente necesario para el desarrollo de las actividades.

- Prestar colaboración y apoyo institucional en la difusión del programa. Para ello cederá el uso de la marca CyberCamp en los términos que se recojan en el convenio específico de colaboración.
- En su caso, aportar contenidos específicos para el evento, tales como: impartición de una charla o taller, generación de materiales específicos, acudir al evento presencial con un stand institucional o similar y cualquier otro que se considere de interés y se describirá en el convenio específico.

6.2. Colaborador

La Universidad o fundación universitaria, deberá responsabilizarse del desarrollo de las actividades programadas y verificar que los conceptos de gasto y cantidades que incluya, se adecúen a la memoria del proyecto cerrada entre ambas entidades y aprobada por la Comisión de Seguimiento.

Las entidades colaboradoras deberán cumplir, además, con las obligaciones, europeas y nacionales, relativas a la financiación del Mecanismo de Recuperación y Resiliencia de la Unión Europea y el Plan de Recuperación, que se establezcan por la normativa europea y nacional. Entre otras, deberán contribuir a los objetivos establecidos en el Plan de Recuperación con respecto al etiquetado digital, con un porcentaje del 100%, y adoptar las medidas necesarias para prevenir, detectar y corregir situaciones de fraude, conflicto de intereses y corrupción

En el diseño y ejecución de las actuaciones objeto de los convenios en el marco del Plan de Recuperación, las entidades colaboradoras garantizarán el respeto al principio de »no causar un perjuicio significativo», conforme a lo previsto en el Plan de Recuperación, en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, y su normativa de desarrollo, en particular la Comunicación de la Comisión Guía técnica sobre la aplicación del principio de «no causar un perjuicio significativo» en virtud del Reglamento relativo al Mecanismo de Recuperación y Resiliencia, así como con lo requerido en la Decisión de Ejecución del Consejo relativa a la aprobación de la evaluación del plan de recuperación y resiliencia de España.

De acuerdo con los fines del **Plan de Recuperación, Transformación y Resiliencia**, si fuera necesario realizar nuevas contrataciones de personal, se tendrán en cuenta criterios de creación neta de empleo en España, subcontratación a empresas que generen empleo en nuestro país o en la Unión Europea, cohesión territorial consistente en que la actividad y el empleo se genere en ciudades pequeñas o pueblos, fuera de las ciudades o zonas industriales y de Igualdad de género, debiendo tener especialmente en cuenta a pymes, micropymes, autónomos y start-ups. Asimismo, deberán aplicarse criterios para mejorar el impacto de género.
En particular, los beneficiarios estarán obligados a crear en España todo el empleo necesario para la realización de la actividad, que se realizará con personal contratado y afiliado a la Seguridad Social en el territorio nacional. El cumplimiento de este requisito tendrá que justificarse documentalmente.

Además, deberán contribuir a los objetivos de soberanía digital y autonomía estratégica de la Unión Europea, así como garantizar la seguridad de la cadena de suministro teniendo en cuenta el contexto internacional y la disponibilidad de cualquier componente o subsistema tecnológico sensible que pueda formar parte de la solución, mediante la

adquisición de equipos, componentes, integraciones de sistemas y software asociado a proveedores ubicados en la Unión Europea.

7. MEMORIA DE CIERRE

A la finalización del convenio suscrito con la entidad, se realizará una memoria de actuaciones, la cual deberá ser aprobada por la Comisión de Seguimiento.

Para la justificación de los gastos, se presentará a INCIBE la siguiente documentación:

- Certificación de la Gerencia o Servicio de Contabilidad al término del periodo de duración del presente Convenio sobre las horas de dedicación de profesores empleadas y coste asociado a esa dedicación, así como un listado adicional de otros gastos y pagos al personal colaborador contratado, en caso necesario. Este certificado indicará, de forma expresa, los registros o archivos donde se encuentra custodiada o depositada la documentación justificativa y los departamentos y/o personas responsables de la misma.
- Memoria académica, con la periodicidad acordada entre las partes, de las actividades realizadas en la forma que acuerde la Comisión de Seguimiento.
- Indicadores de impacto que se acuerden por las partes.

La Universidad mantendrá la custodia de los justificantes de gastos y pagos realizados y se compromete a ponerlos a disposición de INCIBE y de los órganos de control y auditoría competentes durante el periodo legal regulado en las normas nacionales y comunitarias.

INCIBE verificará que los gastos realizados resulten elegibles de acuerdo con las normas y criterios previstos y acordados, pudiendo solicitar el reintegro a la Universidad de aquellas cantidades que no se hayan ejecutado conforme a las mismas, sobre cualquier pago anticipado.

La aprobación final del gasto y de las actuaciones deberá recogerse por escrito y en acta por parte de la Comisión de Seguimiento.

Deberá hacerse referencia a la entidad financiadora y de los fondos origen de la financiación en todas las publicaciones y comunicaciones que se deriven del desarrollo de las actividades.

En cuantas actuaciones de difusión pública se realicen en el desarrollo de las actividades deberán reflejarse las señas de identidad y logos de la Universidad y del Instituto Nacional de Ciberseguridad, así como al Plan de Recuperación, Transformación y Resiliencia.

En todo caso, la marca o el logotipo y distintivos de las partes se utilizarán exclusivamente en la versión que cada una facilite, sin que se puedan alterar colores, formas, símbolos o gráficos. Cualquier alteración de los signos anteriormente mencionados supondrá una infracción de los derechos del titular de la marca.

La Universidad queda expresamente obligada a mantener absoluta confidencialidad y reserva sobre los datos con los que se trabajan con ocasión del desarrollo de las actividades, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al previsto, ni tampoco ceder a otros, ni siquiera a efectos de conservación, sin el previo consentimiento por escrito de la otra parte.

Se considera sujeta a confidencialidad a cualquier información a la que la Universidad acceda en virtud de las colaboraciones acordadas, en especial la información y datos

propios de las partes que con tal carácter se indique, a los que hayan accedido durante la ejecución del mismo, así como la documentación.

La Universidad informará a su personal, colaboradores y subcontratistas de las obligaciones establecidas en la presente cláusula de confidencialidad, así como de las obligaciones relativas al tratamiento automatizado de datos de carácter personal conforme a la legislación vigente, recabando un compromiso, por escrito, de éstos sobre el presente extremo.

La Universidad se obliga al cumplimiento de Legislación en materia de Protección de Datos de Carácter Personal y demás normativa aplicable en materia de protección de datos. Para ello, Universidad e INCIBE suscribirán durante la vigencia de la colaboración cuantos documentos sean necesarios y establecerán las medidas jurídicas, técnicas y organizativas para dar cumplimiento a la normativa de protección de datos de carácter personal durante la ejecución del mismo.

Mediante el correspondiente acuerdo que determine el detalle de las colaboraciones, Universidad e INCIBE se someterán a la legislación española y dicho acuerdo se regirá conforme al artículo 51 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP). El preceptivo acuerdo de colaboración adquirirá naturaleza administrativa, siendo competencia de la Jurisdicción Contencioso Administrativa la resolución de las cuestiones litigiosas que se susciten sobre el mismo

8. SOLICITUD DE PARTICIPACIÓN

Las solicitudes de participación por parte de las universidades y fundaciones universitarias públicas, deben remitirse a sociedad@incibe.es indicando en el asunto “Invitación Pública. Promoción de cultura de ciberseguridad” o por correo ordinario a la siguiente dirección:

S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A.

Atención: CIUDADANOS

Edificio INCIBE

Avenida José Aguado, nº 41

24005 León

Esta Invitación estará abierta por espacio de 25 meses contados a partir del día siguiente a la publicación de la misma.

Las solicitudes deben contener la siguiente información:

- Formulario de solicitud (Anexo I), debidamente cumplimentado.
- Propuestas de colaboración y memoria detallada conforme al Anexo II.

El proceso de selección es el siguiente:

1. La entidad interesada envía el formulario de solicitud (Anexo I), junto al Anexo II y Memoria al buzón sociedad@incibe.es, con firma electrónica válida (se comprobará en valide.es) o por correo ordinario o mensajería a INCIBE.
2. INCIBE, a través de una Comisión técnica designada al efecto, valora la adecuación de la información proporcionada a las presentes bases.

Las propuestas recibirán una calificación sobre un total de 30 puntos a efectos de establecer la priorización. Los criterios de valoración de las propuestas serán los siguientes:

- Experiencia de la Universidad en programas de formación, difusión, divulgación y promoción de la ciberseguridad (hasta 8 puntos).
  - 2 puntos: La universidad ha realizado 5 programas.
  - 4 puntos: La universidad ha realizado entre 6 y 10 programas.
  - 6 puntos: La universidad ha realizado entre 11 y 15 programas.
  - 8 puntos: La universidad ha realizado más de 15 programas.
- Adecuación de la propuesta de actividades. Para cada una de las actividades presentadas se valorará en base a la siguiente baremación y se calculará la media ponderada. Hasta 10 puntos.
  - Nivel de adecuación con el público objetivo. Nivel de ponderación: 4 puntos.
    - Bajo 1 punto
    - Medio 2 puntos.
    - Alto 4 puntos
  - Originalidad. Nivel de ponderación: 4 puntos.
    - Bajo 1 punto
    - Medio 2 puntos
    - Alto 4 puntos
  - Carácter pedagógico. Nivel de ponderación: 2 puntos.
    - Si / No (2 puntos / 0 puntos)
- Nº de actividades propuestas (hasta 8 puntos):
  - 2 puntos: La universidad propone al menos 5 actividades.
  - 5 puntos: La universidad propone entre 5 y 10 actividades.
  - 8 puntos: La universidad propone entre 10 y 15 actividades.
- Nivel de cobertura de los públicos interesados 4 puntos. Un punto por público cubierto (público general, público familiares, público profesional y empresarial, público interesados en desarrollo de talento, empleabilidad y emprendimiento).

3. INCIBE podrá solicitar cuantas aclaraciones sean necesarias para poder valorar la propuesta recibida, o la personalidad jurídica del solicitante.
4. La Comisión técnica elaborará una propuesta de prelación cada 4 meses en el orden de colaboraciones a establecer, iniciando los contactos con la entidad solicitante a efectos de determinar de mutuo acuerdo el alcance y contenido de la colaboración.
5. La prelación de Universidades guiará la propuesta de establecimiento de acuerdos específicos, que estarán limitados por las disponibilidades presupuestarias referidas en apartado 2 de estas Bases.
6. Una vez acordados los términos de la colaboración, se remitirá a la entidad el texto del Convenio de Colaboración, que deberá ser firmado por un representante con poderes suficientes, y por la Dirección General de INCIBE.

7. Con carácter previo a la autorización del convenio, en los supuestos en que se requiera, INCIBE comunicará ante el Ministerio de Hacienda y Función Pública la propuesta de colaboración.
8. Los Convenios de colaboración firmados serán publicados por INCIBE conforme la normativa que les resulta de aplicación, procediendo las entidades conforme a derecho proceda.
9. Junto a los Convenios, las Universidades aportarán declaración responsable de ser conocedor de que la financiación a la que se accede, procede del Mecanismo de Recuperación y Resiliencia de la Unión Europea y que asume todas las obligaciones derivadas del Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021, y de las demás normas de la Unión sobre la materia y por las normas estatales de desarrollo o trasposición de estas, especialmente con respecto al requerimiento de cumplir con el principio de «no ocasionar un perjuicio significativo». Dicha declaración incluirá compromiso por escrito de conceder los derechos y los accesos necesarios para garantizar que la Comisión Europea, a Oficina Europea de Lucha contra el Fraude (OLAF), el Tribunal de Cuentas Europeo, la Fiscalía Europea y las autoridades nacionales competentes ejerzan sus competencias.

- La Comisión técnica tendrá la siguiente composición:
  - Subdirección del área de Sociedad y Empresas.
  - Responsable del área de Ciudadanos en Ciberseguridad.
  - Un representante del Área de Comunicación, Marketing y Relaciones de INCIBE, que podrá ser, bien el /la subdirector/a de la misma, bien el/la Responsable de Relaciones Institucionales y Estrategia.
  - 1 experto externo a INCIBE a propuesta de la RENIC o entidad similar.
  - 1 experto externo a INCIBE a propuesta de la CRUE.

- La Comisión técnica elaborará una propuesta de prelación en el orden de colaboraciones a establecer, iniciando los contactos con la entidad solicitante a efectos de determinar de mutuo acuerdo el alcance y contenido de la colaboración en los términos del apartado 5 de estas Bases.

9. PUBLICIDAD

Todas las acciones, documentación y materiales desplegados en el marco de los acuerdos de colaboración suscritos bajo las presentes bases y condiciones, deberán incluir necesariamente la referencia a que se realizan con el sostén y apoyo del Mecanismo Europeo de Recuperación y Resiliencia (MRR) y como parte de las medidas del Plan de Recuperación Transformación y Resiliencia.

INCIBE facilitará a las Universidades beneficiarias los correspondientes logos oficiales, incluidos los de la marca CyberCamp, y el del Gobierno de España, pudiendo requerir la

inclusión, modificación y difusión correspondientes en todo momento del desarrollo de las acciones acordadas.

Además deberá hacerse referencia a la cofinanciación de INCIBE, por lo que cuantas actuaciones de difusión pública se realicen deberán reflejar las señas de identidad y logos de la Universidad y de INCIBE. Estas marcas o distintivos de las partes se utilizarán exclusivamente en la versión que cada una facilite, sin que se puedan alterar. Tanto la Universidad o fundación como INCIBE se reservan todos los derechos sobre sus marcas y nombres comerciales.

10. RÉGIMEN JURÍDICO

10.1. Órgano competente

En el marco de esta Invitación Pública, INCIBE actuará como impulsor de esta iniciativa y será el responsable de la misma. De igual forma, INCIBE coordinará con total transparencia el proceso de publicación de la convocatoria, presentación de solicitudes, y la posterior selección de las entidades colaboradoras.

Todas las resoluciones que se estimen necesarias para la consecución e interpretación del contenido de estas Bases, se llevarán a cabo por la Dirección General de INCIBE.

10.2. Propiedad intelectual

Los derechos de autor relativos a los contenidos creados o utilizados por cualquiera de las partes en base a actuaciones amparadas en esta convocatoria seguirán perteneciendo a sus legítimos titulares, salvo que se convenga otra forma mediante convenios específicos con aquellos.

Las publicaciones o resultados objeto del desarrollo de las iniciativas deberán reconocer y hacer constar la participación de todos los intervinientes por ambas partes y el reconocimiento a ambas instituciones.

Cada parte mantendrá la propiedad y todos los derechos derivados sobre los elementos, herramientas, proyectos y, en general, sobre cualquier aportación a las iniciativas que le pertenezca con anterioridad a la ejecución de los mismos o los desarrolle al margen del Convenio (“background”) y no sea directamente el resultado de la colaboración (“foreground”).

En el supuesto de resultados susceptibles de protección por alguno de los títulos que el Derecho reconoce, así como de explotación o difusión de dichos resultados, las partes, en un plazo máximo de tres meses a partir de su obtención, se comprometen a suscribir un documento al efecto en el que se determinará la titularidad de los derechos de propiedad y las condiciones de su explotación. En cualquier caso, ambas entidades tendrán derechos intransferibles y no enajenables, ilimitados y a título gratuito y sin otras condiciones sobre

los resultados generados en el marco de la presente Invitación Pública.

Sin perjuicio de lo anterior, las partes se autorizarán mutuamente a la explotación y difusión de los materiales formativos de su propiedad que sean generados durante el convenio y con cargo a su presupuesto en posteriores actividades formativas o de concienciación ya sea a título gratuito u oneroso. En el supuesto de que dichos contenidos y materiales formativos pertenezcan a otras entidades que participan en el Programa se deberá contar con la previa autorización de estas.

Asimismo, si terceros llegaran a participar en las iniciativas, deberán salvaguardarse los derechos de las entidades firmantes de este Convenio sobre los resultados obtenidos, patentables o no, generados por los intervinientes y los correspondientes derechos sobre su explotación. El régimen de asignación y uso de los derechos será acordado expresamente antes de aprobar la participación de terceros en el proyecto.

De resultar seleccionada, la Entidad deberá hacer referencia al Convenio firmado entre ambas partes en todas las publicaciones y comunicaciones que se deriven de su desarrollo. A excepción de aquellos casos en que una de las entidades expresamente comunique a la otra que no desea participar en dichas publicaciones o comunicaciones.

INCIBE y la entidad colaboradora se reservan todos los derechos sobre sus marcas y nombres comerciales y en general todos los derechos de propiedad industrial e intelectual anteriores que sean aportados a los proyectos.

10.3. Confidencialidad

INCIBE se compromete a tratar toda la información o documentación que las partes deban compartir con motivo de esta invitación con la debida confidencialidad y reserva, especialmente aquellos datos de carácter personal y de carácter técnico de los servicios y/o productos, no pudiendo copiar o utilizar dichos datos con fines distintos a los que figura en la convocatoria.

Se considerará información confidencial cualquier información que contenga datos personales del participante, prestando especial atención a los temas relacionados con la tecnología, productos, procedimientos, procesos o know-how de los participantes de la convocatoria.

Se excluye de la categoría de información confidencial toda aquella información que sea divulgada por los solicitantes, que sea de dominio público, que haya de ser revelada de acuerdo con las leyes o con una resolución judicial o acto de autoridad competente o aquella que sea necesaria revelar para la correcta ejecución de la invitación.

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.

10.4. Protección de datos de carácter personal

10.4.1. De las organizaciones que participen en la Invitación Pública

Los datos personales facilitados son recabados por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) como responsable del tratamiento con el fin de gestionar esta Invitación Pública.

Los datos que se recabarán son los recogidos en el formulario de solicitud (Anexo I), para gestionar su participación en esta Invitación y serán tratados de conformidad con lo dispuesto en las normativas vigentes en protección de datos personales, en concreto en el Reglamento (UE) 2016/679 de 27 de abril (GDPR), así como la normativa española vigente en la materia, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y la Ley 1/1982 de protección civil, derecho al honor, intimidad personal y familiar y a la propia imagen.

INCIBE recoge exclusivamente la información personal que sea necesaria para alcanzar el propósito específico que en este caso será gestionar su participación en esta Invitación Pública. Toda esta información no podrá utilizarse para una finalidad distinta e incompatible con la descrita o autorizada. En caso de querer usar dichos datos para otro fin distinto del aquí expuesto, se deberá solicitar el consentimiento del interesado.

Así mismo, los datos serán tratados para cumplir con las obligaciones normativas requeridas a INCIBE.

Los datos personales podrán ser comunicados a autoridades y organismos públicos, para el cumplimiento de una obligación legal requerida a INCIBE.

Los datos serán tratados mientras permanezcan vigentes las autorizaciones derivadas de la participación en la presente Invitación, siendo suprimidos una vez finalizada la misma, siendo conservados exclusivamente:

- Durante el plazo de prescripción de las acciones derivadas de dichas relaciones, a los únicos efectos de cumplir con las obligaciones legales requeridas y para la formulación, ejercicio o defensa de reclamaciones.

¿Qué derechos tiene el participante sobre sus datos personales?:

- Derecho de acceso. Puede preguntar a INCIBE si está tratando sus datos y de qué manera.
- Derecho de rectificación. Puede pedirnos que actualicemos sus datos personales si son incorrectos o inexactos y suprimirlos si así lo desea.
- Derecho de limitación del tratamiento. En este caso únicamente serán conservados por INCIBE para el ejercicio o la defensa de reclamaciones.
- Derecho de oposición. Tras su solicitud de oposición al tratamiento, INCIBE dejará de tratar los datos en la forma que indique, salvo que por motivos legítimos

imperiosos o el ejercicio o la defensa de posibles reclamaciones se tengan que seguir tratando.

- Derecho a la portabilidad de los datos. En caso de que quiera que sus datos sean tratados por otra empresa, INCIBE le facilitará la portabilidad de sus datos al nuevo responsable de acuerdo con lo previsto en la normativa.
- Derecho de supresión. Puede solicitar que eliminemos sus datos cuando ya no sean necesarios para el tratamiento, haya retirado su consentimiento, sea un tratamiento ilícito o haya una obligación legal para hacerlo. Analizaremos el supuesto y aplicaremos la ley.

Para el ejercicio de estos derechos puede dirigirse mediante carta a INCIBE, Avenida José Aguado nº 41 de León o por correo electrónico a dpd@incibe.es

Si necesita más información sobre qué derechos tiene reconocidos en la Ley y cómo ejercerlos, puede dirigirse a la Agencia Española de Protección de Datos, que es la autoridad de control en materia de protección de datos y la autoridad ante la que puede presentar una reclamación.

10.4.2. De los participantes en las actuaciones formativas

Para el tratamiento de los datos personales de los participantes de las iniciativas formativas que se desarrollarán dentro del marco de esta Invitación Pública, las Partes se obligan al cumplimiento del Reglamento (UE) 2016/679 de 27 de abril (GDPR) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección Datos Personales y garantía de los derechos digitales y demás normativa aplicable en materia de protección de datos.

Las Partes, suscribirán durante la ejecución de los futuros acuerdos cuantos documentos sean necesarios y establecerán las medidas jurídicas, técnicas y organizativas para dar cumplimiento a la normativa de protección de datos de carácter personal durante la ejecución del mismo, dependiendo de la tipología de datos personales que para cada actuación sean necesarios.

Asimismo, las partes garantizan que el tratamiento de los datos se producirá dentro de la legítima finalidad de dar cumplimiento al acuerdo que firmarán las entidades, y que se encuentra dentro de los fines legítimos de las mismas, de manera que las entidades garantizarán que los datos de carácter personal objeto de estas actuaciones se han recabado y tratado dando cumplimiento a sus deberes de información y transparencia así como a todas las garantías legales, técnicas y organizativas que exige la normativa de protección de datos.

Cada una de las Partes, como responsable de datos personales facilitará a cada interesado los datos de contacto del Delegado de Protección de Datos.

El/los titular/es de dichos datos podrán ejercer los derechos de acceso, rectificación y supresión, de limitación del tratamiento y de oposición dirigiéndose por escrito a los respectivos Delegados de Protección de Datos, o mediante los mecanismos que las partes

informen y dispongan al efecto.

Asimismo, se informará a cada interesado del derecho a presentar reclamación por el tratamiento de los datos de carácter personal ante la Agencia Española de Protección de Datos (www.aepd.es) o la autoridad de control pertinente, y de la conservación de los datos durante el tiempo necesario para la relación jurídica y de los plazos legales que regulen ésta.

Las partes declararán que han informado a los representantes, personas de contacto u otros empleados cuyos datos personales se recojan en el marco del presente acuerdo de que los datos de carácter personal que figuran en el mismo y todos aquellos que durante la prestación del servicio pudieran recabarse:

a) se tratarán bajo la responsabilidad de la otra parte para la celebración, ejecución y control de este Acuerdo, el cumplimiento de sus obligaciones legales, así como la realización de remisiones de obligado cumplimiento. Este tratamiento se basa en el interés legítimo de las partes y en el cumplimiento de obligaciones legales.

b) podrán comunicarse a

- agencias de prevención de fraude
- Tribunales para cumplir con los requisitos legales y para la administración de justicia
- otros terceros cuando sea necesario para la celebración, ejecución y control de este Acuerdo así como para proteger la seguridad o la integridad de las operaciones comerciales de su empresa o cuando así lo exija una ley.

c) que podrán ejercitar, en cualquier momento, sus derechos de acceso, rectificación, supresión, oposición, portabilidad y de limitación del tratamiento (o cualesquiera otros reconocidos por ley) mediante notificación escrita, a la atención del responsable o delegado de protección de datos, a las direcciones indicadas en el epígrafe siguiente.

d) que en INCIBE el Delegado de Protección de Datos es la figura encargada de supervisar y asesorar sobre el cumplimiento de la normativa de protección de datos. Los interesados podrán ponerse en contacto con el Delegado de Protección de Datos cuyos datos de contacto se indican a continuación:

Por INCIBE: dpd@incibe.es o por correo postal dirigiéndose a Edificio INCIBE en Avenida José Aguado, 41 24005 León.

e) que los datos serán tratados durante la vigencia del Acuerdo y, tras ello, permanecerán bloqueados por el periodo de prescripción de cualesquiera acciones legales o contractuales que resulten de aplicación.

f) que pueden presentar cualquier reclamación o solicitud relacionada con la protección de datos personales ante la Agencia Española de Protección de Datos o ante la autoridad nacional que en su caso sea competente.

10.5. Naturaleza jurídica de los Convenios

Los Convenios que se firmen entre INCIBE y las Universidades y fundaciones públicas tienen naturaleza administrativa, o privada y se regirán, en cada caso, por lo que resulte de la normativa de aplicación en función de los sujetos intervinientes.

10.6. Jurisdicción y resolución de controversias

La resolución de las controversias que pudieran plantearse sobre la interpretación y ejecución de los convenios derivados de esta Invitación deberán solventarse de mutuo acuerdo entre las partes, a través de la Comisión de Seguimiento. En caso de no alcanzarse un acuerdo en sede de comisión, las partes acuerdan someter las controversias surgidas, bien a la jurisdicción contencioso-administrativa que resulte objetiva y territorialmente competente, bien a la civil, en cuyo caso, las partes se someterán preferentemente a los Juzgados y Tribunales de León.

10.7. Publicidad y notificaciones

La información general referida, junto con sus anexos está publicadas en el perfil contratante de la web de INCIBE.

Todas las notificaciones que se deban realizar en el marco de esta Invitación serán realizadas mediante correo electrónico de manera individualizada, haciendo uso de los datos aportados por los solicitantes en el proceso de solicitud, por lo que las entidades colaboradoras deberán tener actualizado el e-mail de contacto, que además deberá corresponder a una persona de la empresa.

Será publicada en la web de INCIBE la lista definitiva de entidades colaboradoras.

Para cualquier aclaración y reclamación sobre la Invitación pueden dirigirse a la siguiente dirección de correo electrónico sociedad@incibe.es, indicando en el asunto “Invitación Pública para la colaboración en la promoción de la cultura de la ciberseguridad mediante la organización de eventos CyberCamp en España”.

León, 3 de Diciembre de 2021

Directora General

S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A.

ANEXO I. FORMULARIO DE SOLICITUD

Datos de la persona que suscribe la solicitud	
Nombre y apellidos	
Departamento o centro al que está adscrito	
DNI	
E-MAIL	
Teléfono	
Datos de la universidad pública a la que pertenece el solicitante	
DNI / CIF	
Dirección Postal	
Nombre de la entidad	
Datos de contacto a efectos de notificaciones (si son diferentes a los arriba indicados)	
Nombre y apellidos	
e-mail	
Teléfono	
Autorización o visto bueno del Rector o Vicerrector delegado para proceder a la solicitud y acordar los términos de la eventual colaboración	
Nombre y apellidos	
e-mail	
Teléfono	
Firma	

ANEXO II. MEMORIA

Esta memoria acompañará a la solicitud y estará conformada por los siguientes apartados:

- **Planteamiento del evento**

  El solicitante deberá hacer una propuesta del planteamiento del evento que presenta incluyendo los aspectos limitantes y KPI poniendo de manifiesto aquellos aspectos de valor que conseguirán que el evento sea un éxito.

- **Recursos**

  Se detallarán todos los aspectos relativos a los recursos con los que cuenta la Universidad para el desarrollo de las actividades, el equipo humano que llevará a cabo la coordinación y el desarrollo de los trabajos señalados, el calendario y plan de trabajo previsto para el desarrollo de las actividades.

- **Experiencia en programas de formación**.

  El solicitante incluirá el listado y descripción de los programas de formación, difusión y promoción de la ciberseguridad que haya realizado en los últimos 3 años para su valoración.

  Para acreditar la experiencia previa, se deberá detallar para cada actividad / programa y/o iniciativa la siguiente información:

Nombre del programa	Breve descripción	Fechas de realización	Número de beneficiarios

- **Memoria de actividades.**

  Para cada una de las actividades propuesta, se deberá dar toda la información posible para poder valorar la adecuación y nivel de cobertura en los términos recogidos en la presente Invitación. Si no se dispone de información suficiente, se otorgarán 0 puntos.

  En esta memoria, se detallará el alcance y coste estimados para cada una de las acciones a organizar para cada una de estas modalidades. Para cada una de las actividades se deberá detallar:

Actividad	Fechas previstas	Breve descripción	Público/s destinatario/s de la actividad	Número de beneficiarios	Coste total	Cofinanciación por parte de la Universidad