GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

BASES REGULADORAS Y CONVOCATORIA PARA EL PROGRAMA DE ACELERACIÓN INTERNACIONAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDICE

ANTECEDENTES Y MOTIVACIÓN

Dentro de las iniciativas promovidas por el Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE) se encuentran las dirigidas a **promover una industria de ciberseguridad fuerte** que contribuya al aumento de la confianza digital. Para ello, **dada la naturaleza global del mercado, se pretende facilitar** el crecimiento de las empresas existentes y **el acceso de nuevas propuestas de alta escalabilidad y proyección internacional.**

El objeto de las presentes bases es el de regular la convocatoria de **la Aceleradora Internacional de Start Ups de ciberseguridad.**

La presente convocatoria está organizada conjuntamente por el Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE), La Agencia de Innovación, Financiación e Internacionalización Empresarial de Castilla y León (ADE) y el Instituto Leonés de Desarrollo, Formación y Empleo (ILDEFE) en los términos recogidos en el Convenio de Colaboración suscrito entre las tres entidades con fecha 7 de junio de 2017.

Dentro de las iniciativas promovidas por el Instituto Nacional de Ciberseguridad de España, S.A. (INCIBE) se encuentran aquellas dirigidas a promover una industria de ciberseguridad fuerte que contribuya al aumento de la confianza digital. Para ello, dada la naturaleza global del mercado, se pretende facilitar el crecimiento de las empresas existentes y el acceso de nuevas propuestas de alta escalabilidad y proyección internacional.

La ADE (ahora Instituto para la Competitividad Empresarial de Castilla y León) es un ente público de la Administración de la Comunidad de Castilla y León adscrito a la Consejería competente en materia de promoción económica. El artículo 3 del Decreto 67/2011, de 15 de diciembre, por el que se aprueba el Reglamento General de la ADE, le atribuye competencias para la ejecución de las políticas de apoyo dirigidas a las empresas en los sectores de la economía productiva, específicamente el desarrollo de actuaciones de apoyo a la creación de empresas, y de manera especial, el apoyo y la promoción para la creación de empresas innovadoras y/o de base tecnológica.

En el ejercicio de estas competencias el Acuerdo 34/2014, de 10 de abril, de la Junta de Castilla y León, por el que se aprueba el I Plan de Apoyo a la Creación de Empresas en Castilla y León, designa a la ADE (ahora Instituto para la Competitividad Empresarial de Castilla y León) como órgano gestor de las Medidas IV.3.2 (Servicios de demanda en I+D+i) y IV.3.5. (Espacios físicos especializados), dentro del Programa IV, Apoyo a la I+D+i y los espacios de innovación, cuyos objetivos son el facilitar el acceso de las personas emprendedoras a los recursos tecnológicos disponibles, potenciar la capacidad innovadora de las nuevas empresas mediante la colaboración con agentes del sistema y acelerar el desarrollo de los proyectos innovadores (respecto a la Medidas IV.3.2) y Facilitar el acceso a infraestructuras adecuadas a las personas con iniciativa emprendedora, valorizar los recursos materiales y tecnológicos existentes y potenciar la colaboración entre Administraciones Públicas, comunidad educativa y agentes relacionados con la innovación (respecto a la Medida IV.3.5)

El ILDEFE es una empresa pública del Ayuntamiento de León entre cuyos objetivos se encuentra la promoción e impulso de las iniciativas públicas generadoras de riqueza, ocupación y bienestar, en cuanto contribuyan al desarrollo económico y social de la ciudad, y la participación, juntamente con la iniciativa privada, en actuaciones de tal naturaleza, así como el desarrollo de todas las actuaciones relacionadas con la formación

profesional, la generación de empleo y la adecuación de la mano de obra a las nuevas condiciones del mercado laboral, y su coordinación con otras actuaciones que, con objetivos similares, desarrollen en el Municipio de León cualesquiera otras entidades o instituciones, públicas o privadas, de cualquier ámbito territorial.

El Convenio de Colaboración suscrito por las tres entidades tiene por objeto **la** promoción del emprendimiento en ciberseguridad mediante el apoyo a la atracción de talento y generación de ideas de negocio y **la aceleración de proyectos emprendedores en materia de ciberseguridad**, cuya fase presencial de aceleración tendrá lugar en la ciudad de León, en los espacios habilitados para ello, pudiendo tener lugar alguna sesión y / o jornada en la Sede de INCIBE.

Para ello, las partes se comprometen a organizar un concurso **de proyectos de emprendimiento empresarial en materia de ciberseguridad,** de acuerdo con los principios de publicidad, transparencia, objetividad, igualdad y no discriminación seguidos de una fase de aceleración presencial de proyectos de emprendimiento.

Los gastos generados en el desarrollo de este Programa de Aceleración serán financiados según se indica a continuación:

a) Con cargo al presupuesto de la ADE (ahora Instituto para la Competitividad Empresarial de Castilla y León): 30.000 euros.
b) Con cargo al presupuesto de ILDEFE: 30.000 euros,
c) Con cargo al presupuesto de INCIBE: 60.000 euros.

En el marco de dicho Convenio se aprueban las presentes Bases.

PRIMERA.- Objeto y alcance del programa

El objeto de las presentes bases es el de regular la convocatoria de participación en el Programa de Aceleración Internacional “Cybersecurity Ventures”, coorganizado por el Instituto Nacional de Ciberseguridad de España, S.A. (en adelante INCIBE), en colaboración con la Junta de Castilla y León, a través del Instituto para la Competitividad Empresarial de Castilla y León (antes ADE), y el Ayuntamiento de León a través del Instituto Leonés de Desarrollo, Formación y Empleo, SA (en adelante ILDEFE), según el Convenio de Colaboración firmado al efecto.

Objetivos del Programa de Aceleración:

- Incentivar el desarrollo de nuevas empresas de base tecnológica en el ámbito de la ciberseguridad.
- Apoyar al talento emprendedor en la maduración de sus proyectos empresariales en ciberseguridad a través de la formación, mentorización y networking con inversores y talento emprendedor.
- Contribuir al despliegue de la estrategia de ciberseguridad en España vinculándola con los retos en ciberseguridad contemplados en el Programa.
- Complementar la oferta de actividades promovidas por INCIBE como centro nacional de referencia en ciberseguridad.

SEGUNDA.- Participantes

La participación en el programa está reservada a empresas de reciente constitución (Start-Ups). de base tecnológica y especializada en ciberseguridad Sin embargo, es posible presentarse al programa de aceleración siempre que la empresa esté en proceso de constitución y ésta se haga efectiva antes s de la resolución del Director General de INCIBE con la clasificación de admitidos al proceso de aceleración, según lo recogido en la base octava de las presentes bases.

Las empresas participantes han de ser microempresas o pymes no cotizadas, constituidas en un periodo inferior a cinco años a la fecha de cierre de la presente convocatoria, que todavía no hayan distribuido beneficios ni surjan de una operación de concentración, .Deben estar legalmente constituidas en España y hallarse al corriente en el cumplimiento de obligaciones frente a la Seguridad Social y la Agencia Tributaria. A tales efectos, se considerará como fecha de constitución la que conste en la solicitud de alta en el censo de empresarios, profesionales y retenedores.

En el caso de presentase un promotor a título individual, deberá ser mayor de edad al momento de cierre de la convocatoria. En el caso de que el proyecto presentado resultara seleccionado, es condición necesaria para participar en el programa de aceleración la constitución de una empresa antes de la resolución del Director General de INCIBE con la clasificación de admitidos al proceso de aceleración, según lo recogido en la base octava de las presentes bases. La empresa constituida debe cumplir con los mismos requisitos exigidos para las empresas que se presentan como tales a la convocatoria.

Por cada empresa del programa de aceleración deberá participar por lo menos una persona que actuará como representante de la empresa. Adicionalmente, podrán participar hasta tres miembros del equipo promotor. Tanto el representante de la empresa

como el resto de las personas del equipo promotor deben identificarse como parte de la solicitud y deben ser todos mayores de edad al momento del cierre de la convocatoria.

Sin embargo, por limitaciones de espacio, sólo podrán asistir de manera simultánea a las actividades presenciales hasta dos personas por empresa.

TERCERA.- Propuestas y retos

Las solicitudes o propuestas al programa de aceleración las constituyen empresas o proyectos de empresas (en el caso de que no esté aún constituida como tal) que buscan desarrollar **nuevos negocios** en el ámbito de la Ciberseguridad, con productos o servicios innovadores orientados al mercado. Si bien la convocatoria es amplia abarcando todo tipo de negocios vinculados a la ciberseguridad, el programa busca incentivar que los proyectos aborden determinados retos previamente identificados. Las propuestas que se alineen con los desafíos planteados por estos retos y los aborden de manera explícita serán valoradas con una mayor puntación en el criterio “alineamiento”, tal como se explica más adelante en el apartado “Criterios y proceso de selección”.

Se identifican dos tipos de retos:

- Retos estratégicos
- Retos específicos de empresas

Los retos estratégicos se corresponden con retos identificados por organismos nacionales, europeos o internacionales e identifican oportunidades de negocio desde una perspectiva “top-down”. Para la definición de estos retos estratégicos se ha tomado como primera referencia el documento de “Tendencias en el Mercado de la Ciberseguridad”, publicado por INCIBE (Instituto Nacional de Ciberseguridad) en Julio 2016. Estos retos se han enriquecido con aportaciones escogidas de otros documentos de estrategia publicados por entidades de referencia internacional como “European Cyber Security Organization” (ECSO) o la agencia europea “European Union Agency for Network and Information Security” (ENISA).

Asimismo podrán incorporarse y publicarse retos específicos de empresas, entendidos como desafíos a los que se enfrentan empresas para el desarrollo e innovación en sus negocios. La integración de estos retos se basará en que constituyan una oportunidad de mercado para aquellos proponentes que los aborden a través de su participación en el programa de aceleración.

Los retos estratégicos y los retos específicos de empresas se publican en la página web de INCIBE https://www.incibe.es (apartado Programa de aceleración).y en el Anexo I a estas Bases.

CUARTA.- Plazos y forma de presentación de las solicitudes

Los candidatos deberán presentar su propuesta desde el día de su publicación hasta el cierre de la convocatoria el 10 de septiembre de 2017 a las 23:59 (CET). **No se admitirán solicitudes que se reciban fuera de este plazo, siendo excluidas del Programa.**

Las propuestas podrán presentarse a través de los siguientes canales:

- Correo electrónico en la dirección ventures@incibe.es con firma electrónica válida del representante legal de la empresa en el caso de Start Ups constituidas, o del promotor individual (firmas que serán validada en "valide.es").
- Por correo ordinario o mensajería, físicamente en la siguiente dirección:

  Avenida José Aguado 41
  Edificio INCIBE
  24005, León (España)
  Att. Cybersecurity Ventures

  Debiendo estar en INCIBE en la fecha límite de presentación de propuestas.
- A través de la plataforma F6S (plataforma de promoción del emprendimiento líder mundial) con firma electrónica válida del representante legal de la empresa en el caso de Start Ups constituidas, o del promotor individual (firmas que serán validada en "valide.es"). https://www.f6s.com/cybersecurityventuresapplication2017

Los solicitantes aportarán la información requerida utilizando el formulario de presentación de la propuesta que se encuentra disponible en el mismo portal Web de INCIBE y como Anexo a estas Bases.

QUINTA.- Contenido de las solicitudes o propuestas

Cada empresa participante (o promotor/a a título individual) puede presentar sólo una propuesta. En caso de existir múltiples propuestas, sólo se tomará en consideración la última recibida por cualquiera de los medios habilitados (plataforma web, correo electrónico o correo ordinario)

La propuesta puede presentarse en español o en inglés.

La entidad solicitante deberá enviar la siguiente documentación:

- Parte A: Información administrativa
- Parte B: Descripción del proyecto
- Parte C: Interés en el programa de aceleración

La **parte A** contiene la información administrativa sobre el proyecto y el representante de la propuesta.

La declaración jurada, debe ser firmada por el representante legal de la Start-Up, y en el caso de empresas no constituidas por un representante que designen. Además, esta declaración incluye la designación obligatoria de una persona concreta como contacto y deberá estar firmada por los integrantes del equipo. Dicha persona de contacto, que puede coincidir o no con el representante, lo será a todos los efectos: comunicaciones, recepción de premios y, en general, cualquier contacto que los promotores de las presentes bases consideren, pudiendo delegar en otro miembro del equipo ante la imposibilidad de atender las solicitudes por motivos debidamente justificados.

La información se debe introducir siguiendo el modelo a través de un conjunto de formularios en línea en el Sistema de Presentación de Propuesta Electrónica (https://www.f6s.com/cybersecurityventuresapplication2017), a través de correo electrónico ventures@incibe.es o físicamente en el edificio INCIBE (Avenida José Aguado nº 41. 24005, León).

La **parte A** debidamente cumplimentada y firmada, también debe incluir la siguiente documentación (original en caso de envío físico) o en documentos pdf firmados con firma electrónica válida (si se presenta por correo electrónico o Plataforma):

- **Si se trata de empresa constituida:**
  - Original o copia simple de la escritura de constitución o modificación inscrita, en su caso, en el Registro Mercantil, cuando este requisito fuera exigible conforme a la legislación mercantil que le sea aplicable. Si no lo fuere, escritura o documento de constitución, estatutos o acto fundacional, en el que constaren las normas por las que se regula su actividad, inscritos, en su caso, en el correspondiente Registro oficial.
  - Copia compulsada del CIF.
  - Deberá acreditarse la representación por cualquier medio válido en Derecho. Además deberá aportarse DNI del representante.
  - Certificaciones administrativas positivas, expedidas por el órgano competente, que acrediten que el beneficiario se encuentra al corriente en sus obligaciones tributarias y frente a la Seguridad Social.
  - Copia de la declaración censal de alta.

- **En caso de que el solicitante sean promotores a título individual en trámites de constitución de la empresa:**
  - Fotocopia compulsada del DNI en vigor o pasaporte, en caso de no ser de nacionalidad española, y justificante de residencia en territorio español (p. ej. volante de empadronamiento).

La **parte B** contiene la descripción del proyecto empresarial, identificando mercado, propuesta de valor, competencia, etc. siguiendo los apartados del modelo de presentación de solicitudes.

La **parte C** de la propuesta recoge el interés de la empresa o proyecto para participar en programa de aceleración, incluyendo las motivaciones del equipo y la alineación con los retos planteados. La parte C debe seguir los apartados del modelo de presentación de solicitudes.

SEXTA.-Aceptación de las Bases

La participación en el programa supone la aceptación íntegra e incondicional de estas Bases, sin salvedades ni condicionantes. Esto se atestiguará mediante declaración jurada incluida como parte de la solicitud que deberá estar firmada por el representante de la empresa y por el resto de miembros del equipo promotor.

En el caso de promotores a título individual que no hayan constituido la empresa en el momento de presentación de la solicitud de participación en el programa, habrán de utilizar el modelo de declaración específico y, una vez hayan constituido la empresa, deberán proceder a aportar la declaración y documentación exigida para empresas constituidas con anterioridad al comienzo del programa según lo previsto en la Base octava de las presentes bases. Los participantes serán los únicos responsables de la veracidad de las manifestaciones contenidas en la documentación presentada, pudiendo la organización verificar la veracidad en cualquier momento.

SÉPTIMA.-Subsanación de las solicitudes o propuestas

Durante el plazo de presentación de propuestas se habilitará un mecanismo de consulta de dudas sobre el proceso de presentación a través del email. Las consultas podrán ser enviadas a la dirección de correo electrónico ventures@incibe.es. Las respuestas a estas consultas serán publicadas en la página web de IINCIBE (apartado Programa de aceleración). No se responderá a consultas sobre un proyecto específico, sino que las consultas deben ser genéricas sobre el proceso de solicitud.

Al terminar el plazo de presentación de propuestas, los solicitantes recibirán una comunicación por correo electrónico confirmando la recepción de la propuesta.

Finalizado el plazo de presentación de solicitudes la Comisión de Seguimiento examinará la documentación aportada por los solicitantes con el fin de verificar el cumplimiento de los requisitos establecidos en estas bases. Finalizada la verificación, el resultado se plasmará en un acta que se publicará en la página web de INCIBE y se notificará individualmente por correo electrónico, y que contendrá:

- Listado de no admitidos: por haberse recibido su solicitud fuera de plazo o a través de canales no autorizados en estas Bases.
- Listado provisional de admitidos:
  - Admitidos que han acreditado debidamente el cumplimiento de todos los requisitos.
  - Admitidos que habiendo acreditado el cumplimiento de los requisitos por tratarse de promotores individuales queda pendiente su admisión definitiva a la presentación de la documentación que se exige a las empresas constituidas conforme a estas Bases.
  - Admitidos que han de subsanar la documentación presentada por no haber quedado acreditados todos los requisitos de documentación establecidos en estas Bases con indicación de la documentación a subsanar o aclaraciones a realizar.

Los solicitantes dispondrán de tres días hábiles desde la notificación de INCIBE para la subsanación de dichos defectos. En caso de no subsanarse en tiempo y forma, las propuestas serán excluidas del Programa.

Una vez finalizado el plazo de subsanación, y analizada la documentación recibida durante el mismo, la Comisión de Seguimiento elevará acta propuesta al Director General de INCIBE quien resolverá sobre la admisión y exclusión definitiva de los solicitantes y su envío al Comité evaluador a los efectos de clasificar y de seleccionar las que participarán en el Programa. La admisión de los promotores individuales quedará condicionada a su constitución como empresas en los términos previstos en estas Bases.

OCTAVA.-Proceso de selección

Las propuestas admitidas serán evaluadas por un comité evaluador independiente que será nombrado por la Comisión de seguimiento de estas Bases mediante acto al efecto.

Dicha Comisión de Seguimiento estará formada por dos representantes de INCIBE, un representante del Instituto para la Competitividad Empresarial de Castilla y León (antes ADE) y un representante de ILDEFE, que se constituirá con la firma de estas Bases, por designación de los representantes de las tres entidades.

La Comisión de Seguimiento con el asesoramiento del comité evaluador, pre-seleccionará hasta 25 de las propuestas presentadas conforme a los criterios recogidos en la Base novena.

Las propuestas seleccionadas serán invitadas a una entrevista presencial. Como resultado de dicha entrevista el Comité evaluador elaborará una propuesta de clasificación de la que se seleccionarán los 15 mejores proyectos que participarán presencialmente en un pitch en el 11 ENISE que se celebrará en León los días 24 y 25 de octubre de 2017, donde se preseleccionarán los 10 proyectos que pasan al programa de aceleración, más los 5 proyectos siguientes que serán mantenidos en reserva y que serán convocados en caso de renuncia de alguno de los proyectos seleccionados, o por falta de justificación de los requisitos exigidos de las preseleccionadas.

La clasificación del Comité deberá ser validada por la Comisión de Seguimiento que aprobará la **propuesta provisional** de clasificación y publicará la misma en la web de INCIBE. En el caso de que alguno de 10 primeros proyectos sean proyectos presentados por promotores individuales, en el mismo acto la Comisión requerirá la presentación de la documentación acreditativa de la constitución de empresa, así como la documentación exigida en estas Bases a empresas constituidas con un plazo de 10 días hábiles para su justificación.

Finalizado este plazo, la Comisión de seguimiento se reunirá para revisar la documentación presentada, y acordará:

- O bien la exclusión de la propuesta por no haber acreditado la constitución como empresa, y nueva propuesta provisional de clasificación conforme a la lista de espera, hasta agotarse la misma.
- O en el caso de haberse acreditado la constitución como empresa elevará propuesta definitiva al Director General con los 10 proyectos clasificados al programa de aceleración.

Finalizado este proceso se dictará resolución por el Director General que acordará la clasificación definitiva y los 10 proyectos seleccionados, así como en su caso la lista de reserva notificando la resolución a todos los participantes y publicándola en la página web de INCIBE

La siguiente tabla resume las fechas importantes para la presentación y selección de proyectos:

Hito	Método	Fechas estimadas
Inicio registro y recepción de propuestas	Vía web / email / correo ordinario	11-jul-17
Registro y recepción de propuestas	Vía web / email / correo ordinario	10-sep-17
Periodo de subsanación	Conforme al acta de la Comisión de Seguimiento	11/15-sep-17
Pre-selección de hasta 25 proyectos finalistas		04-oct-17
Entrevista personal con el jurado y proceso de preselección de 15 proyectos.		09/17-oct-17

Presentación de los proyectos y preselección de los 10 seleccionados y 5 reservas	Presencial / ENISE	A partir del 24-oct-17

NOVENA.-Proceso de evaluación y criterios

Las propuestas serán evaluadas por un comité evaluador independiente formado por expertos.

Todo el proceso de evaluación se rige por estos principios:

- Independencia: La evaluación se realiza de manera imparcial teniendo sólo en cuenta los méritos de los proyectos presentados, independientemente del origen o identidad de los solicitantes. En caso de conflicto de interés el evaluador debe abstenerse de evaluar ese proyecto.
- Confidencialidad: Los evaluadores se mantendrán anónimos (su identidad es desconocida para los solicitantes) y también firmarán una declaración de confidencialidad con el compromiso de no revelar a ningún tercero ningún detalle de la propuesta ni durante la evaluación ni posteriormente.
- Equidad: Cada propuesta es evaluada por al menos dos evaluadores diferentes.

La evaluación se realizará analizando los siguientes criterios:

- Madurez del proyecto (peso = 25%)
- Impacto del proyecto (peso = 25%)
- Motivaciones y aprovechamiento del programa de aceleración (peso = 30%)
- Alineación con los retos planteados (peso = 20%)

Cada uno de los criterios contribuye con un peso diferente en la valoración total, según se indica. Los criterios de madurez e impacto analizan fundamentalmente la parte B de la propuesta, mientras que el criterio de alineamiento con los objetivos del programa de aceleración se basa fundamentalmente en el análisis de la parte C.

Los elementos que cada criterio tiene en cuenta se explican en la siguiente tabla:

Criterio	Explicación: elementos que se tienen en cuenta para la valoración del criterio	Peso y umbral mínimo
Madurez del proyecto	■ Mercado: Identificado, validado y dimensionado. Canales de comercialización identificados ■ Tecnología: Desarrollada, validada, eficacia demostrada. ■ Rentabilidad: Demostrada, avalada con evidencias. Socios identificados. ■ Ventaja competitiva: Soportada en evidencias (patentes, protección, etc.). ■ Equipo: Identificado, comprometido y completo.	peso = 25%
Impacto del proyecto	■ Mercado: Grande y creciente, disruptivo, mercado global, canales internacionales. ■ Tecnología: Rupturista, innovadora. ■ Rentabilidad: Creciente, exponencial. ■ Ventaja competitiva: Diferenciación contundente respecto de competidores. Ventana de oportunidad sostenida en el tiempo.	peso = 25% umbral = 3

Criterio	Explicación: elementos que se tienen en cuenta para la valoración del criterio	Peso y umbral mínimo
	■ Equipo: capacitado, multidisciplinar, internacional, atractivo.	
Motivaciones y aprovechamiento del programa de aceleración	■ Motivación: Motivaciones del equipo promotor para su participación en el programa de aceleración. ¿De qué manera piensan aprovechar el programa? ¿Por qué creen que su proyecto debe ser apoyado?	peso = 30%
Alineación con los retos planteados	■ Alineación con los retos del programa de aceleración : Valoración de la medida en la cual el proyecto aborda a alguno de los retos planteados en la convocatoria (ya sean estratégicos o específicos de empresas)	peso = 20%

Cada criterio es evaluado con una puntuación de 0 a 5 según la siguiente escala:

- **0 – No abordado:** La propuesta no aborda el criterio o no se puede juzgar debido a la falta de información o información incompleta;
- **1 – Muy pobre:** El criterio se aborda de manera superficial o inadecuada, o hay serias debilidades inherentes;
- **2 – Pobre:** Aunque la propuesta aborda el criterio, hay algunas debilidades significativas
- **3 – Suficiente:** La propuesta aborda suficientemente el criterio, aunque pueden existir amplios márgenes de mejora
- **4 - Muy bien:** La propuesta aborda muy bien el criterio, aunque todavía son posibles algunas mejoras.
- **5 – Excelente:** La propuesta aborda con éxito todos los aspectos relevantes del criterio en cuestión. Cualquier deficiencia es menor.

El programa de aceleración pone el énfasis en apoyar proyectos de alto impacto, por esa razón el único criterio que requiere un umbral mínimo es el de impacto del proyecto, que debe estar valorado al menos un 3 (suficiente) y, de no alcanzar el umbral mínimo solicitado, la propuesta no será admitida al proceso de aceleración. No hay umbrales mínimos para el resto de criterios.

A partir del promedio de las puntuaciones de los evaluadores, se elaborará una clasificación de todas las propuestas. En caso de empate, se tendrán en cuenta los valores obtenidos en los criterios individuales priorizando en el orden: 1- Motivaciones, 2- Impacto, 3- Madurez y 4- Alineación. Si persistiera el empate, la decisión recaerá en la Comisión de Seguimiento. El Comité evaluador pre-seleccionará conforme a estos criterios hasta 25 de ellas que serán invitadas a una entrevista presencial. Como resultado de dicha entrevista se elaborará una clasificación de la que se seleccionarán los 10 primeros proyectos que participarán en el programa de aceleración, más los 5 proyectos siguientes que serán mantenidos en reserva y que serán convocados en caso de abandono de alguno de los proyectos seleccionados.

Todo el proceso de selección será tutelado por la Comisión de seguimiento, que será la responsable de elevar la propuesta a la Dirección General de INCIBE quien acordará la relación de proyectos seleccionados para la participación gratuita en el Programa ***Cybersecurity Ventures.***

DÉCIMA.-Desarrollo del Programa de Aceleración

El programa de aceleración tiene como objetivo el desarrollo de las empresas preparándolas para ser atractivas como inversiones y para desarrollar su modelo de negocio y propuesta de valor hacia los clientes. Con este fin, el programa de aceleración desarrolla actividades tanto en común para todos los proyectos que participan del programa, como específicas para cada uno de los proyectos. Dichas actividades se estructuran de la siguiente manera:

Hoja de ruta individualizada: Consiste en un análisis individualizado de cada proyecto y en la definición conjunta de una hoja de ruta individualizada que establecerá el plan de aceleración e identificará una serie de hitos para crear valor en la empresa.

Las horas detalladas a continuación han de tomarse como **mínimas.**

Formación (60 horas): Consiste en una serie de seminarios focalizados o píldoras formativas orientados a desarrollar competencias en los siguientes ámbitos:

- Tu negocio: formación orientada a desarrollar competencias para concebir y dar forma a un negocio de base tecnológica.
- El ecosistema emprendedor: píldoras formativas donde el foco está en desarrollar la relación de la empresa con otros actores del ecosistema, como inversores, clientes, canales, etc.
- Tus competencias personales: formación orientada a desarrollar las competencias personales como emprendedor, ya sea en la gestión, en las relaciones humanas, en presentaciones en público, etc.

Esta formación se completará con otro tipo de sesiones, como presentación de casos por parte de otros emprendedores (10 horas) y conferencias inspiradoras por parte de personas de relevancia internacional: leadership series (3 horas), etc.

Mentorización (58 horas): Consiste en una orientación para el desarrollo de la idea de negocio. Cada proyecto contará con un mentor de referencia que coordinará el apoyo de otros mentores específicos en distintos ámbitos según las necesidades.

Networking con inversores y emprendedores (10 horas): Consiste en varias sesiones de trabajo con inversores business angels, capital riesgo, corporate Venturing, etc. También se facilitará a los equipos promotores encuentros de captación de talento para favorecer el desarrollo de sus proyectos.

Demo Day: Es una jornada en la que los promotores de las oportunidades aceleradas presentarán sus proyectos empresariales. La fecha para la realización, así como la ubicación, se decidirá en su momento por la Comisión de Seguimiento y será trasladada a los proyectos participantes en cuando esté definida.

Las actuaciones formativas previstas en el Programa de Aceleración se llevarán a cabo coordinadamente y en colaboración entre el INCIBE, el Instituto para la Competitividad Empresarial de Castilla y León (antes ADE) y el ILDEFE, en los espacios de emprendimiento que el Instituto para la Competitividad Empresarial de Castilla y León (antes ADE) pondrá a disposición de los emprendedores, en el Parque Tecnológico de León, Edificio de Usos Comunes (Calle Julia Morros, 1, de Armunia - León), en los términos que normativamente corresponda.

La siguiente tabla resume los hitos y fechas aproximadas del desarrollo del programa de aceleración.

Hito	Formato	Fechas aproximadas
Definición de la hoja de ruta individualizada	Presencial / remoto	25-oct/17-nov-17
Formación Presencial Mentorización – Networking con inversores	Presencial / remoto	20-nov/28-feb-18
Demo Day	Presencial	feb-18
Final del proceso de aceleración	Presencial	feb-18

UNDÉCIMA.-Compromisos para la participación en el Programa

Los participantes seleccionados para el programa de aceleración se comprometen a cumplir íntegramente las actividades que lo componen (participación en sesiones formativas, actividades de mentoring, etc.). El primer hito a cumplir es desarrollar y concretar conjuntamente con el mentor asignado la "hoja de ruta individualizada" que contendrá un plan de aceleración e identificará una serie de actuaciones de creación de valor que se perseguirán durante el desarrollo del programa. Durante el desarrollo del programa de aceleración se requiere **una participación mínima del 80% de las horas** de alguna persona del equipo promotor en el conjunto de sesiones y actividades incluidas en la hoja de ruta individualizada (tomando como referencia las 141 horas detalladas en la base novena). La participación no se limita a la asistencia, sino que también comprende la realización del trabajo necesario para cumplir con los hitos que se acuerden como parte del plan.

La falta de cumplimiento de alguno o todos estos compromisos darán lugar a la exclusión de la Start-Up del programa de aceleración, no pudiendo acceder al resto de actividades ni ser merecedor de los premios previstos. Los organizadores se reservan el derecho a la solicitar la devolución de los importes recibidos. La decisión sobre la exclusión será tomada por la Comisión de Seguimiento del programa de aceleración.

Si la exclusión de una Start-Up sucede durante el primer mes del programa, dedicado al desarrollo de la hoja de ruta individualizada, entonces será posible la sustitución de la start-up por otra de la lista de reserva. La sustitución se hará por estricto orden de clasificación resultante del proceso de selección y estará a cargo de la Comisión de Seguimiento.

DUODÉCIMA.- Premios

Los proyectos seleccionados reciben como premio en especie la participación en forma gratuita en el Programa de Aceleración ***Cybersecurity Ventures*.** Además de ello, el programa de aceleración está dotado con 120.000 euros en premios en metálico para ayudar al impulso de los proyectos empresariales seleccionados.

Los premios se repartirán de la siguiente manera:

1. Cada una de las 10 empresas seleccionadas que completen satisfactoriamente la fase de definición de la hoja de ruta individualizada y se comprometan a realizar el programa de aceleración recibirán 2.000 euros al finalizar dicha fase, previa resolución del Director General de INCIBE.

2. Cada una de las 10 empresas que completen satisfactoriamente todo el programa de aceleración hasta la presentación en el Demo Day y cumpliendo el plan de aceleración, es decir, aprovechamiento de la formación presencial en León y participación mínima del 80% en el conjunto de sesiones y actividades del plan y realización del trabajo necesario para cumplir los hitos que se acuerden como parte del plan. Recibirán 4.000 euros al cumplimentar la presentación en el Demo Day, previa resolución del Director General de INCIBE.

Como resultado de la participación en el programa de aceleración y la presentación en el Demo Day, se elaborará una clasificación de los 3 mejores proyectos. El jurado para el otorgamiento de estos premios estará compuesto por personas relevantes del ecosistema emprendedor en ciberseguridad incluyendo representantes de INCIBE, de la Junta de Castilla y León, e ILDEFE, a propuesta de la Comisión de Seguimiento del Convenio de Colaboración para la aceleración de proyectos emprendedores.
Este jurado analizará el aprovechamiento del proceso de aceleración y la presentación final en el Demo Day con los siguientes pesos:

- Memoria final, aprovechamiento y evolución del proyecto durante el programa de aceleración (peso = 50%)
- Presentación final del proyecto en el Demo Day: innovación y ventaja competitiva de la solución, identificación del nicho de mercado, modelo de negocio y proyecciones, tracción actual y plan a corto plazo, adecuación del equipo a la consecución de hitos (peso = 50%).

A propuesta de este Jurado, la Comisión de Seguimiento elevará propuesta a la Dirección General de INCIBE, que acordará la distribución de los 60.000 euros en premios de la siguiente manera:

- 1er premio: 28.000€
- 2do premio: 18.000€
- 3er premio: 14.000€

Es decir, el programa de aceleración entregará a las empresas un total de 120.000 euros en premios en metálico distribuidos como sigue:

- 1ª empresa clasificada: 34.000€
- 2ª empresa clasificada: 24.000€
- 3ª empresa clasificada: 20.000€
- De 4ª a 10ª empresa clasificada: 6.000€

Con carácter previo a la resolución del Director General que acuerde la entrega de estos premios, en metálico se exigirá al premiado la presentación de los certificados positivos de la Agencia Estatal de Administración tributaria y de la Tesorería General de la Seguridad Social de cumplimiento con sus obligaciones así como el Anexo III de datos bancarios.

El premio se entregará a la entidad legalmente constituida del proyecto elegido y al importe total se retraerán en su caso los impuestos según la legislación vigente.

En caso de renuncia o abandono del programa, o en el supuesto de falta de aprovechamiento por parte de los seleccionados en los términos previstos en estas Bases, la Dirección General de INCIBE a propuesta de la Comisión de Seguimiento exigirá la devolución de los fondos recibidos así como los intereses de demora

devengados. El interés de demora aplicable será el interés legal del dinero incrementado en un 25 por ciento, salvo que la Ley de Presupuestos Generales del Estado establezca otro diferente, y se aplicará desde la fecha en que conste en contabilidad la realización del pago de la ayuda hasta la fecha en que se acuerde el reintegro

DÉCIMO TERCERA.- Régimen jurídico

Normativa de aplicación y jurisdicción

Las presentes Bases se rigen por la legislación española.

En todo lo no previsto en estas Bases, se estará a lo establecido en la Ley 38/2003, de 17 de noviembre, General de Subvenciones, en lo que resulte de aplicación a las Sociedades Públicas.

La presente modalidad de ayudas se establece al amparo del Reglamento (UE) nº 1407/2013 de la Comisión, de 18 de diciembre de 2013, relativo a la aplicación de los artículos 107 y 108 del Tratado de funcionamiento de la Unión Europea a las ayudas de *minimis* (DO L 352, de 24 de diciembre de 2013) por lo que la empresa beneficiaria no podrá exceder el límite de 200.000 euros de ayudas percibidas en un periodo de tres años (importe total de ayudas de *minimis* del ejercicio fiscal actual y los dos anteriores). A tal efecto la Pyme queda obligada a comunicar a las entidades organizadoras la obtención de cualquier ayuda de *minimis* durante tres ejercicios fiscales.

Las ayudas de *minimis* son aquellas que por su importe reducido no se considera que afecten a la competencia en ámbito comunitario y por ello están exentas de la obligación de notificación previa y también comunicación a posteriori a la Comisión Europea conforme a lo previsto en el artículo 3.1 del Reglamento (UE) número 1407/2013 de la Comisión que exime de la notificación del art. 108.3 del Tratado UE.

Para la calificación como Pyme, será de aplicación a estas Bases la Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas.

La presentación de propuestas a este programa, supone la renuncia expresa a cualquier fuero y legislación que pudiera corresponderles, sometiéndose expresamente a la ley española y a la jurisdicción de los juzgados y tribunales de León.

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 programa que deberá ajustarse a lo previsto en estas Bases.

Órgano competente

En el marco de estas Bases, INCIBE actuará como impulsor de esta iniciativa. De igual forma, INCIBE coordinará la total transparencia del proceso de publicación de la convocatoria, presentación de solicitudes, así como la resolución del procedimiento y el seguimiento y pago de los premios.

Cuantas resoluciones se estimen necesarias para la consecución del programa de ayudas se llevarán a cabo por la Dirección General de INCIBE, previa propuesta de la Comisión de Seguimiento que se constituirá con la publicación de estas Bases. Dicha Comisión estará integrada por dos miembros de INCIBE (Instituto Nacional de Ciberseguridad de España, S.A.), un miembro del Instituto para la Competitividad

Empresarial de Castilla y León (antes ADE), y uno de ILDEFE (Instituto Leonés de Desarrollo, Formación y Empleo, S.A.), y si fuera necesario expertos externos Su funcionamiento se determinará por las partes en la primera reunión de común acuerdo conforme a las normas de funcionamiento de los órganos colegiados (LRJSP 40/2015).

La Comisión de Evaluación, será la encargada de elevar la propuesta de selección y de reservas, a la Dirección General de INCIBE. También corresponde a esta Comisión la propuesta de premios regulados en la Base duodécima, así como la propuesta de reintegro o la propuesta ante cualquier otra situación de hecho o de derecho que determine una resolución por parte del Director General de INCIBE.

Publicidad y comunicaciones

Las presentes bases junto con sus anexos serán publicadas en el perfil del contratante de la web de INCIBE.

Todas las notificaciones que se deban realizar en el marco del programa 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 beneficiarias deberán tener actualizado el e-mail de contacto, que además deberá corresponder con la persona que la entidad beneficiaria haya designado a estos efectos.

Serán publicadas en el perfil del contratante de la web la listas de admitidos, la lista de excluidos, y la lista definitiva de beneficiarios.

Para cualquier aclaración y reclamación sobre el programa pueden dirigirse a la siguiente dirección de correo electrónico: ventures@incibe.es.

Confidencialidad

Las entidades organizadoras del programa, se comprometen a mantener la confidencialidad de las ideas/proyectos que se presenten y desarrollen a lo largo del programa y sobre los propios candidatos, con independencia de que éstos puedan ser o no finalmente seleccionados.

Las entidades organizadoras garantizan la confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión de esta convocatoria, especialmente los de carácter personal y de carácter técnico de los proyectos, 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 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 de los eventos, sin perjuicio de la obligación de INCIBE de garantizar una adecuada publicidad de las ayudas.

Protección de datos de carácter personal

Esa información se almacenará en un fichero, cuyo titular es INCIBE, “Programa de excelencia en Ciberseguridad” cuya finalidad es la gestión de actividades de formación, capacitación profesional y promoción del talento enmarcadas dentro del programa de excelencia en ciberseguridad, frente a quien el titular podrá ejercer sus derechos de acceso, rectificación, cancelación u oposición, en los términos fijados en la normativa de protección de datos de carácter personal, mediante carta a INCIBE, Avenida José Aguado nº 41 de León o por correo electrónico a calidad@incibe.es

Los candidatos autorizan que los datos obtenidos a partir de su participación en el Programa se utilicen con la finalidad de: realizar el proceso de inscripción, participación, valoración de las propuestas y, en caso de resultar seleccionados, desarrollo del programa de aceleración. Además el participante también consiente en que la organización almacene sus datos personales con la finalidad de reproducir su intervención, y para la comunicación pública de su elección como propuesta seleccionada.

Propiedad intelectual

El participante acepta que nada en estas bases le autoriza o da derecho a utilizar las marcas y logos de INCIBE sin su autorización.

La organización no reclama propiedad alguna sobre la información aportada por el participante o cualquier propiedad intelectual que pueda contener. El participante no cede a los organizadores derechos a ninguna patente o propuesta de patente relacionada con la información, tecnología, datos, etc., descritos en la propuesta de participación

Los aspectos publicables de las ideas y proyectos seleccionados (resumen del proyecto), 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.

Cesión de derechos de imagen

Los participantes, mediante la aceptación de estas bases, ceden en exclusiva y de forma gratuita a INCIBE el uso de su imagen personal, que pudiera ser captada durante su participación en el programa.

Responsabilidad

La organización no será responsable por ningún daño, pérdida, coste, perjuicio, reclamaciones, etc. en que los participantes pudieran incurrir o pudieran sufrir a resultas de la presentación de sus candidaturas.

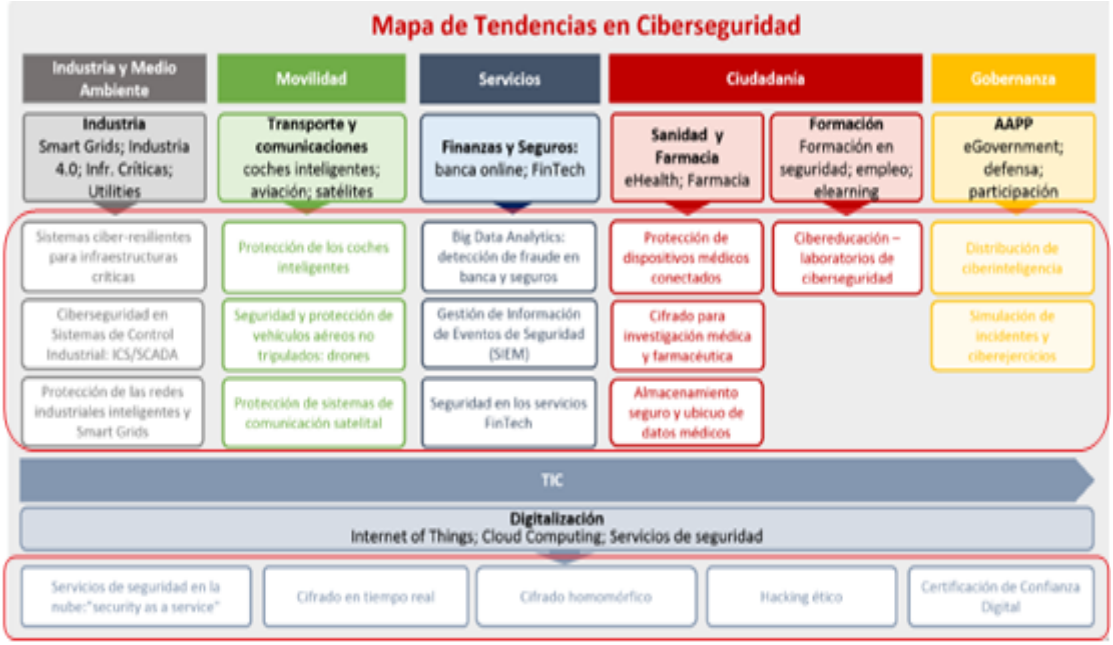
Adicionalmente, no alcanzará responsabilidad alguna a la entidad concedente del Premio en el supuesto de que la idea cuya explotación se propone o cualquiera de los documentos presentados por el participante vulnere de algún modo los derechos de terceros en materia de propiedad intelectual, industrial o de cualquier otra índole.

León, 11 de julio de 2017
DIRECTOR GENERAL DEL INSTITUTO NACIONAL DE CIBERSEGURIDAD DE ESPAÑA, S.A. (INCIBE)

ANEXO I RETOS ESTRATÉGICOS DEL PROGRAMA DE ACELERACIÓN

RETOS ESTRATÉGICOS:

La figura 1 presenta los retos estratégicos en ciberseguridad correspondiéndose con las tendencias identificadas en el documento de "Tendencias en el Mercado de la Ciberseguridad". Se puede consultar una explicación más detallada de cada uno de los retos en el Anexo 1 directamente accediendo al citado documento a través de la web de INCIBE (www.incibe.es)



Teniendo en cuenta la cadena de valor de la ciberseguridad y su impacto en ciudadanos, empresas y Administraciones Públicas, se ha diseñado un mapa de tendencias de demanda en el que se identifican 20 tendencias globales en ciberseguridad catalogadas en torno a 6 sectores de actividad.

Sector Industrial y Medio Ambiente.

- Sistemas ciber-resilientes para Infraestructuras Críticas. La destrucción o perturbación de infraestructuras estratégicas cuyo funcionamiento es indispensable tendría graves consecuencias sobre servicios esenciales, por lo que requieren de sistemas diseñados para hacer frente a una crisis de seguridad sin que su actividad se vea afectada.
- Ciberseguridad en Sistemas de Control Industrial: ICS/SCADA. La complejidad de los sistemas ICS/SCADA radica principalmente en su naturaleza multidisciplinar y aplicable a multitud de sectores. Ello justifica la necesidad de implantar altos niveles de ciberseguridad en los sistemas SCADA.
- Protección de las redes industriales inteligentes y Smart Grids. La necesidad de protección de las redes de sensores industriales radica en medidas de seguridad tales como protocolos de autenticación, cifrado de conexiones M2M y eliminación de redundancias.

Sector Movilidad

- Protección de vehículos inteligentes. La protección de vehículos inteligentes hace referencia a la seguridad de los sistemas de control de vehículos interconectados y de vehículos terrestres autónomos, así como de los sistemas inteligentes que interaccionan con ellos por medio de redes de comunicaciones específicas. Estas redes deben estar protegidas contra bloqueos de la señal, ataques de denegación de servicio y transmisión de datos falsos a los vehículos terrestres conectados y a sus conductores.
- Seguridad y protección de vehículos aéreos no tripulados: drones. El desarrollo y uso de drones supone un gran reto para la seguridad. Desde el punto de vista de la ciberseguridad, estos dispositivos están expuestos a riesgos de pérdida de confidencialidad, integridad y disponibilidad de los datos.
- Protección de sistemas de comunicación vía satélite. Las Comunicaciones por Satélite juegan un papel vital en el sistema de telecomunicaciones global. Estos sistemas presentan distintas vulnerabilidades que podrían permitir a atacantes remotos inutilizar por completo los dispositivos. Entre los sistemas afectados se podrían encontrar múltiples sistemas y servicios críticos, como: servicios de emergencia, militares, aviones, barcos, sistemas industriales, etc.

Sector Economía

- Big Data Analytics: detección de fraude en banca y seguros. El uso de Big Data Analytics en el sector bancario y de seguros, permite entre otras la detección y prevención del fraude en tiempo real, reduciendo los costes de monitorización e investigación de incidentes y por tanto reduciendo las pérdidas derivadas de actividades fraudulentas.
- Gestión de Información de Eventos de Seguridad (SIEM). Se basa en la detección de amenazas y respuesta a incidentes de seguridad a través de la obtención en tiempo real de eventos de seguridad y su análisis histórico, a partir de una amplia variedad de fuentes de eventos y datos contextuales.
- Seguridad en los servicios Fintech. La seguridad en servicios Fintech se basa en el desarrollo de nuevas soluciones de protección de sistemas o aplicaciones de pago online, sistemas de m-commerce o comercio móvil, dispositivos de tecnología NFC, lectores de tarjetas para móviles, etc., basadas en la autenticación de usuario y soluciones de prevención de fraude.

Sector Ciudadanía

- Protección de dispositivos médicos conectados. Estos dispositivos pueden exponer a los pacientes y a las organizaciones de atención de la salud, a los riesgos de la seguridad y la protección. Todos estos dispositivos interconectados en una red necesitan asegurar la confidencialidad, integridad y control de los mismos, especialmente, en aquellos cuyo software no está personalizado para su uso.
- Cifrado para investigación médica y farmacéutica. La tendencia de seguridad de datos médicos avanza hacia un cifrado apto para hacer coincidir las fuentes de información de múltiples centros médicos, que están cifrados con claves diferentes, sin descifrado de la información, salvaguardando la confidencialidad en la información de los pacientes.

- Almacenamiento seguro y ubicuo de datos médicos. La sensibilidad de la información de los pacientes requiere no sólo de un sistema de almacenamiento cifrado, sino de un mecanismo de transferencia seguro, garantizando que la ubicuidad de los datos personales y clínicos de los pacientes no pone en peligro su confidencialidad.
- Cibereducación – Laboratorios de seguridad. La integración de la educación con la tecnología y la ciberseguridad converge en lo que se reconoce como cibereducación. Se trata de una modalidad educativa que formula la enseñanza a partir de diferentes competencias y disciplinas, tales como: interactuación, retroalimentación, gamificación, simulación, etc. aplicadas a la formación en ciberseguridad.

Sector Gobernanza

- Distribución de ciberinteligencia. Se trata de un modelo basado en el intercambio de información entre organismos, públicos y privados, proveniente del análisis de ciberamenazas con el objetivo de mejorar y agilizar la detección y actuación ante las amenazas en ciberseguridad.
- Simulación de incidentes y ciberejercicios. Los sistemas de simulación de escenarios e incidentes se basan en la utilización de entornos de entrenamiento, que ponen a prueba la capacidad tecnológica y de reacción de las herramientas y recursos de una organización. Los ciberejercicios, por su parte, permiten evaluar el estado de preparación de los participantes frente a crisis de origen cibernético.

Sector TIC

- Servicios de seguridad en la nube: “security as a service”. Estos servicios son generalmente modelos de outsourcing de la administración de la seguridad, que se aprovechan de la escalabilidad del modelo de Cloud Computing permitiendo a las organizaciones dimensionar los esfuerzos a su capacidad actual.
- Cifrado en tiempo real. Se trata de un mecanismo de protección de la seguridad de los datos en las transacciones electrónicas en el que los datos se cifran antes de ser almacenados y se descifran al descargarse, previamente a su utilización. Este tipo de cifrado permanece en segundo plano ante el usuario.
- Cifrado homomórfico. Esta tendencia de cifrado permite que la información que se codifique pueda ser compartida con terceras partes y ser utilizada en cálculos y procesos computacionales, sin que los sistemas implicados puedan interpretar dicha información pero sí ofrecer un resultado no cifrado a esos cálculos y procesos.
- Hacking ético. Se basa en la búsqueda de vulnerabilidades mediante la utilización de pruebas de penetración o “pentest” en las redes de una organización con el objetivo de prevenir posibles fallos de seguridad, mitigar el impacto provocado por cualquier incidente de seguridad, priorizar riesgos y verificar el cumplimiento normativo.
- Certificado de confianza digital. Consiste en comprobar, materializar y dar visibilidad el nivel de ciberseguridad que implementa un proveedor en un servicio determinado, es decir, la emisión de sellos de confianza digital que valoran objetivamente las medidas de seguridad integradas por el proveedor de servicios.

RETOS ESPECÍFICOS:

Retos propuestos por empresas

Generación de mecanismos de impacto de concienciación en Ciberseguridad

Plataforma que integre diferentes elementos que permitan evaluar el nivel de conciencia en términos de Ciberseguridad de una organización así como hacer un seguimiento de dicho nivel tras diversas acciones de concienciación.

La plataforma debería ser capaz de simular campañas, extremo a extremo, con los ataques más comunes enfocados hacia el usuario interno, como puede ser el phishing o malware, empleando técnicas y herramientas de ingeniería social y generando patrones de evasión contra los principales controles de seguridad con los que las compañías cuentan. Así mismo, debe medir la efectividad de dichas campañas, proponer modelos de concienciación basados en el resultado obtenido y establecer un modelo de seguimiento que mida la evolución en términos de concienciación de la organización a través de distintas oleadas/campañas.

Nuevas herramientas, sistemas y servicios basados en la normativa PSD2

Herramientas o aplicaciones que permitan iniciar pagos, basadas en la normativa PSD2. Sistemas de autenticación que puedan cumplir con PSD2 para firmar transacciones.

Nuevos métodos de pago y ticketing basados en movilidad y/o geolocalización

Nuevos servicios de pago y ticketing, en base a la ubicación del usuario, distancia recorrida, etc. considerando los requerimientos de seguridad en las transacciones y privacidad de los usuarios.

Protección y securización de Sistemas de Control Industrial (ICS) empleados en infraestructuras críticas del sector eléctrico

Adaptación de técnicas y herramientas de Ciberseguridad provenientes de sistemas IT sobre sistemas OT, definición de casos de pruebas específicos para estos equipos industriales y pentesting sobre equipos reales bajo un entorno de test.

Prevención de ataques DDos sobre los servidores DNS de las empresas con servicios abiertos al público

Las empresas que tratan datos sensibles y ofrecen servicios públicos en Internet, están expuestas a ataques DoS (Denial of Service). Si bien se hace hincapié en la protección de las entradas de servicios de las aplicaciones, los servidores DNS también están expuestos y son un objetivo de dichos ataques.

Seguridad en Internet of Things (IoT)

Medidas de seguridad para la securización de los dispositivos y las comunicaciones del Internet de las cosas (IoT): Soluciones perimetrales, mejora de los actuales estándares y protocolos, así como la creación de nuevos estándares específicos.

Copia cifrada de datos en la nube, manteniendo los datos críticos de los clientes a salvo de cualquier tipo de ataque / pérdida

Mecanismo que permita realizar copias de datos en la nube, de forma asíncrona y utilizando métodos que aseguren la seguridad y autenticidad de la información. Se debe indicar los requisitos de comunicaciones, ancho de banda o velocidad de transferencia que aseguren que la información ha sido copiada/transferida correctamente y que la copia se mantiene inalterada. Los datos deben estar encriptados desde el origen y las claves de encriptado deben ser conocidas sólo por el Cliente final.

Robot de Ciberseguridad, dando al CISO de las empresas información en tiempo real y de forma continuada de lo que está pasando en su landscape de TI

Aplicación basada en Inteligencia Artificial que permita gestionar la información/eventos/logs generados por los diferentes sistemas de seguridad y puestos de trabajo, cuyo motor sea capaz de analizar y tomar decisiones de manera preventiva, generando, además, informes y estadísticas precisas sobre las vulnerabilidades detectadas en tiempo real y las acciones tomadas con carácter preventivo. La aplicación debería contar con:

Motor de lógica preventiva basada en IA; detectar ataques de forma temprana, lanzar acciones correctivas (i.e. cerrar puertos) y emitir informes de actividades de remediación.

Mecanismo de consolidación, normalización y carga de eventos de seguridad (logs, SIEM, etc.) para alimentar la BBDD de eventos de seguridad.

Identificación de las amenazas de la compañía

Al estilo de los threat map o cyber attack como los que los fabricantes de antimalware o elementos de seguridad perimetral tienen publicados en Internet, pero con un ámbito diferente; en este caso el de la empresa donde se instale. Se debe identificar y representar de una forma visual los eventos de seguridad que se estén produciendo en la compañía, pudiéndose seleccionar tipos de ataques (malware, DDoS, inyección de código, etc.), por localizaciones (país, sede,..) u otros criterios.

Identificación y gestión continúa de la exposición a vulnerabilidades de los sistemas en producción

Los sistemas en producción, son difíciles de analizar y más cuando tienen que estar 24 horas operativos. La compañía requiere simular mediante un “equipo victima virtual” si los ataques de explotación de vulnerabilidades podrían atravesar las defensas y tener éxito. El sistema de gestión realizará en la fase de exploración de la superficie de ataque, identificando puertos y servicios. Esta información puede ser alimentada con información concreta de parches y versiones. En la fase de ejecución realizará el ataque y caso de ser positivo recibirá desde la sonda el resultado del mismo.

Amenazas Ciber-físicas en infraestructuras críticas

Identificar si una instalación está sufriendo ataques combinados e identificar qué ataques físicos pueden suponer un incremento de la amenaza de ciberseguridad.

ANEXO II MODELO DE PRESENTACIÓN DE SOLICITUD

PARTE A: INFORMACIÓN ADMINISTRATIVA Y DECLARACIONES RESPONSABLES

***Datos de la empresa o proyecto empresarial[1]**
[Nombre de la empresa o proyecto empresarial]* [CIF] [Página web] [Email] [Teléfono de contacto] [Dirección {calle, localidad, CA, CP, País}]

***Descripción de la actividad**
[Breve descripción de la actividad de la empresa]

***Sector de actividad**
[Sector en el que se encuadra la actividad de la empresa]

[1] Para promotores individuales

***Ámbito tecnológico**
[Tecnología estratégica de la empresa]

***Información del Representante de la Empresa**
[Nombre, Apellidos]* [DNI]* [Teléfono]* [Email]* [Dirección de Residencia]

***Información del Equipo de proyecto y del representante a efectos de notificaciones**
[Persona 1: Nombre, Apellidos, DNI, email] [Persona 2: Nombre, Apellidos, DNI, email] …

La parte A incluye la declaración jurada según el modelo que se incluye más abajo.

MODELO DE DECLARACIÓN JURADA (para start-ups constituidas)

D. _____ con documento nacional de identidad número _____, actuando en nombre de _____ con domicilio en _____ calle _____ , según poder otorgado ante el notario de _____ D. _____, con fecha _____, bajo el número de protocolo _____ DECLARA BAJO SU RESPONSABILIDAD:

Y los miembros del equipo:

D/Dña. ……<nombre y apellidos>…… mayor de edad, con D.N.I. nº …… y domicilio en…… calle ……..

D/Dña. ……<nombre y apellidos>…… mayor de edad, con D.N.I. nº …… y domicilio en…… calle ……..

OTROS DATOS DE LA ENTIDAD Y DATOS DE CONTACTO

1. Persona de contacto
2. Cargo
3. Teléfono de contacto
4. Página web
5. Correo electrónico*

*__IMPORTANTE:__ La dirección de correo electrónico aportada en este apartado será utilizada para todas las notificaciones relacionadas con la solicitud y el proceso de selección.

☐DECLARAN BAJOS JURAMENTO:

Que conocen y aceptan lo dispuesto en las Bases y la Convocatoria del Programa de Aceleración “Cybersecurity Ventures” publicado en la web de INCIBE.

Que la información entregada es fidedigna y que son autores intelectuales de las ideas o proyectos que presentan y que no han hecho uso de información privilegiada o registrada sin los permisos correspondientes, haciéndose responsables por cualquier reclamación sobre propiedad intelectual o utilización de información de dominio privado, manteniendo indemne a la organización ante cualquier posible reclamación.

Que no se encuentran incursos en ninguna otra prohibición o inhabilitación para la obtención de ayudas públicas

Que se hallan al corriente en el cumplimiento de las obligaciones tributarias y frente a la Seguridad Social impuestas por las disposiciones vigentes.

Que la empresa tiene su domicilio social en España

Que, en el caso de ser seleccionados, se comprometen a participar en las condiciones establecidas en las bases del programa de aceleración “Cybersecurity Ventures”

Que informarán sobre cualquier cambio en la constitución del equipo en el momento en que se produzca.

☐DECLARACIÓN DE PYME

El solicitante declara que conforme a lo previsto en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas y la definición de PYME recogida en el Reglamento (CE) Nº 800/2008 de 6 de agosto de 2008) es una:

☐Mediana empresa

☐Pequeña empresa

☐Micro empresa

El solicitante declara los siguientes datos:

Categoría de empresa	Nºtrabajadores	Volumen negocio	Balance general

☐**DECLARACIÓN DE AYUDAS DE MINIMIS**

El solicitante declara:

☐ Que NO ha obtenido, ningún tipo de ayuda de las Administraciones Públicas españolas y/o comunitarias, sujetas al régimen de minimis en los últimos tres años.

☐ Que SI ha obtenido las siguientes ayudas de las Administraciones Públicas españolas ó comunitarias sujetas al régimen de minimis en los últimos tres años:2

Organismo	Fecha de concesión	Objeto	Importe concedido

Importe máximo de ayuda de minimis concedidas: 200.000 € en últimos tres años (100.000 € en el caso de empresas del sector de transporte por carretera).

El solicitante declara que la empresa no realiza operaciones en los sectores incluidos en el artículo 1.1 del Reglamento de minimis.

☐**DECLARACIÓN DE ACEPTACIÓN DE LAS BASES Y CONVOCATORIA**

Asimismo declara que conoce y acepta lo dispuesto en las Bases y la Convocatoria https://www.incibe.es/convocatorias/contratacion/procedimientos_en_vigor/

Se acompañan a este Anexo los documentos exigidos en la Base Quinta.

Fdo…….

Fdo…….

Fdo…….

Firma del representante y de todos los miembros del equipo en su caso.

_____, a _____ de _____ de 2017

[2] Deberán indicarse todas las ayudas obtenidas en los dos ejercicios fiscales anteriores y en el ejercicio fiscal en curso.

MODELO DE DECLARACIÓN JURADA (para promotores a título individual)

D/Dña. ……<nombre y apellidos>…… mayor de edad, con D.N.I. nº …… y domicilio en…… calle ……..

Y los miembros del equipo

D/Dña. ……<nombre y apellidos>…… mayor de edad, con D.N.I. nº …… y domicilio en…… calle ……..

D/Dña. ……<nombre y apellidos>…… mayor de edad, con D.N.I. nº …… y domicilio en…… calle ……..

☐**DECLARAN BAJOS JURAMENTO:**

Que conocen y aceptan lo dispuesto en las Bases y la Convocatoria del Programa de Aceleración "Cybersecurity Ventures" publicado en la web de INCIBE.

Que la información entregada es fidedigna y que son autores intelectuales de las ideas o proyectos que presentan y que no han hecho uso de información privilegiada o registrada sin los permisos correspondientes, haciéndose responsables por cualquier reclamación sobre propiedad intelectual o utilización de información de dominio privado, manteniendo indemne a la organización ante cualquier posible reclamación.

Que no se encuentran incursos en ninguna otra prohibición o inhabilitación para la obtención de ayudas públicas

Que al menos un miembro del equipo tiene la residencia en España.

Que, en el caso de ser seleccionados, se comprometen a participar en las condiciones establecidas en las bases del programa de aceleración "Cybersecurity Ventures".

Que informarán sobre cualquier cambio en la constitución del equipo en el momento en que se produzca.

Que se comprometen en caso de ser seleccionados a constituirse como empresa en los términos indicados en el Programa y a presentar la documentación que corresponda.

☐**DECLARACIÓN DE ACEPTACIÓN DE LAS BASES Y CONVOCATORIA**

Asimismo declara que conoce y acepta lo dispuesto en las Bases y la Convocatoria https://www.incibe.es/convocatorias/contratacion/procedimientos_en_vigor/

Fdo…….

Fdo…….

Fdo…….

Firma del representante y de todos los miembros del equipo en su caso.

_____, a _____ de _____ de 2017

PARTE B: DESCRIPCIÓN DEL PROYECTO

Extensión máxima 5 páginas
Fuente: Arial
Tamaño Fuente: 11pt

Se tratarán los siguientes aspectos desde dos puntos de vista: desde el punto de vista de madurez y desde el de impacto.

1 – Mercado
¿Quiénes son los clientes potenciales? *¿Cómo de grande es el mercado objetivo? Descríbalo de manera cualitativa y cuantitativa.* *¿Cómo se va a llegar a dicho mercado? ¿Qué canales de distribución serán utilizados?*

2 – Tecnología
¿Cuán disruptiva es la tecnología empleada por la empresa? *¿Posee la empresa la propiedad de dicha tecnología?* *¿Tiene la empresa previsto el desarrollo de mejoras en su tecnología o nuevos desarrollos en los próximos meses?* *¿Es la tecnología la base de su ventaja competitiva?*

3 – Rentabilidad
Explique cómo su proyecto será sostenible y producirá beneficios (ingresos mayores que los gastos). Explique la estructura de costes e ingresos (de donde vienen).

4 - Ventaja competitiva
¿En qué innova su proyecto que suponga una ventaja competitiva (por ejemplo procesos, patentes, experiencia o tecnología propietaria)? *¿Quiénes son los competidores? ¿Cómo se posiciona su solución ante la del resto de competidores?*

5 - Equipo

¿Quiénes son los miembros clave de su equipo? Para cada uno proporcione una breve descripción de su experiencia y su rol o contribución al proyecto. ¿Qué compromiso tienen con el proyecto?

PARTE C – INTERÉS EN EL PROGRAMA DE ACELERACIÓN

Extensión máxima: 2 páginas
Fuente: Arial
Tamaño Fuente: 11pt

1.- Motivación
Explicar las motivaciones del equipo promotor para la participación en el programa de aceleración. ¿Cuál es el plan de creación de valor en la empresa y de qué manera en programa de aceleración va a contribuir a ellos?

2.- Alineación con los retos del programa de aceleración
Identificar el/los retos que aborda el proyecto empresarial. Explicar cómo responde la actividad de la empresa al reto seleccionado.

ANEXO III – DATOS BANCARIOS

D. _____ con documento nacional de identidad número _____, actuando en nombre de _____ con domicilio en _____ calle _____ , según poder otorgado ante el notario de _____ D. _____, con fecha _____, bajo el número de protocolo _____ DECLARA BAJO SU RESPONSABILIDAD que la cuenta bancaria titularidad de la entidad a la que represento donde debe realizarse el ingreso de la ayuda es la siguiente:

Nº de cuenta de la entidad beneficiaria

IBAN	Entidad	Oficina	Digito de control	Número de cuenta