Aceleradora Internacional de Ciberseguridad

cyber security ventures

Junta de Castilla y León

Ade
Agencia de Innovación, Financiación e Internacionalización Empresarial

AYUNTAMIENTO DE LEÓN

ildefe

www.incibe.es

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

GOBIERNO DE ESPAÑA

MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

- **Apoyo de INCIBE a emprendedores y start-ups**
- **Programa Cybersecurity Ventures**
  - Objetivos
  - ¿Qué vamos a hacer?
  - Requisitos de la convocatoria 2017

- **Apoyo de INCIBE a emprendedores y start-ups**

INCIBE es el referente público para la dinamización y fortalecimiento de la industria de la ciberseguridad en España

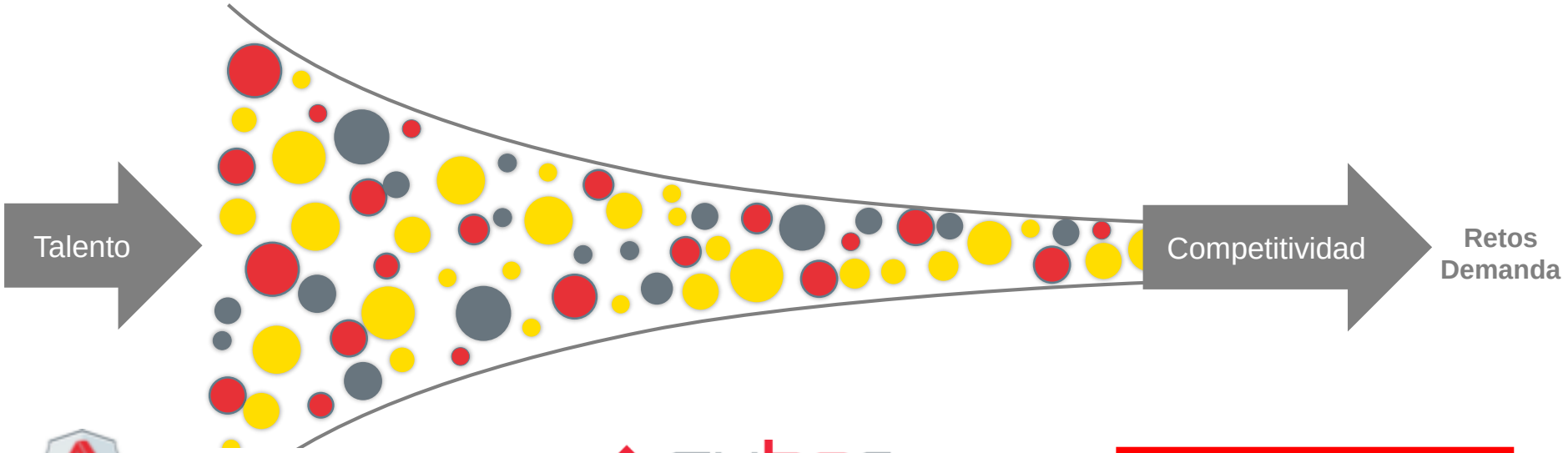
Objetivos

Programas de incubación y aceleración de referencia en ciberseguridad **en Europa**.

Acompañamiento a empresas españolas de ciberseguridad en su **desarrollo y visibilidad internacional**.

¿Cómo lo estamos haciendo?

Emprendedores **Start-ups** **Polo tecnológico**



cyber camp

ciber emprende

cyber security ventures

Polo Tecnológico

Seed - Incubación
- Creación equipo
- Jornadas y contenidos online
- Desarrollo de comunidad
- Ideas y desarrollo prototipo
- FFFs y BAs

Early - Aceleración
- Nicho de mercado
- Lanzamiento MVP
- Primeros clientes
- Crecimiento de plantilla
- Fondos inversión privados y públicos

Growth - Crecimiento
- Beneficios estables
- Internacionalización
- Modelo escalable en ventas
- Innovación nuevos productos
- Marca España

Casos de éxito aceleradas

Electronic IDentification

Identificación Online Disruptiva: Desarrollo de servicios para verificar la identidad de las personas en el canal online con las máximas garantías de las normativas

...continuumsecurity...
THE PROCESS OF SECURE SOFTWARE

Desarrollo de herramientas de ciberseguridad que automatizan los **análisis de riesgos en aplicaciones** y gestionan las posibles amenazas a lo largo de todo el ciclo de desarrollo del software.

Agora Voting

360º de **soluciones electorales**. Votaciones Electrónicas Auditables, Transparentes y Totalmente Verificables.

CounterCraft

Solución disruptiva que **usa técnicas y herramientas de engaño para detectar, descubrir y manipular a los adversarios**. Emplea campañas de contrainteligencia.

hackdoor

Solución integral de monitorización y **alerta continua de amenazas, riesgos y vulnerabilidades de ciberseguridad** en cloud.

incibe_ SMID Prot-On enigmedia cyber security ventures

- **Programa Cybersecurity Ventures**
  - Objetivos
  - ¿Qué vamos a hacer?
  - Requisitos de la convocatoria 2017

cyber security ventures

Programa de aceleración en ciberseguridad

iniciativa de INCIBE en colaboración con la Junta de Castilla y León, a través del Instituto para la Competitividad Empresarial de Castilla y León, y el Instituto Leonés de Desarrollo Formación y Empleo SA (ILDEFE)

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Junta de Castilla y León

Ade
Agencia de Innovación, Financiación e Internacionalización Empresarial

AYUNTAMIENTO DE LEÓN

ildefe

incibe_

cyber security ventures

1. Desarrollo de **nuevas empresas** y apoyo al **talento emprendedor** en ciberseguridad

- Aceleración de empresas de **reciente creación** (menos de 5 años) en el ámbito de la ciberseguridad.
- Programa de aceleración **individualizado**, incluyendo actividades de formación, mentoring, y **relación con inversores** desde el inicio
- Aceleradora con **carácter internacional**, esto implica que se buscará atraer a **emprendedores, inversores** extranjeros y un **mercado** global.

2. Contribución al **eje II PCD** y despliegue de la **estrategia en Ciberseguridad** en España

- Convocatoria abierta pero **criterios de evaluación** premian a proyectos que abordan **retos estratégicos** de ciberseguridad **para España**.
- Vinculación con **empresas tractoras** o potenciales clientes, a través de la publicación de **retos específicos** empresas para estímulo de demanda.
- **Visibilidad internacional**, posicionándola como una **iniciativa de primer nivel** orientada a la ciberseguridad.

3. Colaboración institucional y **de manera sinérgica** con otras actividades INCIBE

- Aportación de **valor local y regional** en el programa y apoyo para **implantación** de empresas en CCAA de Castilla y León.
- Combina actividades en remoto con **aceleración presencial** que se desarrolla en León, en contacto **con instituciones relevantes**
- Apoyo de **ICEX, CDTI, ENISA** y otras entidades del gobierno de España.
- Relación estrecha y **sinergias con otras iniciativas** de INCIBE

- **Programa de aceleración**
  - ¿Qué vamos a hacer?

¿A quien va dirigido?

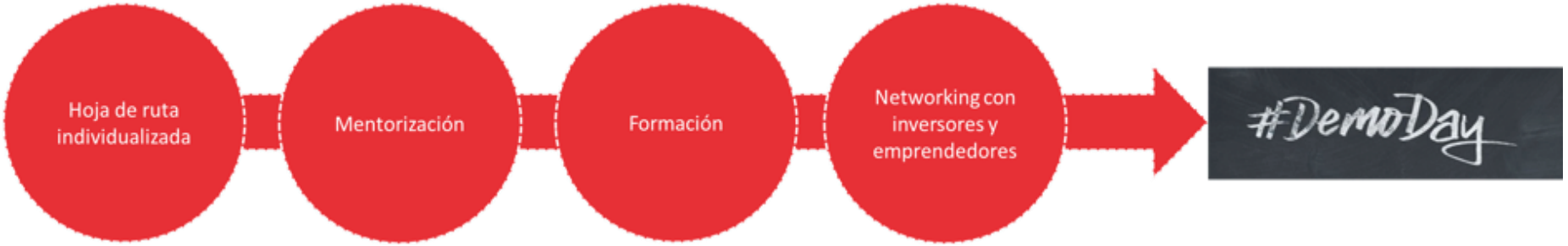
Start-up que:

- ✓ **quiere desarrollar un nuevo negocio en el ámbito de ciberseguridad**
- ✓ **aporta innovación tecnológica y propuesta de valor en estado avanzado de desarrollo**
- ✓ **tiene ambición de desarrollar un mercado global y de ser atractiva como inversión**

Características del programa

- **Específico en ámbito de ciberseguridad, traccionado por retos estratégicos y de empresas**
- **Apoyo por parte de "Consejo Asesor" y "Comité Científico", integrados por personalidades relevantes del sector de ciberseguridad**
- **Carácter internacional**
- **Premios en metálico** para los mejores proyectos.

Desarrollo del programa



Fechas relevantes

Hito	Formato	Fechas estimadas
Definición de la hoja de ruta individualizada	Presencial/Remoto	Oct-Nov 2017
Formación	Presencial	Nov 2017 - Ene 2018
Mentorización – Ntw inversores	Presencial / remoto	Nov 2017 - Feb 2018
Demo Day	Presencial	Feb 2018


URA UNIVERSITY TECHNOLOGY PREVIEW
TOM LINK
#DemoDay
Client ready!
Investment ready!

Red de inversión “seed y early stage”

Innvierte ciberseguridad CDTI-SETSI
A través de INCIBE, es un **fondo público/privado** de prueba de concepto con un nivel de inversión de 20M€ en un horizonte de 10 años.

Atracción de nuevos proyectos de **inversión directa extranjera**

Fondo IBF es el Foro de **Inversión corporativa** compuesto de unas 40 empresas tractoras

Fondo “prueba de concepto” que despliega capacidades tecnológicas

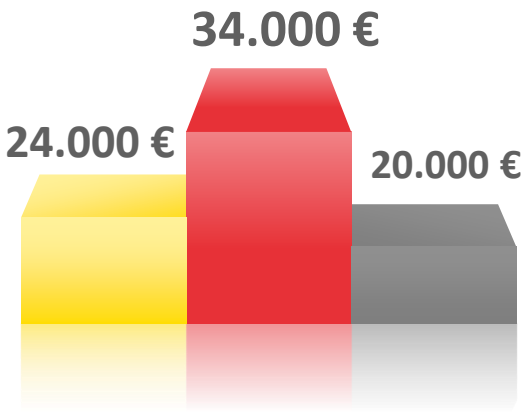
Cybersecurity Ventures ofrece acceso a redes de terceros, como la **Red Europea de Business Angels**.

Premios

- **Participación en forma gratuita en el programa de aceleración**

- **Hasta 120.000€ en premios en metálico**
  - **2.000€** al completar satisfactoriamente la fase de definición de la hoja de ruta individualizada
  - **4.000€** al completar satisfactoriamente el programa de aceleración y cumplir el plan de aceleración

Premios tres mejores proyectos:



Premios del 4º al 10º: 6.000 €

- **Programa de aceleración**
  - Requisitos de la convocatoria 2017

Participantes

¿Quién puede presentarse?

- Empresas de **reciente constitución** (no más de 5 años) o con fecha de constitución previa al comienzo del programa de aceleración.
- Promotor **a título individual** con compromiso de constituir una empresa antes del comienzo del programa

¿Cuántas personas pueden participar?

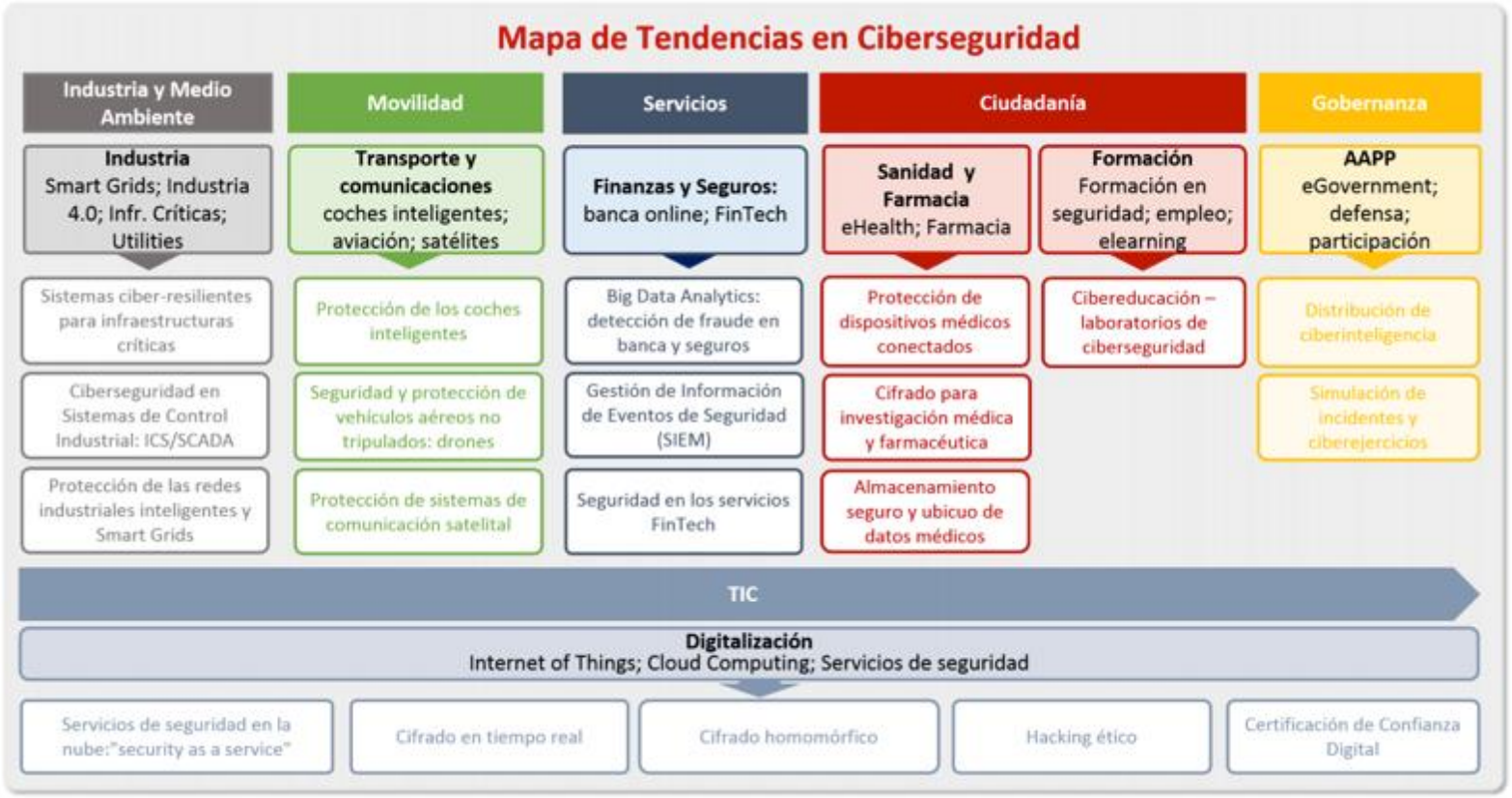
- De manera presencial y al mismo tiempo dos personas por cada empresa.

¿A qué se comprometen?

- **Participación mínima** del 80% en las actividades definidas en la hoja de ruta individualizada.
- **Aceptación** íntegra e incondicional de las **bases del programa** de aceleración.

Retos estratégicos

- La convocatoria abarca **todo tipo de negocios** vinculados a la Ciberseguridad.
- Criterio alineamiento: se valorarán con mayor puntuación los proyectos que aborden alguno de **retos estratégicos** de mayor oportunidad, o **retos orientados**



Retos

2. RETOS ESPECÍFICOS DE EMPRESAS (1/4):

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

Retos

2. RETOS ESPECÍFICOS DE EMPRESAS (2/4):

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.

Retos

2. RETOS ESPECÍFICOS DE EMPRESAS (3/4):

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)
- 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

Retos

2. RETOS ESPECÍFICOS DE EMPRESAS (4/4):

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 continua 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.

¡Atentos a la convocatoria!

- El plazo para el envío de propuestas permanecerá **abierto** en las próximas semanas hasta el **cierre de la convocatoria estimada el 10 de septiembre** a las 24:00 (CET).

- **Fechas relevantes**

Hito	Comunicación	Fecha limite
Registro y recepción de propuestas	Vía Web/ email	10 sept 2017
Cierre del periodo de subsanación	Vía Web/ email	15 sept 2017
Evaluación de propuestas y preselección 20	Vía email	04 oct 2017
Entrevista personal "Pitches" y preguntas	Presencial	10 oct 2017
Selección 10 proyectos finalistas y 5 reserva	Vía email	11 oct 2017
Comienzo del programa de aceleración	Presencial	24-25 oct 2017

¿Cómo presentarse?

- **A través del portal web de INCIBE https://www.incibe.es/ventures**
- **A través de formulario F6S o correo electrónico ventures@incibe.es**
- **En español o en inglés.**
- **La propuesta de participación tiene tres partes obligatorias:**
  - **Parte A: Información administrativa** *(Datos de la empresa o proyecto empresarial, Descripción de la actividad, Sector de actividad, Ámbito tecnológico, Representante empresa)*
    - **Declaración jurada**
    - Empresa constituida, fotocopia compulsada del **CIF**.
    - En trámites: **DNI promotor**, o **pasaporte** y justificante **residencia** territorio español.
  - **Parte B: Descripción del proyecto** *(Mercado, Tecnología, Rentabilidad, Ventaja, Equipo)*
  - **Parte C: Interés en el programa** *(Motivación, y Alineación con los retos descritos)*

Proceso y criterios de evaluación (I)

- **Las propuestas presentadas serán evaluadas por un comité evaluador:**
  - Independiente
  - De forma confidencial
  - Proceso equitativo

- Se preseleccionarán **hasta 20 propuestas** que serán invitadas a una **entrevista presencial.**
- Se seleccionarán los **10 primeros** proyectos para participar en el programa de aceleración
- Se seleccionarán **5 proyectos como reserva** que serán convocados en caso de abandono de alguno de los proyectos seleccionados.

Proceso y criterios de evaluación (II)

Criterio (0 a 5)	Elementos para la valoración del criterio	Peso y umbral
Madurez del proyecto	• Mercado: Identificado, validado y dimensionado. Canales de comercialización • 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, mercado global, canales internacionales. • Tecnología: Rupturista, innovadora. • Rentabilidad: Creciente, exponencial. • Ventaja competitiva: Diferenciación contundente respecto de competidores. Ventana de oportunidad sostenida en el tiempo. • Equipo: capacitado, multidisciplinar, internacional, atractivo.	peso = 25% umbral = 3
Motivaciones y aprovechamiento programa	• Motivaciones del equipo promotor para la participación en el programa de aceleración. ¿De qué manera se piensa aprovechar el programa? ¿Por qué el proyecto debe ser apoyado?	peso = 30%
Alineación con los retos	• Valoración de la medida en la cual el proyecto aborda a alguno de los retos planteados en la convocatoria (estratégicos o específicos)	peso = 20%

Call to action

1 Registra tus datos de contacto en:
https://www.f6s.com/cybersecurityventuresapplication2017/apply
Te avisaremos sobre las novedades de la convocatoria

2 Comienza a preparar YA tu solicitud
La fecha límite de presentación es el 10 de septiembre 2017

3 Si tiene dudas, escríbenos a:
ventures@incibe.es

Gracias por su atención

Ignacio.luna@incibe.es

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD