IK4
Research Alliance

Visión IK4 de la Ciberseguridad Industrial

17 de octubre de 2017

AZTERLAN | CEIT | CIDETEC | GAIKER | IDEKO | IKERLAN | LORTEK | TEKNIKER | VICOMTECH

¿Qué es IK4 Research Alliance?

¿Qué es IK4?

Somos una **Alianza Privada de 9 Centros Tecnológicos** cuya misión es **la generación, captación y transferencia de conocimiento científico-tecnológico,** con el fin de ponerlo a disposición de las empresas **para que puedan complementar sus capacidades tecnológicas,** facilitando así la mejora de su competitividad.

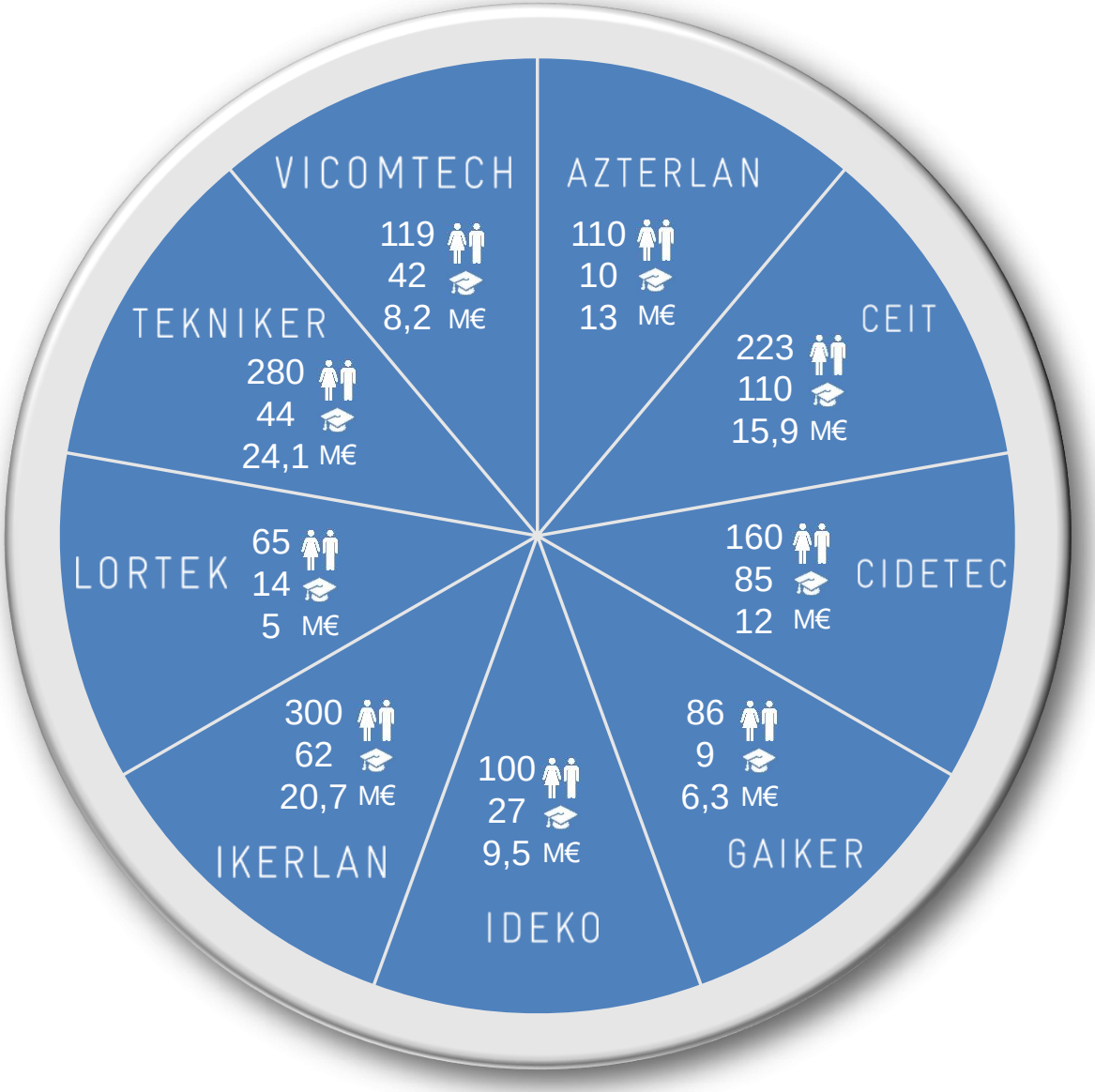
AZTERLAN	GAIKER	LORTEK
CEIT	IDEKO	TEKNIKER
CIDETEC	IKERLAN	VICOMTECH

IK4
Research Alliance

¿En dónde está IK4?

IK4 Research Alliance

Cifras básicas



IK4 Research Alliance

1443

403 (28%)

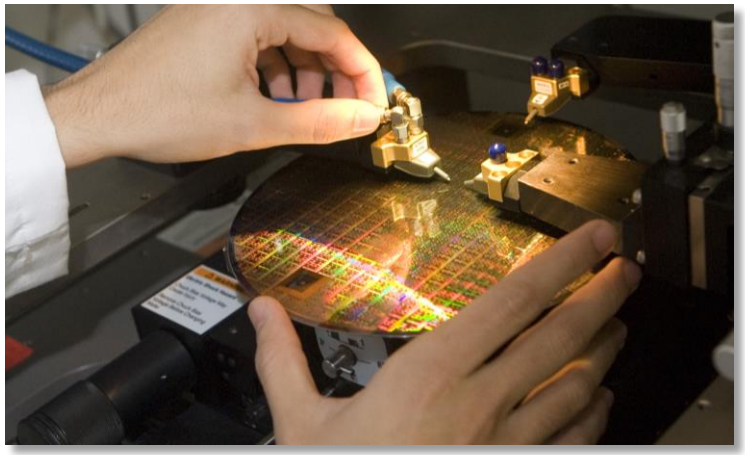
114,6 M€

Fuente: Cierre 2016 de los Centros Tecnológicos

IK4 Research Alliance

Impacto Empresarial

	2016	2015
Ingresos totales (M€)	**114,6**	**111,2**
Facturación empresas (%)	**55,75**	**59,62**
Patentes solicitadas	**43**	**35**
Patentes concedidas	**17**	**10**
Spin-offs año/total	**1 / 89**	**2 / 88**
Nº Empresas	**951**	**871**
Personas transferidas a empresas	**62**	**66**



Excelencia Científico-Tecnológica

	2016	2015
Artículos ISI	**224**	**223**
Comunicaciones congresos	**234**	**123**
Congresos internacionales organizados	**2**	**2**
Capítulos de libros internacionales	**3**	**7**
Tesis doctorales en relación con proyectos	**41**	**40**

Fuente: Cierre 2016 de los Centros Tecnológicos

Ámbitos Estratégicos de la Alianza

17,53%

Energía

Fabricación avanzada

56,87%

13,42%

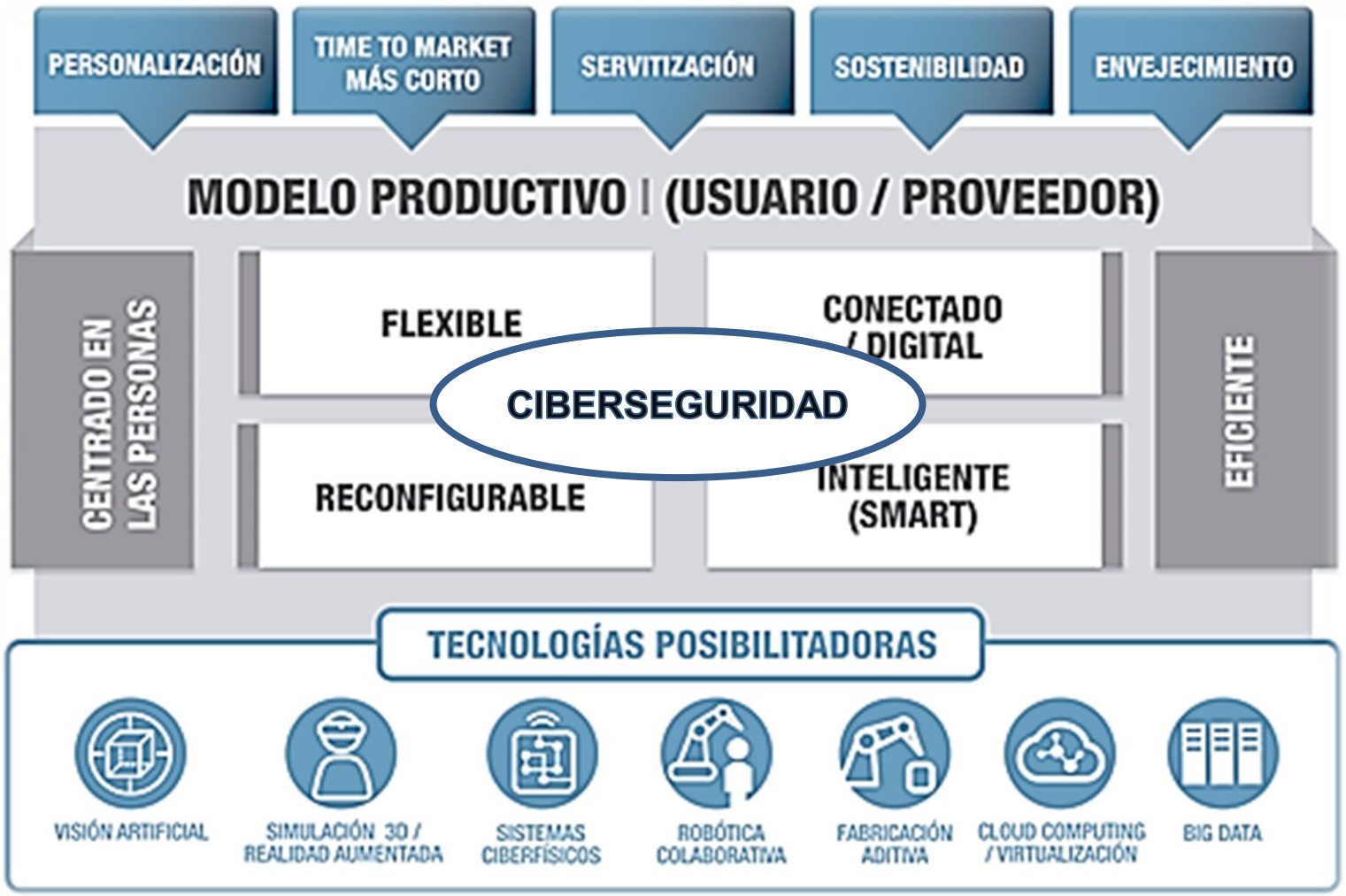
Salud

Transporte y Movilidad

7,41%

Visión IK4 de la Ciberseguridad Industrial

IK4 y la Industria 4.0



Definición y conceptos claves de la ciberseguridad

- La **ciberseguridad** se refiere al conjunto de tecnologías, procesos y prácticas preventivas utilizadas para protegerla integridad de las redes, sistemas de computación, programas y datos de ataques, daños o accesos no autorizados.

- Existen múltiples tipos de **ciberataques** que pueden sufrir las organizaciones industriales, de servicios o las infraestructuras críticas. Por ejemplo:
  - Interrupción de los servicios que prestan
  - Acceso a información valiosa con fines delictivos o ciberespionaje

- El alcance de las **actuaciones** debe incluir a todos los sistemas conectados de cualquiera de los componentes del ICS (Industrial Control Systems):
  - Servidores
  - Aplicaciones
  - Componentes de red
  - Dispositivos de control (PLC, CPS, SCADA)

Tendencias relevantes que incrementan la necesidad de inversión en Ciberseguridad

- Auge y crecimiento de **internet** e internet de las cosas
- **Ubicuidad** de las redes de telefonía y datos con capacidad de transmitir grandes cantidades de información de forma fiable y en tiempo real
- Grandes **avances en electrónica** tanto en miniaturización como en precisión y precio facilitando la aparición de infinidad de sensores y sistemas de monitorización y comunicación
- **Globalización** de los mercados, y por lo tanto, mayor lejanía física de los clientes y aparición de nuevos competidores
- La obligación de poner en el mercado nuevos **productos de alto valor añadido** que compensen esa mayor competencia y fidelicen a los clientes (personalización, …)
- Necesidad de disponer de capacidades avanzadas de **ciberseguridad** para minimizar los riesgos de la utilización masiva de equipos conectados (IoT)

Posicionamiento y Capacidades de IK4 en Ciberseguridad

- **Seguridad de los sistemas embebidos**
  - Seguridad basada en hardware
  - Metodología de desarrollo: ciclo de vida y certificación
  - Validación y auditoría de medidas de seguridad

- **IoT ciberseguro**
  - Seguridad de conectividad y protocolos
  - Arquitecturas ciberseguras con conexión al cloud

- **Seguridad de red OT (Operational Technology)**
  - Soluciones de ciberseguridad en planta
  - Infraestructura de recolección, pre-procesamiento y almacenamiento flexible de datos para el análisis de la ciberseguridad

- **Gestión integral de la ciberseguridad**
  - Resiliencia en las Organizaciones
  - Análisis de riesgos
  - Análisis de comunicaciones y datos en operación
  - Visualización de la información, centro de datos y gestión de la ciberseguridad

Proyecto ELKARTEK “SEKU-TEK”: Objetivos

- Desarrollar **tecnologías de ciberseguridad que den solución al Negocio Avanzado e Inteligente de la Industria Vasca**, y prevengan ataques y protejan el negocio de las empresas industriales vascas, investigando en una **Nueva Generación** de componentes seguros que se integren en el ecosistema industrial.

- **Garantizar la competitividad y excelencia de los agentes de la Red Vasca de Investigación, en torno a tecnologías de ciberseguridad de primer nivel** (con alcances TRL 3 y 4, que en siguientes fases del proyecto lleguen a alcances TRL 5, 6 y 7) **adecuadas a las necesidades del tejido industrial vasco**, para que puedan ser fácilmente transferidas.

Proyecto ELKARTEK “SEKU-TEK”: Consorcio

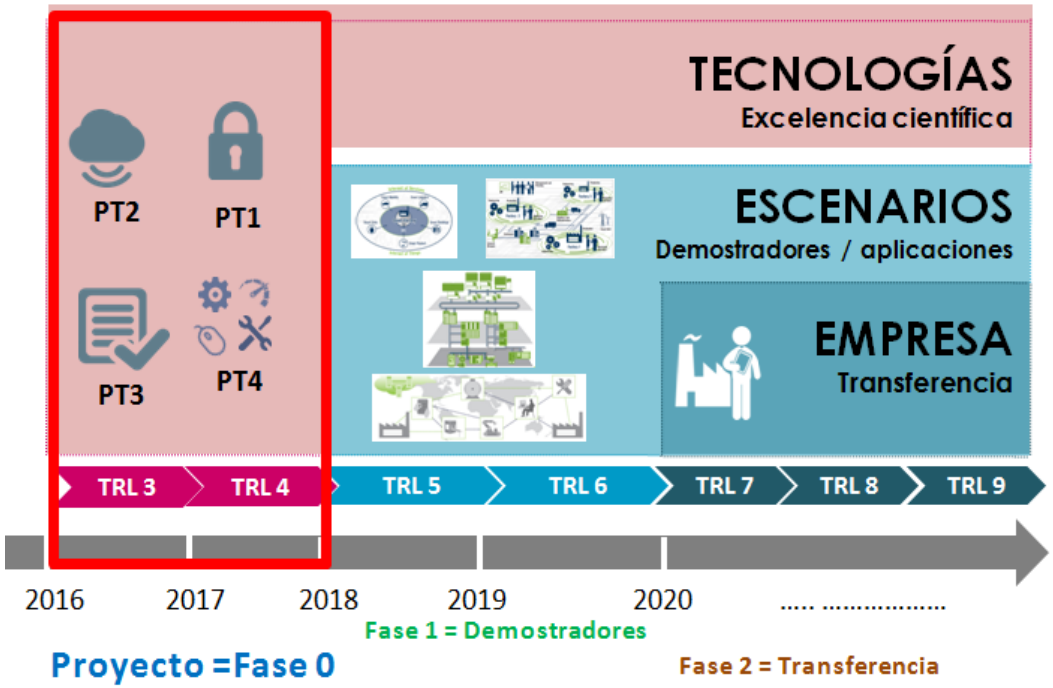
Proyecto ELKARTEK “SEKU-TEK”: Aproximación tecnológica y calendario

Seguridad de red OT
Nube física/virtual con apoyo para IoT cibeseguro, análisis de datos y visualización

IoT ciberseguro
Conectividad, intercambio de datos y protocolos de comunicación

Seguridad de los sistemas ciber-físicos
Sistema embebidos confiable con apoyo para IoT ciberseguro

Gestión integral de la ciberseguridad
Identificar, Proteger, Detectar, Responder, Recuperar



Visión 2022

- **Se dispone de la tecnología** necesaria para abordar la seguridad de los sistemas embebidos, de los elementos de los procesos productivos, de la red OT y en general de todas las Tecnologías de la Información y las comunicaciones que forman parte del ecosistema industrial.
- **NO EXISTEN EMPRESAS NO CIBERSEGURAS**: La internacionalización y competitividad de las empresas se garantiza a través de la mejora de sus capacidades de ciberseguridad como garantía de negocio.
- La confianza en la tecnología posibilita **nuevos servicios** inteligentes. Tejido tecnológico e industrial preparado para los nuevos escenarios en los que afloran nuevos riesgos y amenazas más difíciles de prever.
- Existe un **sector maduro** de la ciberseguridad industrial.
- Se han **desarrollado** acciones regulativas, normativas y extendido las buenas prácticas.
- **Los sistemas safety son además ciberseguros**.

Especialización tecnológica “conectada”

Prioridades tecnológicas SRIA ECSO

- Assurance and security&privacy by design
- Identity, access and trust management
- Data security
- Protecting the ICT Infrastructure
- Security services

Colaboración con grupos internacionales

AZTERLAN | CEIT | CIDETEC | GAIKER | IDEKO | IKERLAN | LORTEK | TEKNIKER | VICOMTECH