"Ciberseguridad en entornos IoT y evaluación de impacto en infraestructuras críticas"

Octubre 2017

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

Ceit-IK4 introducción

- **Datos relevantes** www.ceit.es
  - 223
  - 110
  - 15,9 M€
- **Ubicación**

  2 centros en Donostia-San Sebastián:

  Ibaeta y Parque Tecnológico de Miramón

- **Especialización**
  - Materiales y fabricación
  - Transporte y energía
  - Agua y salud
  - Tecnologías de la Información y Comunicación (TIC)

Ceit

Ceit es un centro de investigación privado y sin ánimo de lucro

- Creado en 1982 por la Universidad de Navarra.
- Agente de la Red Vasca de Ciencia, Tecnología e Innovación apoyada por el Gobierno Vasco.

Ceit realiza actividades de dos tipos:

- **Investigación bajo contrato:**
  - Proyectos industriales.
  - De acuerdo a los requisitos y especificaciones del cliente.
- **Investigación básica:**
  - Orientada al desarrollo de nuevo conocimiento y tecnología, con vista hacia la aplicación industrial.
  - Investigación liderada por doctores dando lugar a la realización de tesis doctorales.
  - Los resultados obtenidos de carácter no-confidencial son publicados en revistas y conferencias internacionales.

Ceit busca y ofrece:

- Colaboración cercana con la industria en medio-largo plazo.
- Conocimiento del negocio en el sector y entendimiento del impacto de la tecnología e innovación en las ventas y el beneficio.
- Colaboraciones para el desarrollo de nuevos productos y soluciones.

Ceit: spin-offs

Design of wastewater plants
13 employees
Sold to Praxair group
1996

Internet security and filtering
108 employees
Sold to main shareholders
1997

Motion capture, biomechanics, computer visión
24 employees
Sold to main shareholders
1998

Integrated circuits for RF communications
10 employees
Sold to Ixys
2000

Enterprise software solutions
21 employees
Sold to main shareholders
2000

Training simulators
49 employees
Ceit 14%
2002

On-line colour machine vision
Out of business
2004

Communication solutions
13 employees
Sold to Alcad
2005

Mechanical characterisation of materials
Sold to main shareholder
2005

High performance metallic powders
8 employees
Sold to Erasteel
2007

Membranes for wastewater treatments
12 employees
Ceit 22,7%
2008

Ultra-low power RFID passive sensors
6 employees
Ceit 20%
2008

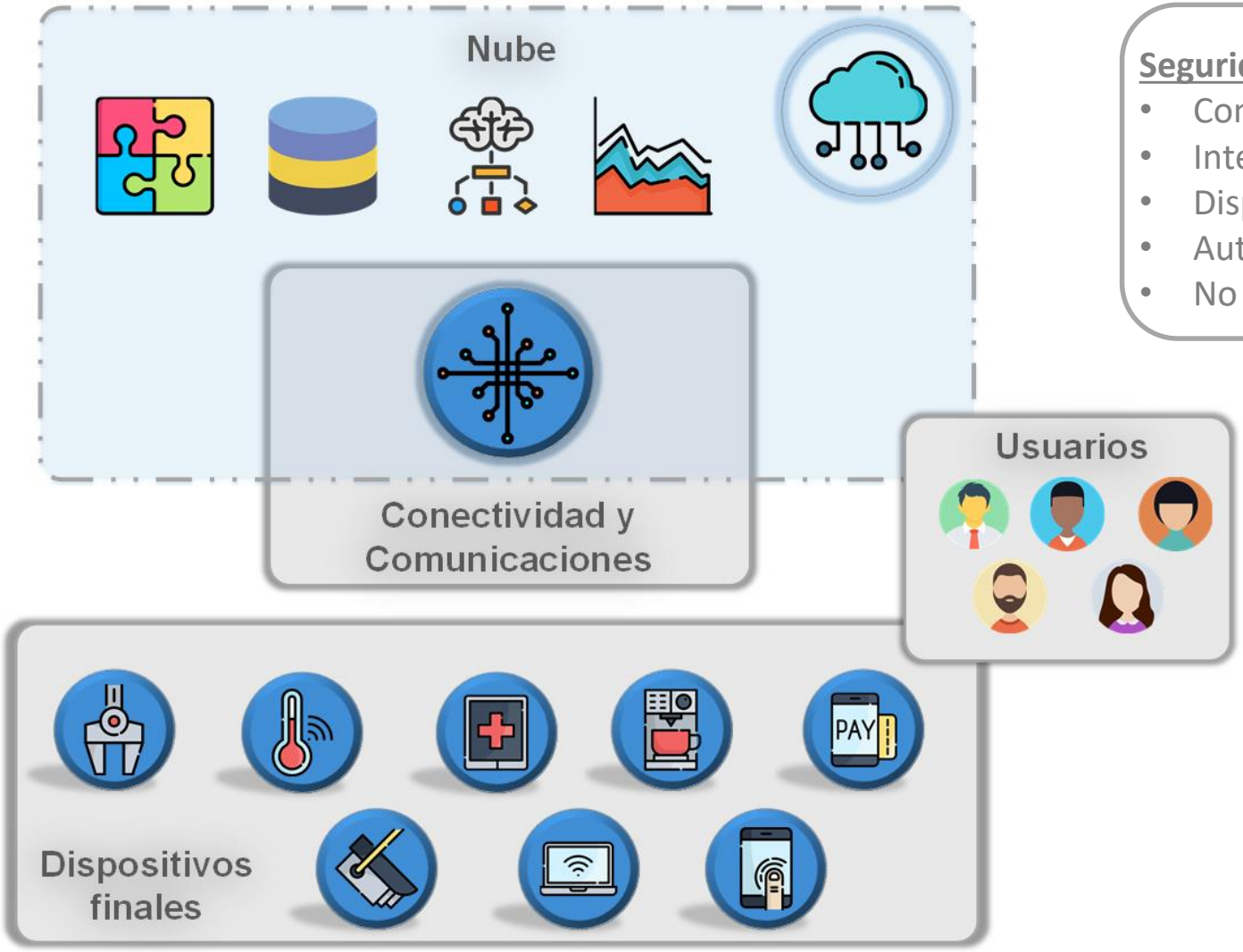
Advanced solutions for the optimal management of wastewater
1 employee
Ceit 100%
2013

Recovery of precious metals
1 employee
Ceit 100%
2013

"Ciberseguridad en entornos IoT y evaluación de impacto en infraestructuras críticas"

1. **Ecosistema IoT**
   - Dispositivo final IoT
   - Red de comunicaciones
   - Usuario final
2. **Evaluación en infraestructuras críticas (IC)**
   - Evaluación de impacto a través de laboratorio virtual.
   - Resiliencia en infraestructuras críticas.
3. **Líneas actuales y futuras**

1. Ecosistema IoT



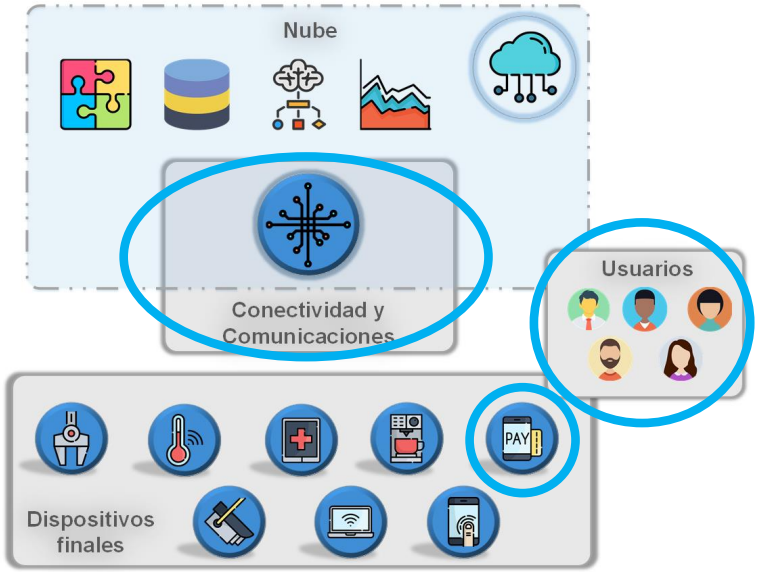
Seguridad:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- No repudio

Amenazas y desafíos para la ciberseguridad IoT*

Problemas existentes:

- Malas configuraciones.
- Uso de credenciales por defecto.
- Software vulnerable.
- Dificultad en realizar actualizaciones.
- Convivencia con dispositivos heredados.
- Uso de protocolos de comunicación no seguros.
- Denegación de servicio.
- Aumento de la superficie de exposición.
- Baja usabilidad.



Tendencia a la miniaturización:

- Hardware con recursos de computación limitados.

La ciberseguridad ha de tener en cuenta todos los elementos del ecosistema IoT.

*Fuente: Incibe, Huawei, *Creación de un mundo IoT fiable y gestionado*, 2017

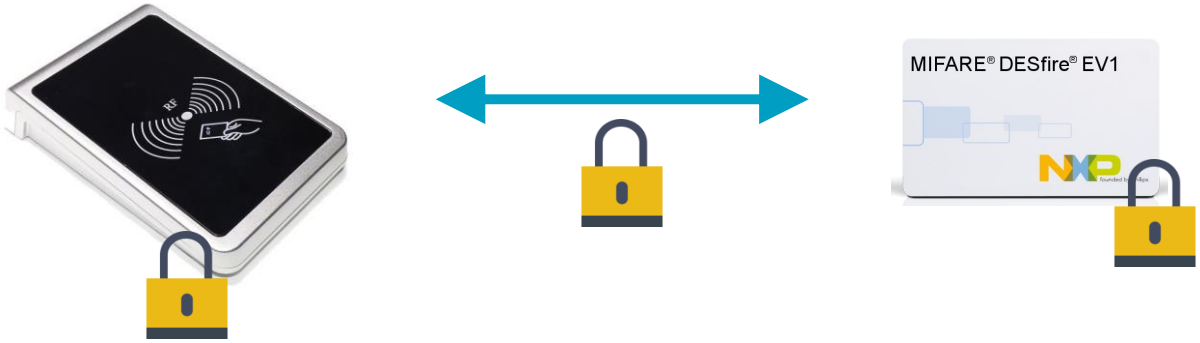
Tarjeta de proximidad para realización de pagos

Peligros

- Si no hay cifrado:
  - La comunicación puede ser escuchada por terceros (confidencialidad).
  - El dato en curso puede ser modificado (integridad).
  - Incapacidad de autenticar el end-point (autenticación).
  - Repudio (no-repudio).
- La tarjeta podría ser clonada o su información manipulada.

Contramedidas

- Uso de criptografía:
  - En capa de aplicación.
  - En hardware.
- Co-procesadores hardware seguros de ayuda a la computación: TPM, SAM, ...



1. Ecosistema IoT: Dispositivo final IoT

Control de acceso en flotas de autobús

Objetivos:

- *Securizar* pagos en autobús mediante tarjeta de proximidad.
- Uso de criptografía en capa de aplicación para protección de billetes de autobús y tarjetas de proximidad inseguras.
- Uso de tecnologías seguras:
  - Tarjeta de proximidad segura.
  - Elementos HW para ayuda criptográfica en el lector (SAM) .

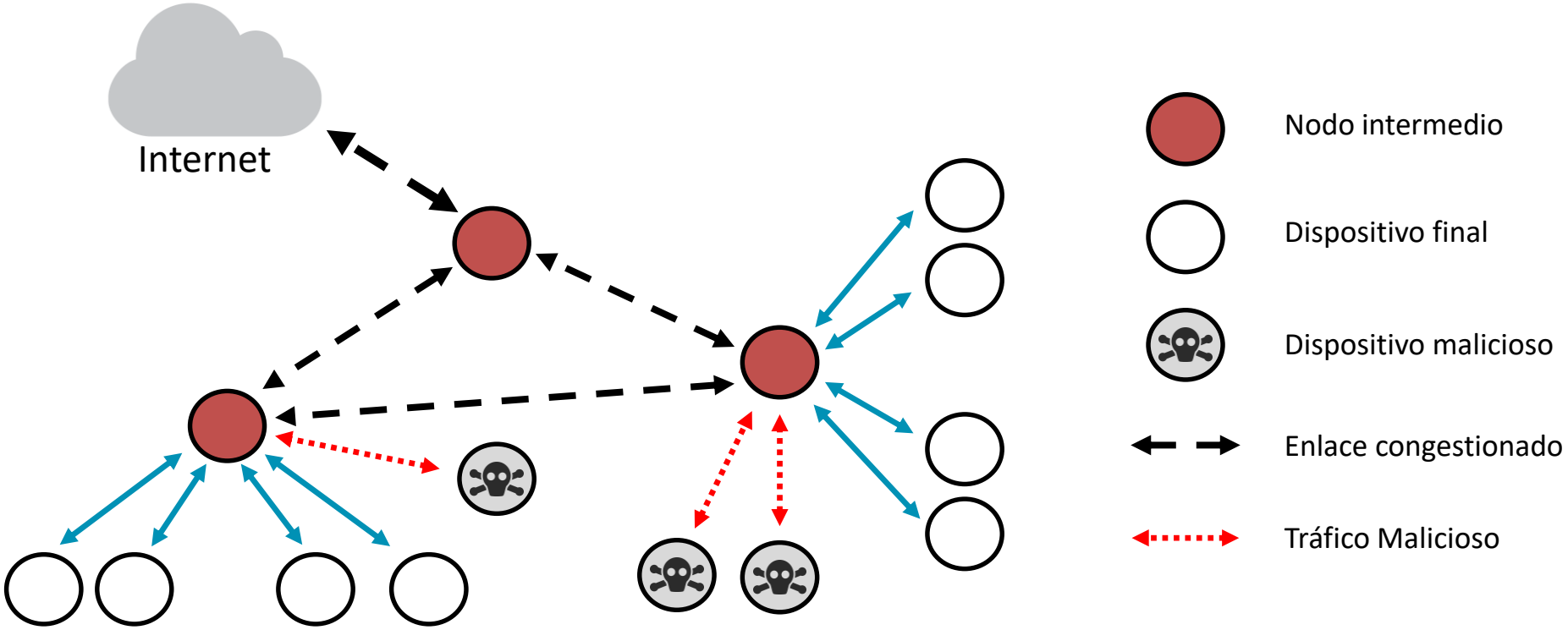
Tecnologías aplicadas:

- Tarjetas de proximidad: Mifare Classic y Mifare DESFire EV1 y EV2.
- SAM (Secure Access Module).
- Integrado con plataformas open source.

Disponibilidad de comunicaciones

Denegación de servicio (DoS) volumétrico.

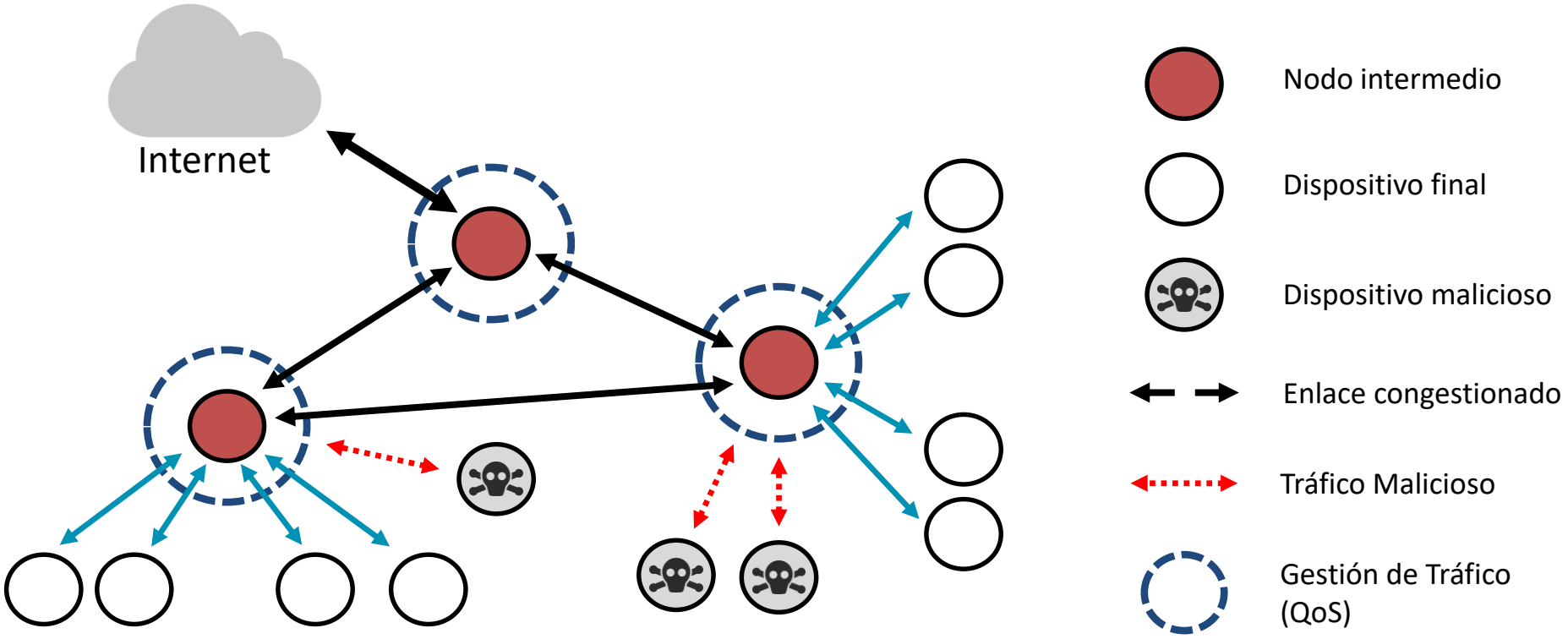
- Nodos infectados pueden generar tráfico malicioso (Mirai botnet).
- Generación de tráfico por servicios legítimos pero menos prioritarios que comparten el canal.
- Pérdida de disponibilidad del servicio.



Disponibilidad de comunicaciones

Asegurar disponibilidad mediante el control de la calidad de servicio (QoS).

- Nodo intermedio: punto clave para evitar DoS volumétrico.
- Gestión QoS inteligente en nodos intermedios de la red.
- Mitigación de la Denegación de Servicio.



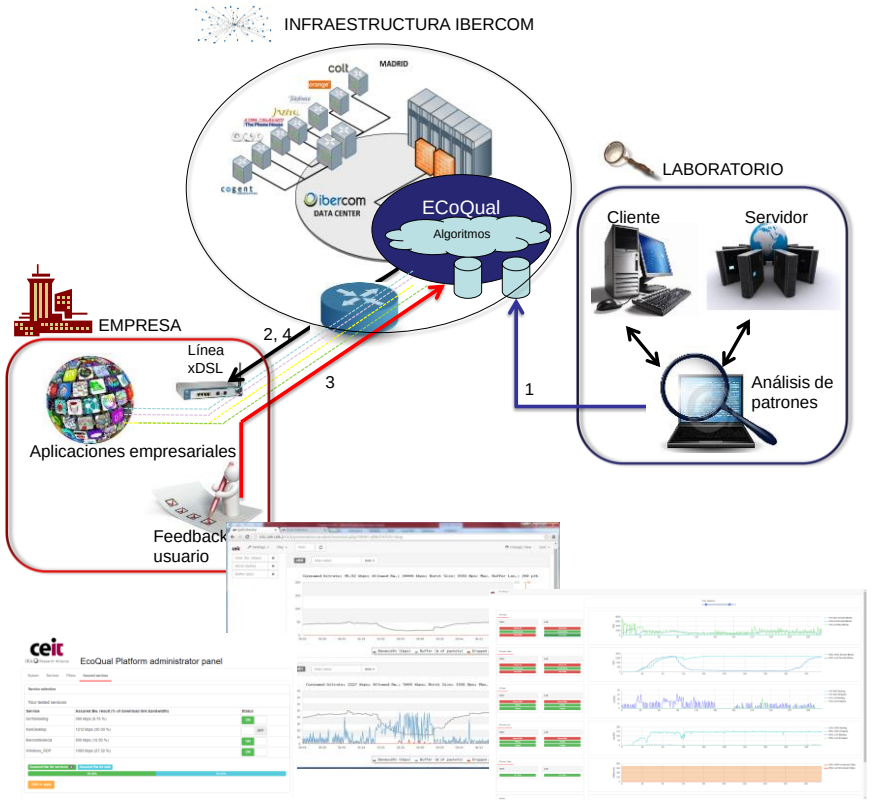
ECoQual: Evaluación y Configuración de la gestión de QoS de aplicaciones industriales en el Gateway de acceso a Internet

Objetivos:

- Desarrollo de una herramienta de análisis de requisitos de QoS para aplicaciones industriales.
- Metodología para la configuración inteligente de la distribución de ancho de banda (aseguramiento y/o priorización de tráfico) teniendo en cuenta la personalización por parte del usuario final.
- Gestión y configuración de QoS en el punto de acceso para las aplicaciones industriales configurados por el usuario.
- Centralización de la información de los puntos de acceso para análisis Big Data.

Tecnologías aplicadas:

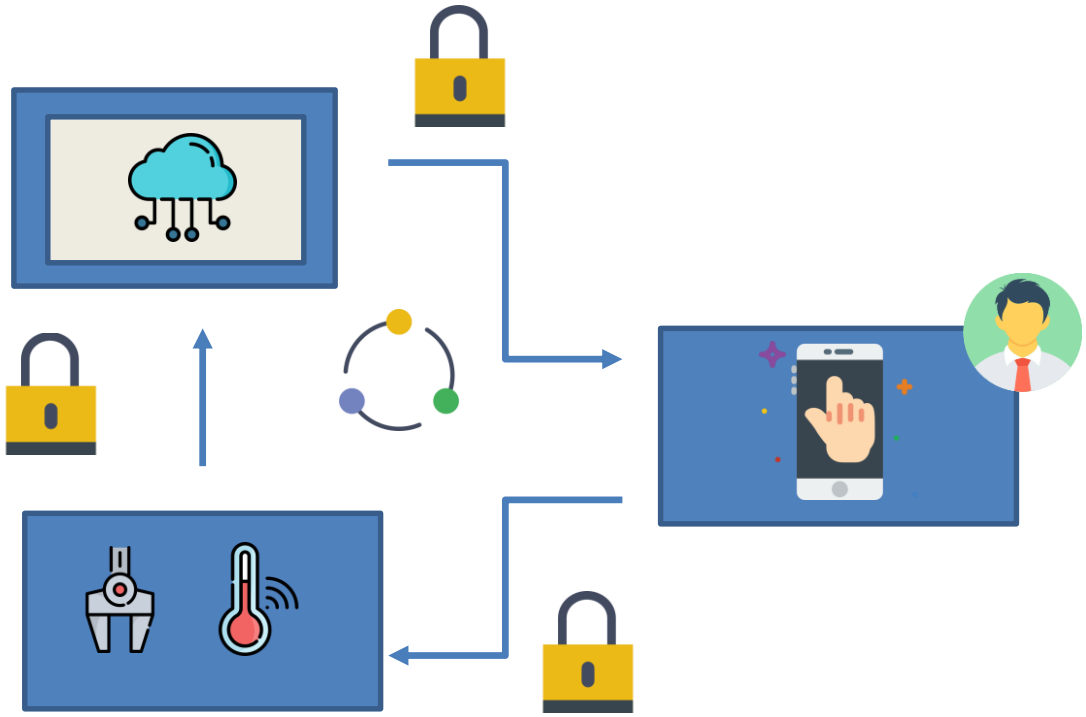
- Técnicas avanzadas de clasificación y detección de aplicaciones.
- Algoritmos de colas para priorización de tráfico.
- Comunicaciones de red cifradas y autenticación a nivel de aplicación.



Arquitecturas ciberseguras

Seguridad y Usabilidad

- Ser humano como eslabón más débil.
- El trabajador ha de estar dispuesto a USAR las medidas de seguridad requeridas.
- La mejora de la usabilidad mejora la seguridad.



1. **Ecosistema IoT**
   - Dispositivo final IoT
   - Red de comunicaciones
   - Usuario final
2. **Evaluación en infraestructuras críticas (IC)**
   - Evaluación de impacto a través de laboratorio virtual.
   - Resiliencia en infraestructuras críticas.
3. **Líneas actuales y futuras**

Ciberseguridad en infraestructuras críticas

Los ecosistemas IoT también están presentes en infraestructura críticas:

- Transporte
- Generación eléctrica
- 'Smart grids'
- Saneamiento y distribución de agua
- Salud

El impacto de la 'in-seguridad' en la infraestructura crítica es alto, dado que el impacto en 'security' afecta directamente a 'safety'.

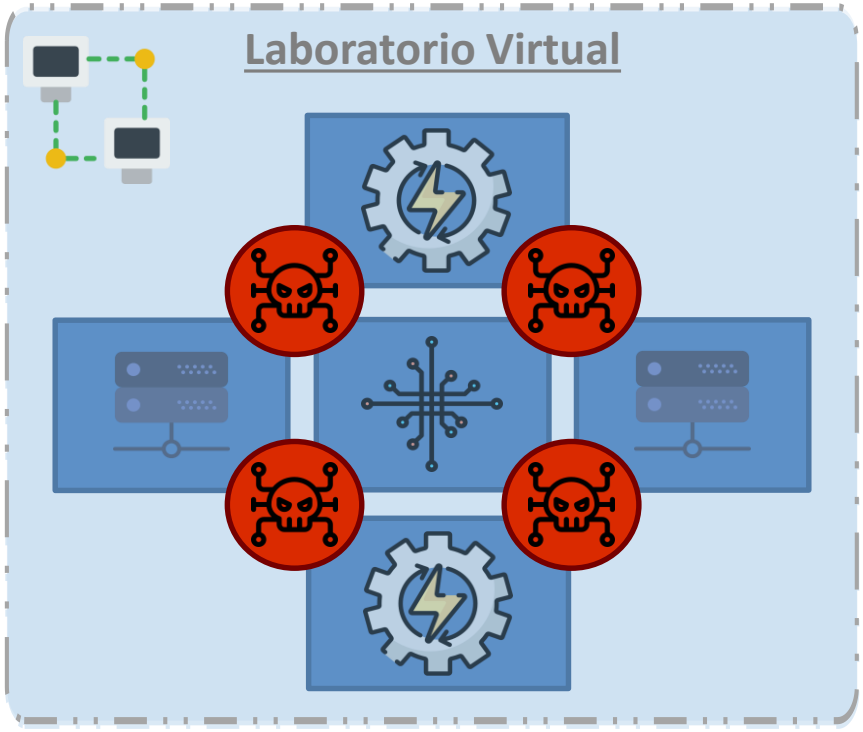
Es necesario trabajar en la prevención, detección, respuesta y mitigación de las amenazas a las infraestructuras críticas.

- Evaluación del impacto en infraestructuras críticas a través de laboratorios virtuales.
- Análisis de la resiliencia en infraestructuras críticas.

Evaluación de impacto

Necesidad de evaluar el impacto safety-security

- Generación de laboratorios de evaluación de impacto.
- Laboratorio virtual y 'digital-twin'.
- Análisis del impacto safety-security mediante técnicas de inyección de fallos.



2. Evaluación en IC: Laboratorio virtual

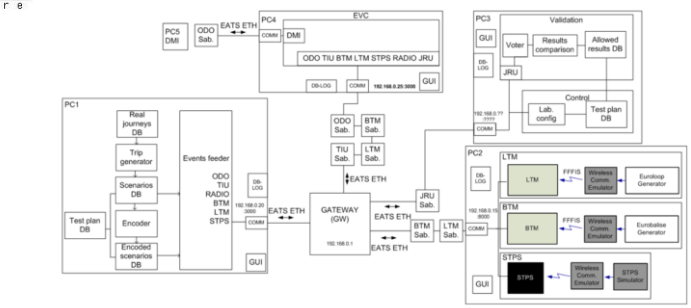
EATS: ETCS Advanced Testing and Smart Train Positioning System

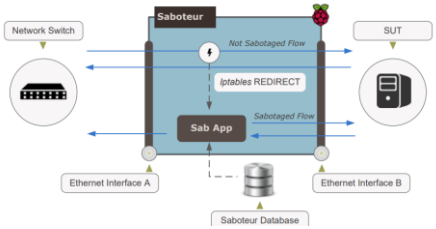
Objetivos:

- Mejora de testeo en laboratorios para equipamiento ETCS embarcado.
  - Reducción de costes de certificación y autorización para la instalación de nuevos equipos.
  - Incorporación de laboratorios virtuales para la validación de ETCS (European Train Control System)

Tecnologías aplicadas:

- Laboratorio virtual – virtualización y emulación de componentes (‘digital-twin’).
- Técnicas de inyección de fallos mediante saboteador transparente y configurable.
- Monitorización y análisis del comportamiento de los sistemas.





Resiliencia en infraestructuras críticas

Definición de Resiliencia:

> *"Ciber-resiliencia es uno de los principios establecidos en la Estrategia de Ciberseguridad Nacional. La resiliencia es una cualidad inherente a un organismo, entidad, empresa o estado que le permite hacer frente a una crisis sin que su actividad se vea afectada."*
>
> (Instituto Español de Estudios Estratégicos, 2015)

Estrecha colaboración con Tecnun (Escuela de Ingenieros de la Universidad de Navarra)

- Ceit: conocimiento de las TICs en el ámbito de la ciberseguridad.
- Tecnun: metodología para la evaluación y análisis de la resiliencia en organizaciones y procesos.

2. Evaluación en IC: Resiliencia

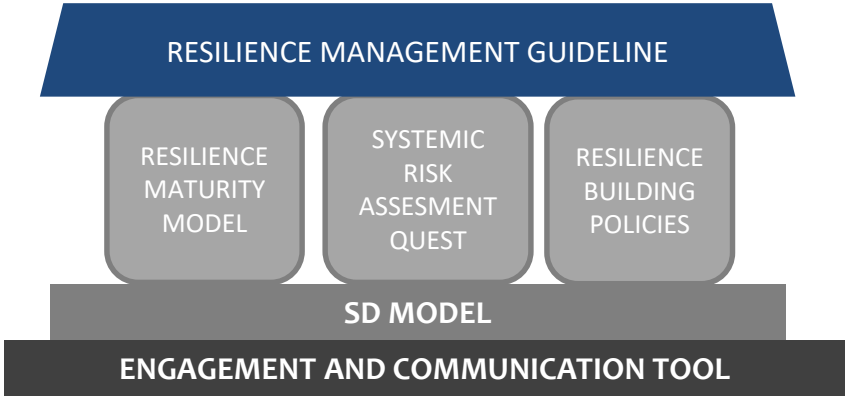
SMR: Smart Mature Resilience
www.smr-project.eu

Objetivos:

- El objetivo general es desarrollar, evaluar y demostrar una Guía para la Gestión de la Resiliencia Europea.
- Desarrollar, validar e implementar 5 herramientas que facilitan el cumplimiento del objetivo general.
- Generar una "columna vertebral" de ciudades resilientes en Europa.

Metodologías aplicadas:

- Group Model Building
- Modelos de dinámica de sistemas
- Programación web
- Group Explorer
- Workshops



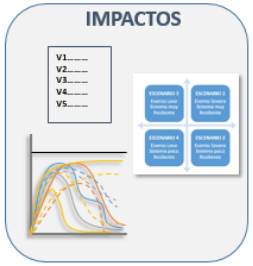
Mejora de la resiliencia en las infraestructuras críticas

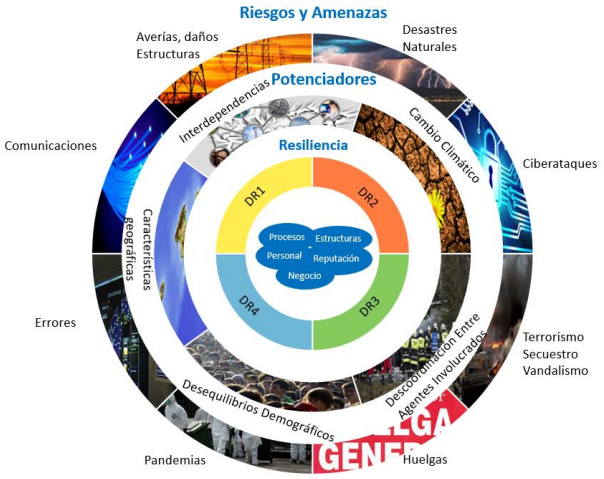
Objetivos:

- Desarrollar una metodología que permite evaluar la resiliencia de una compañía del sector de las IC, estimando su nivel de resiliencia actual y estableciendo acciones para mejorarla.
- Ayudar en el proceso de toma de decisiones en cuanto a las acciones que se han de implantar.

Herramientas:

- Evaluador del nivel de resiliencia.
- Caracterización de eventos.
- Caracterización de impactos.





1. **Ecosistema IoT**
   - Dispositivo final IoT
   - Red de comunicaciones
   - Usuario final
2. **Evaluación en infraestructuras críticas (IC)**
   - Evaluación de impacto a través de laboratorio virtual.
   - Resiliencia en infraestructuras críticas.
3. **Líneas actuales y futuras**

Sekutek

- Embrión para la generación de conocimiento que se materializa en tesis doctorales y publicaciones científicas.
- Buscando siempre una posterior transferencia del conocimiento adquirido hacia la industria. Generación de un tejido industrial vasco ciberseguro.
- Objetivo principal de Ceit: abordar y dar respuesta a desafíos de la sociedad e industria en el campo de ciberseguridad relativo a IoT e IIoT (Industrial Internet of Things).

ECSO (European Cyber Security Organisation)

- Colaboración con la Comisión Europea y entidades involucradas en ECSO en la definición de la Agenda Estratégica de Investigación e Innovación.
- Estrecho contacto con la iniciativa de investigación a nivel europeo en materia de ciberseguridad.

Colaboración con empresas referentes en sectores verticales

- Ofreciendo una solución integral: entendiendo y adaptándose a las necesidades de la empresa desde una visión multidisciplinar.
- Estableciendo vínculos y asociaciones que ayuden a maximizar un entorno ciberseguro.

Dr. Javier Añorga

e-mail: jabenito@ceit.es

IK4 Research Alliance

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