



Connect

tecnal:a

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

"Confidentiality as a driver of digital transformation"

Visión

Por qué la confidencialidad es una palanca estratégica para colaborar con datos sensibles.

Actitud

Confidential Containers en OpenShift como garantía técnica más allá de la obligación legal.



Aitzol Zubizarreta Pikabea

aitzol.zubizarreta@tecnalia.com

CIO

TECNALIA Research & Innovation



Iván Gutiérrez Agüero

ivan.gutierrez@tecnalia.com

Head of Frontier Cybersecurity

TECNALIA Research & Innovation



TECNALIA: investigación aplicada que llega al mercado

Transformamos la investigación tecnológica en prosperidad, junto a empresas e instituciones

Identificamos oportunidades e ideamos soluciones desarrollando e integrando las tecnologías digitales idóneas, con un objetivo: alinear la transformación del negocio con el cambio de modelo digital y abrir nuevas oportunidades.

1.512

personas expertas

29

nacionalidades

Nuestra propuesta diferencial

Digitalización inteligente

Inteligencia artificial y espacios de datos

Digitalización segura

Tecnologías de privacidad, ciberseguridad y blockchain

Digitalización de valor

Realidad extendida y visión artificial

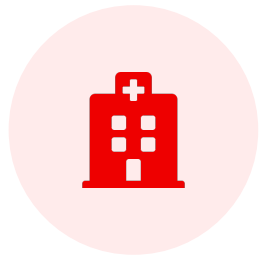


La innovación necesita colaboración



El valor se crea cada vez más entre organizaciones

No dentro de una sola: la innovación exige combinar datos, modelos y capacidades de distintos actores



Hospital

Datos clínicos



Investigación

Modelos y algoritmos



Empresa

Servicios e innovación



Cloud

Capacidad de cómputo

Pero colaborar significa cruzar fronteras de confianza.



El dato tiene valor porque tiene contexto y propietario

Cuatro preguntas que cualquier organización se hace antes de compartir datos sensibles

PRIVACIDAD

¿Quién puede verlo?

CONFIDENCIALIDAD

¿Quién puede acceder mientras se procesa?

SOBERANÍA

¿Quién decide cómo y dónde se usa?

CONFIANZA

¿De quién tengo que fiarme?

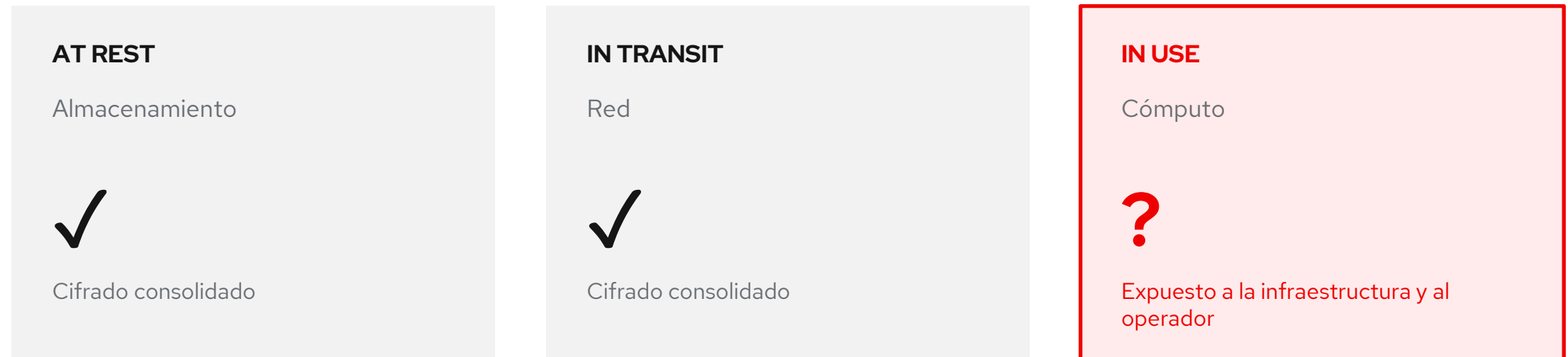
La pregunta ya no es solo «¿está seguro?»

Es «¿puedo colaborar sin ceder el control?»



La pieza que faltaba: proteger el dato en uso

Llevamos años cifrando el dato almacenado y en tránsito; el momento del procesamiento seguía expuesto



Confidential Computing extiende la protección al momento en que el dato está siendo procesado.



De confiar en el operador a verificar el entorno

La confianza deja de depender únicamente de quién opera la infraestructura

Modelo tradicional

Workload + datos

se ejecutan sobre la infraestructura de un operador

Garantía: contratos, auditorías, reputación

Base de la confianza: la organización

Confidential Computing

Workload + datos

se ejecutan en un entorno protegido y aislado

Garantía: atestación remota y verificable

Base de la confianza: la evidencia técnica

Un tercero puede procesar mis datos sin que yo tenga que confiar en él: me basta con verificar el entorno.



Confidential Containers en OpenShift

Llevar las garantías de confidencialidad al modelo de despliegue que ya usamos

Aplicación / workload

Confidential Container (CoCo)

OpenShift / Kubernetes

Hardware de Confidential Computing

Qué aporta

Sin rediseñar la aplicación: el mismo pod, con aislamiento por hardware.

Atestación integrada: el entorno demuestra su integridad antes de recibir datos o claves.

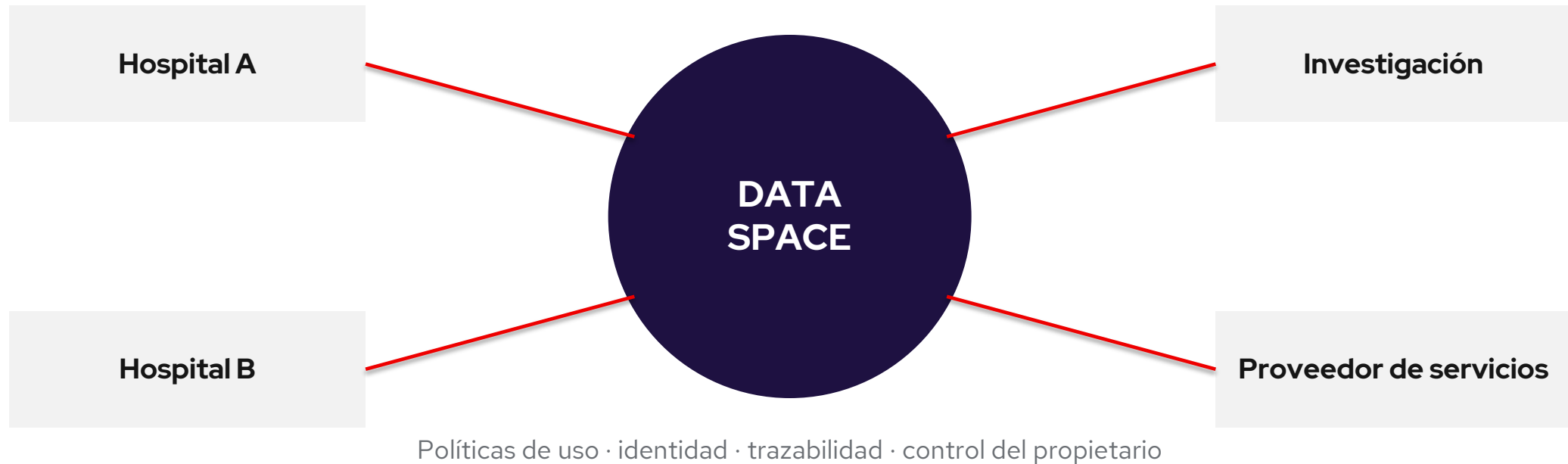
Operación conocida: el equipo de plataforma sigue trabajando con OpenShift.

Confidencialidad como una propiedad más de la plataforma, no como un proyecto aparte.



Espacios de datos: compartir valor sin ceder soberanía

Confidential Computing resuelve el procesamiento; los espacios de datos resuelven el gobierno



Juntos hacen posible procesar datos de varias organizaciones sin que ninguna ceda el control.





Iván Gutiérrez Agüero

Head of Frontier Cybersecurity
TECNALIA Research & Innovation

Actitud

**Confidential Containers en OpenShift como
garantía técnica más allá de la obligación legal.**

Confidentiality is our enabler.





El enemigo silencioso

¿En qué condiciones podemos confiar en un sistema que, por diseño, ya asumimos comprometido?

La búsqueda de la confianza total en entornos de desconfianza.



¿Qué ocurre cuando necesitamos cooperar?

- a) Miedo
- b) Rechazo
- c) Compartición de datos no controlada



De confiar en la **infraestructura**

Compartir datos

A verificar la **ejecución**

Compartir resultados



Black box de computación

Creamos soluciones confidenciales para mejorar los ecosistemas de innovación ***de forma estructural.***



Analiza datos sensibles sin exponerlos.

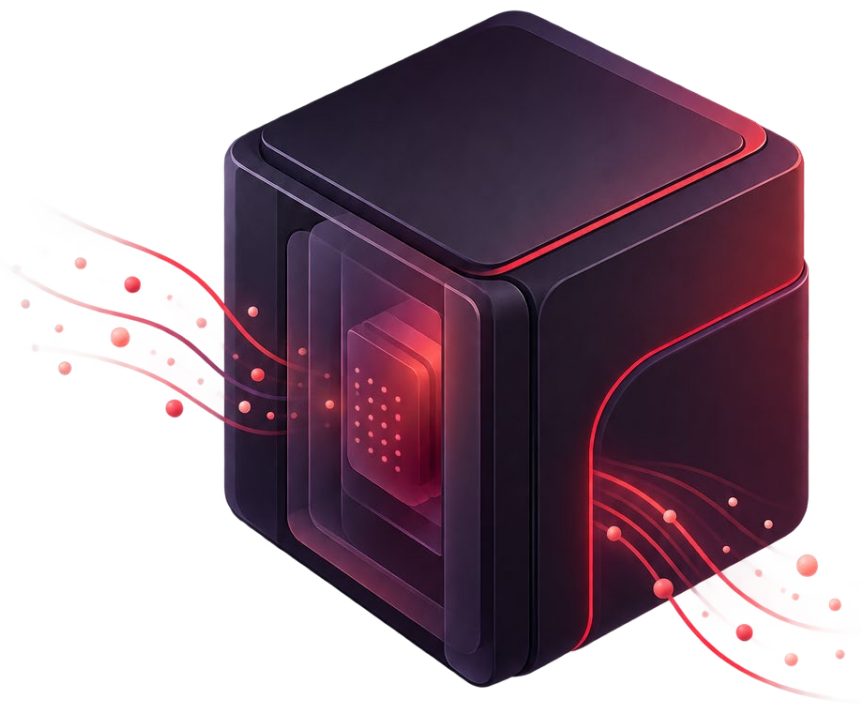


Crea valor compartido entre organizaciones.



Black box de computación

Self-Proving Secure Processing Environment

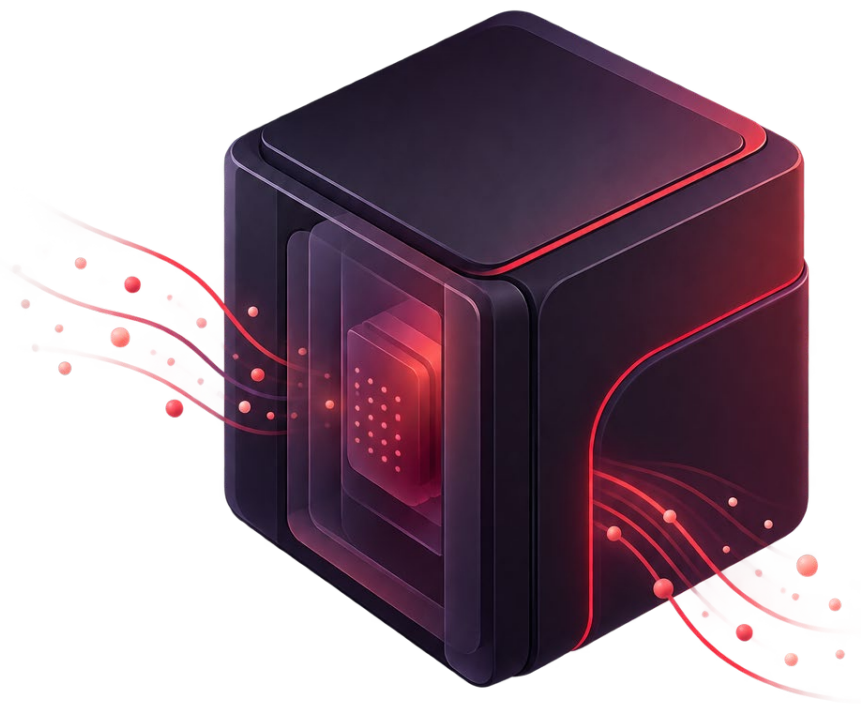


1. Un data holder debe habilitar el acceso a sus datos a través de un SPE. **No es opcional.**
2. Art. 73 "state-of-the-art measures": **Un SPE sin computación confidencial** cumple el texto, no la intención.
3. Riesgo: **Conviven dos activos** en un solo operador.



Black box de computación

Self-Proving Secure Processing Environment



4. Solución: Ocultar datos, algoritmos y material criptográfico. **Exponer resultados.**
5. Todo se procesa en un punto de encuentro que **no pertenece a los propietarios.**
6. **La confianza se reemplaza por evidencia.**
Aunque falle todo lo demás.
7. El implementing act vendrá a codificar lo que ya estamos haciendo.





DEMO





Connect

tecnal:a

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

La Confidencialidad es nuestro Motor ¿Y el tuyo?

La capacidad de computar sin exponer datos
definirá quién puede colaborar, innovar y escalar.



Soberanía del dato



Nuevos modelos de colaboración



Connect

Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



x.com/RedHat

tecnal:a

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

