

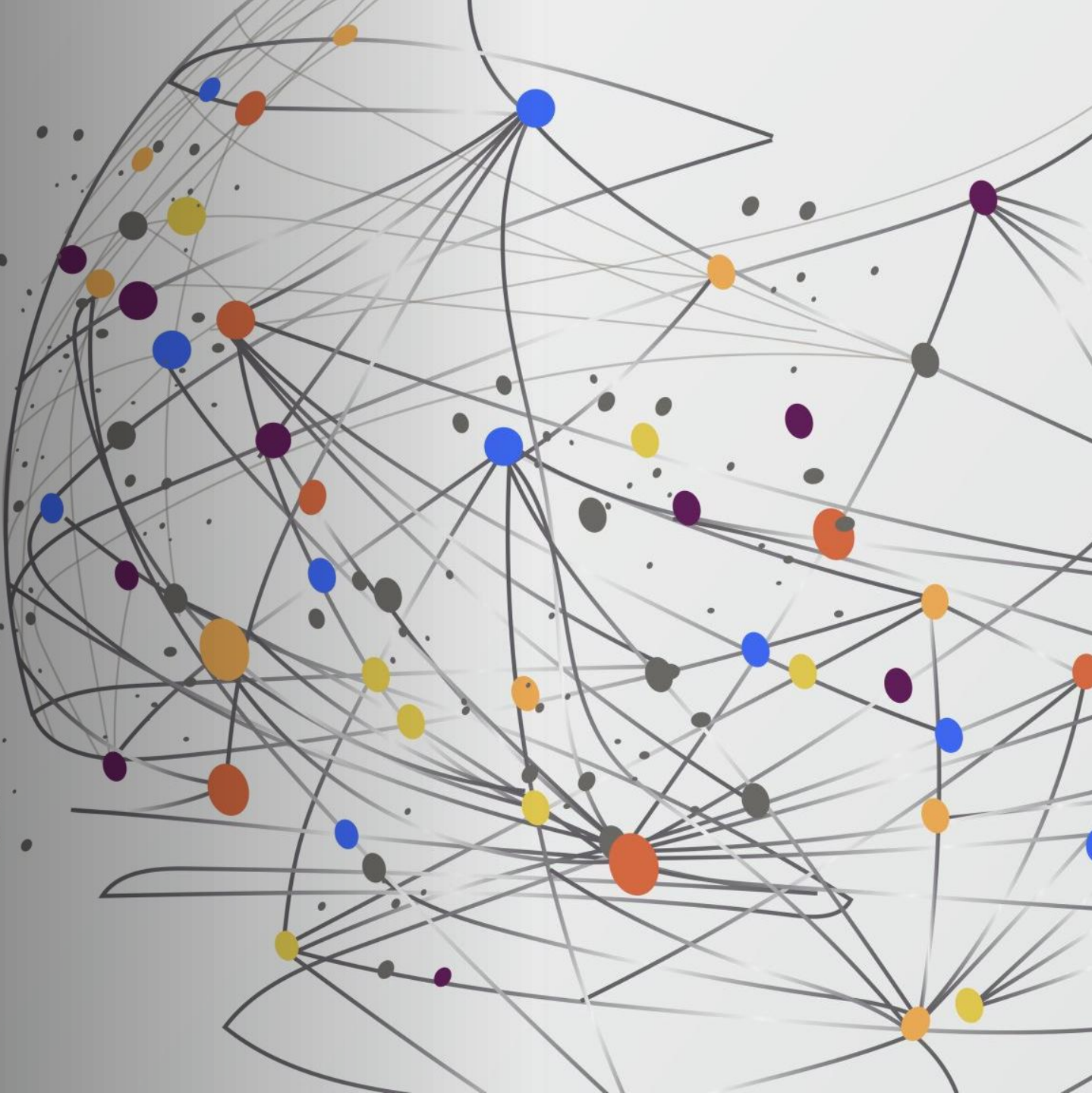
Resiliencia digital y soberanía tecnológica en sanidad: la capacidad de cuidar cuando todo falla

DIRECCIÓN GENERAL DE PLANIFICACIÓN, ORDENACIÓN,
GESTIÓN DEL CONOCIMIENTO Y SALUD DIGITAL

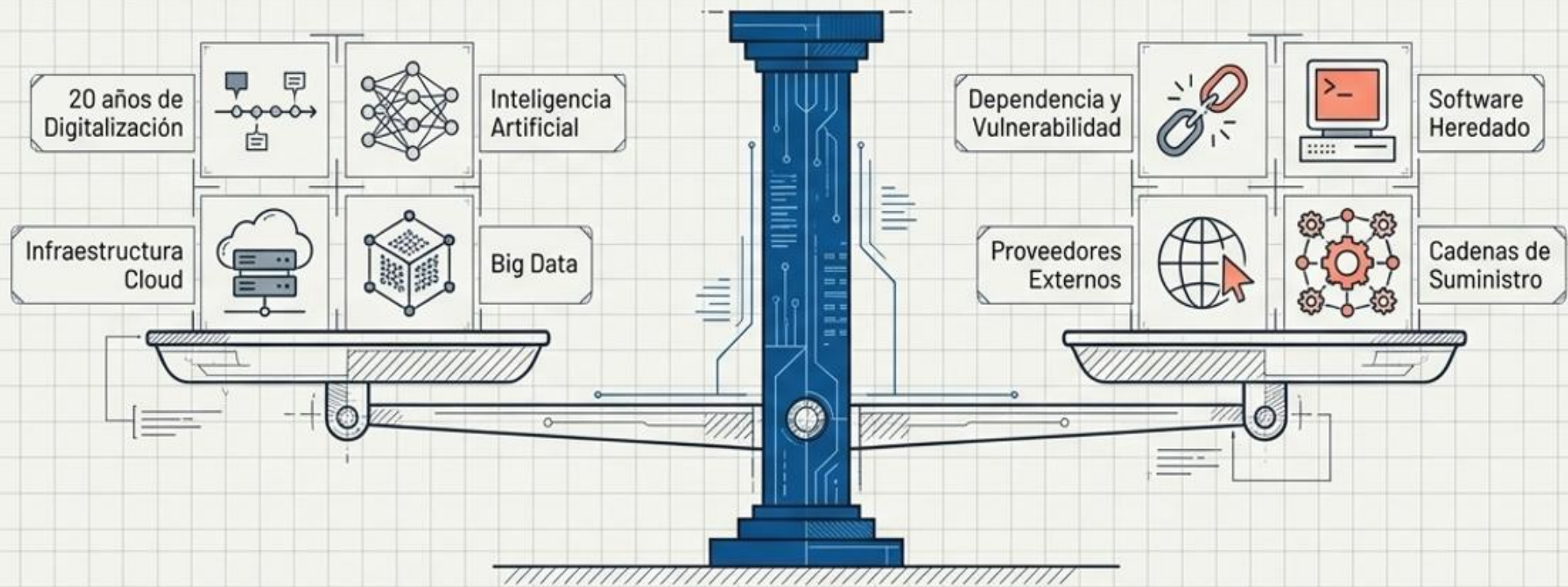
GOBIERNO DE CANTABRIA

Revista Sociedad de la Información Digital

Madrid, 13 de octubre de 2026



A mayor digitalización, mayor dependencia tecnológica

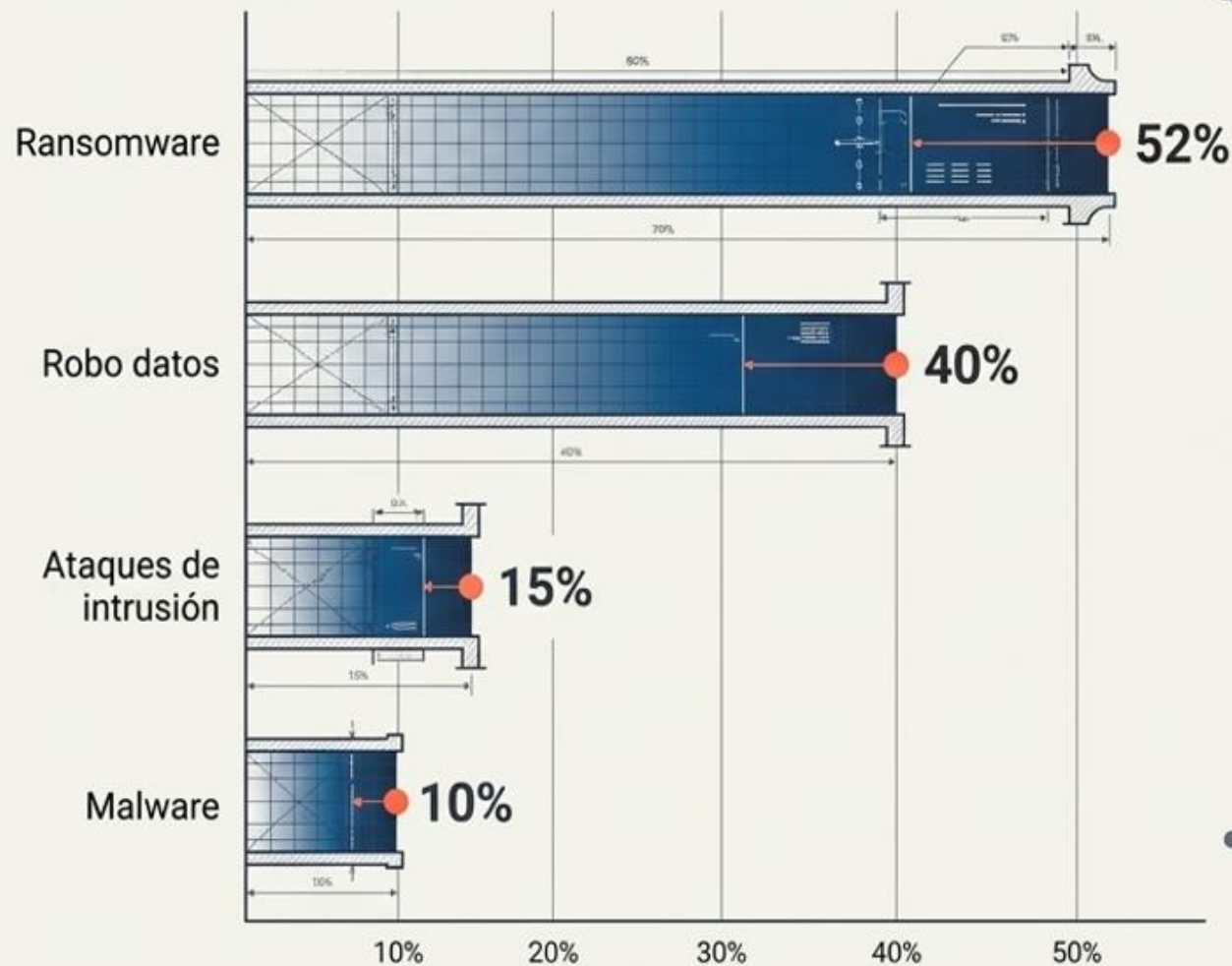


El éxito de las últimas dos décadas ha creado nuestra mayor vulnerabilidad estructural. La dependencia del software, los proveedores, las infraestructuras cloud y las cadenas de suministro exige un cambio de paradigma hacia la soberanía tecnológica.

El sector sanitario como objetivo principal de la ciberdelincuencia

+40%

de incremento en ataques de secuestro de datos (Ransomware) en el sector salud en España.



El cambio de **paradigma:** **De la protección a la resiliencia**

Enfoque Tradicional (Ciberseguridad Reactiva)



Visión de la tecnología:
Herramienta operativa.



Objetivo principal: Evitar la brecha de datos (Compliance).



Respuesta al ataque: Apagón preventivo y parálisis clínica.



Metodología: Auditorías estáticas anuales.

Enfoque de Resiliencia (Soberanía Tecnológica)



Visión de la tecnología:
Infraestructura Crítica Nacional.



Objetivo principal: Garantizar la capacidad asistencial continua.

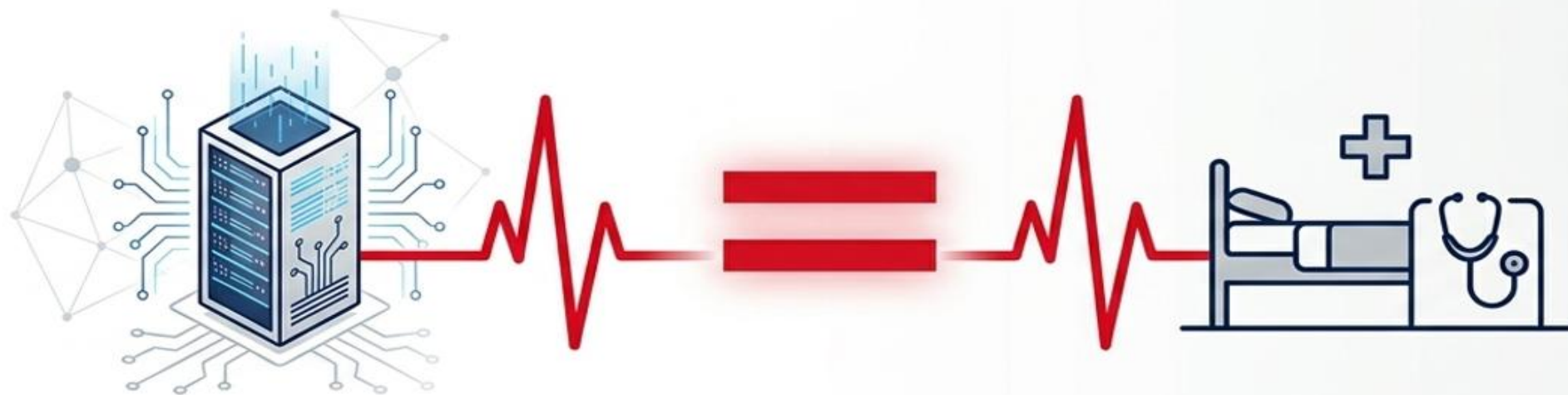


Respuesta al ataque: Contención aislada y asistencia ininterrumpida.



Metodología: Simulación continua y Gemelos Digitales (Cyber Range).

¿Puede recuperarse el Sistema?
¿Puede mantenerse la asistencia clínica mientras se recupera?

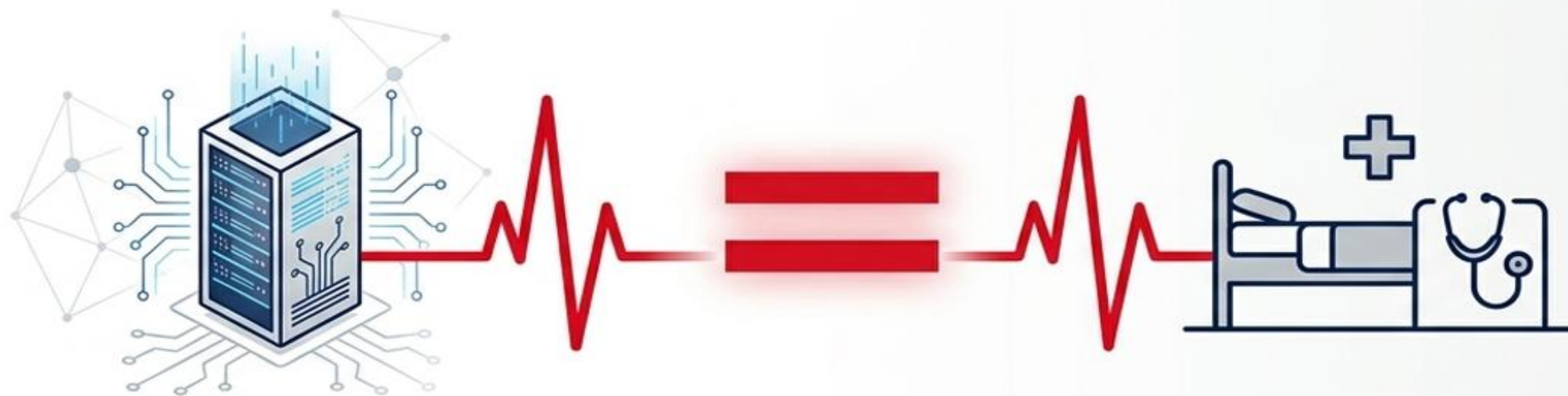


**RESILIENCIA
DIGITAL**

**CAPACIDAD
ASISTENCIAL**

**La ciberseguridad ya no es un centro de costes informáticos;
es el garante del latido del hospital.**

¿Puede recuperarse el Sistema?
¿Puede mantenerse la asistencia clínica mientras se recupera?



**RESILIENCIA
DIGITAL**

**CAPACIDAD
ASISTENCIAL**

La ciberseguridad ya no es un centro de costes informáticos;
es el garante del latido del hospital.

El marco normativo:

De la recomendación a la obligación legal

 Directiva SRI2 / NIS2 (Europa)	ENS (España)
• Directiva (UE) 2022/2555 (14 dic 2022). • Objetivo: Nivel común de ciberseguridad en todos los Estados Miembros. • Clasificación: Define al Sector Salud como infraestructura de “alta criticidad”, imponiendo controles técnicos y organizativos estrictos.	• Esquema Nacional de Seguridad (Real Decreto 311/2012). • Objetivo: Condiciones necesarias para la confianza en el uso de medios electrónicos. • Aplicación en Cantabria: Prioridad absoluta alcanzar la Certificación de Conformidad ENS a nivel ALTO. 

El objetivo de alto valor: Hospitales como infraestructuras críticas



La Arquitectura de Resiliencia

Alineación Nacional (SNS)

Estrategia de Salud Digital
(2021-2026)

Estrategia de Ciberseguridad
(2025-2028)

Plan Marco de Contingencias

Participación activa en Subcomisión de Ciberseguridad y grupos de trabajo nacionales.

El Núcleo Estratégico

Plan de Salud Digital de Cantabria 2024-2027

Eje 3.3: Seguridad de la Información y Protección de Datos

[Normativo]

[Organizativo]

[Tecnológico]

Acción Táctica e Infraestructura

Respaldo y Continuidad

Infraestructuras del Centro de Datos del Hospital de Sierrallana (Nuevos servicios de respaldo).

Securización Clínica

Inversión en protección de aplicaciones, puestos de trabajo y dispositivos médicos.

Plan de Salud Digital 2024-2027: Inversión en Ciberseguridad

En el marco del Plan de Salud Digital 2024-2027 (Eje 3: Gobernanza TIC, Línea 3.3), se impulsa la protección de datos y la seguridad de la información en el entorno sanitario mediante financiación pública y propia.

Financiación Externa y Ciberseguridad

1,6 M€
en Fondos Europeos
Next Generation
(PRTR)



WAF, licencias
antivirus



tecnología
packet broker



Seguridad Integral

1 M€ del Fondo
de Sostenibilidad
Farmaindustria

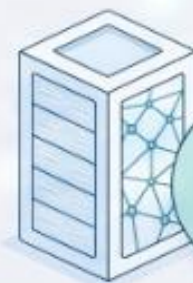


Oficina de
Ciberseguridad
del SCS



Alta disponibilidad

Continuidad del Negocio y Proyectos Clave



**Fondos Propios para la
Continuidad Operativa**



Sistema BRS:
Balanceo y redundancia
en alta disponibilidad

Innovación Operativa y Acceso Seguro



Despliegue piloto
de dispositivos
electromédicos IoT



Acceso VPN
con doble factor



Protección Técnica

Vigilancia digital activa, detecciones del antivirus y resumen de eventos de protección de equipos.



El Factor Humano

Auditoría humana: Acciones formativas OSI y resultados de campañas de simulacro de Phishing.



Respuesta

Gestión reforzada de incidentes y monitorización de reportes por correo electrónico.



Transparencia Organizativa

Cultura de seguridad: Los informes se divulgan proactivamente entre todo el personal del SCS.

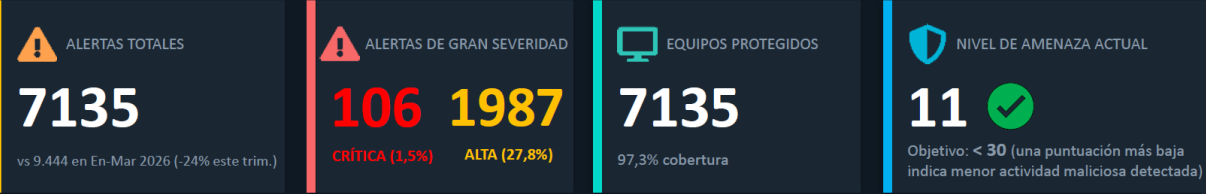
OSI: Impulsor de Seguridad

Reporte Trimestral de Datos Visuales

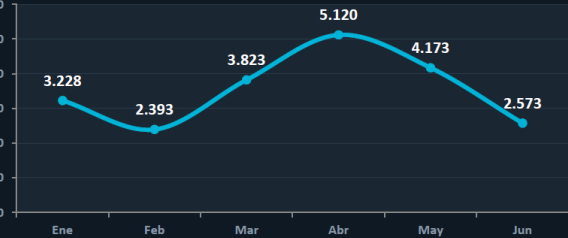
Monitorización 24x7 & Cumplimiento ENS

Resumen de eventos de protección de equipos

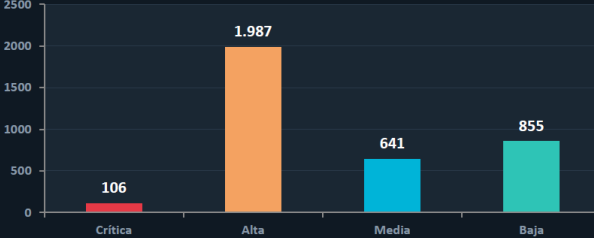
Alertas, protección y exposición de los equipos monitorizados en el antivirus Falcon Crowdstrike



Número de alertas totales detectadas (6 meses)



Severidad de las alertas detectadas (se excluyen alertas informativas)



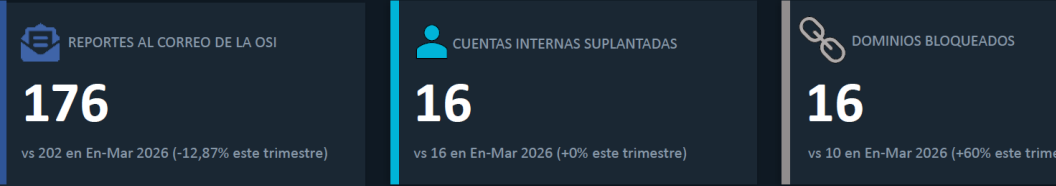
Acciones formativas OSI

Eventos formativos programados anualmente como cursos en Moodle, formaciones presenciales y simulacros de phishing

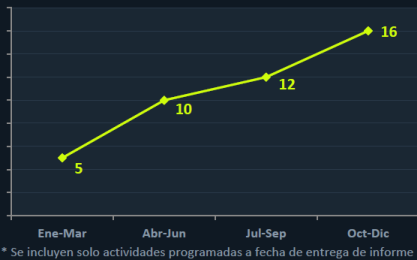


Incidentes y otros reportes por correo electrónico

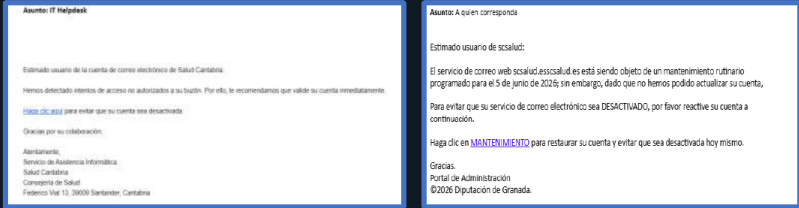
Phishing, spam y otros reportes atendidos en el buzón de seguridadTIC@scsalud.es



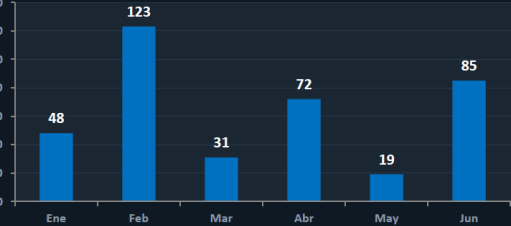
Programación formativa 2026 (trimestral) *



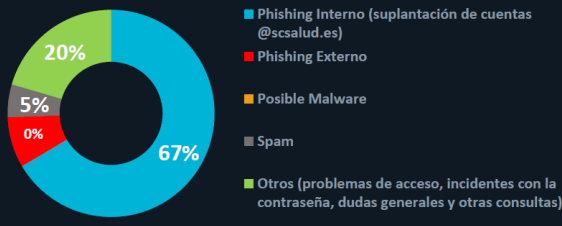
Últimas campañas de phishing activas:



Evolución de reportes atendidos en el buzón de correo

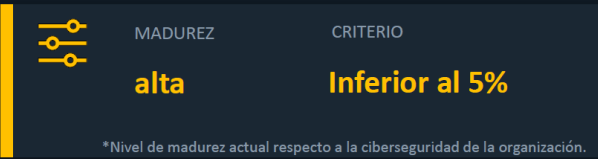
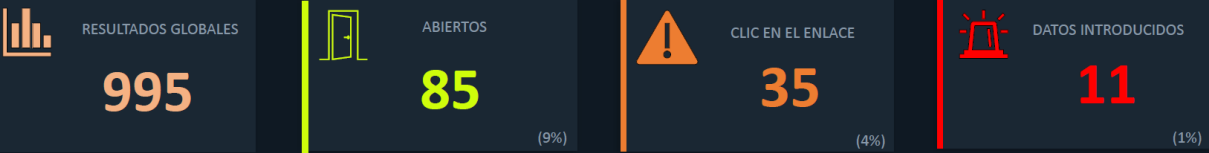


Tipo de reportes atendidos según su categoría



Resultado Campaña Simulacro Phishing

Resultados del simulacro phishing realizado en mayo.



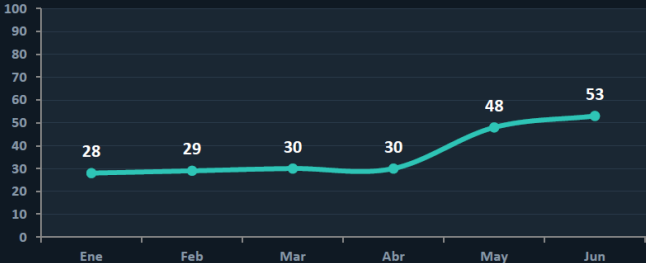
Monitorización 24x7 y cumplimiento Esquema Nacional de Seguridad



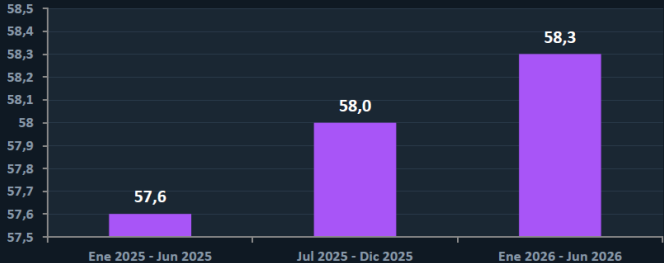
Centro de operaciones de seguridad 24x7, cumplimiento del Esquema Nacional de Seguridad y puntuación de dispositivos médicos conectados



Porcentaje de cumplimiento Esquema Nacional de Seguridad (6 meses)



Puntuación de seguridad en dispositivos medicos conectados (semestral)



Más allá de la defensa: Innovación proactiva con C-SHIELD

Cantabria Smart Health Infrastructure for Emergency Leadership & Defence



Co-funded by the
European Union



Programa: Europa Digital (DIGITAL)
del Centro Europeo de Competencia
en Ciberseguridad (ECCC).

Duración: 2 años.

Presupuesto Total: 1.268.534 €
(Subvención europea: > 634.000 €).

Consortio multidisciplinar:

Servicio Cántabro de Salud, Consejería de Salud, Grupo de Ingeniería Telemática (Univ. de Cantabria) y Oficina de Proyectos Europeos.



Los 4 pilares operativos del proyecto C-SHIELD



Co-funded by the
European Union

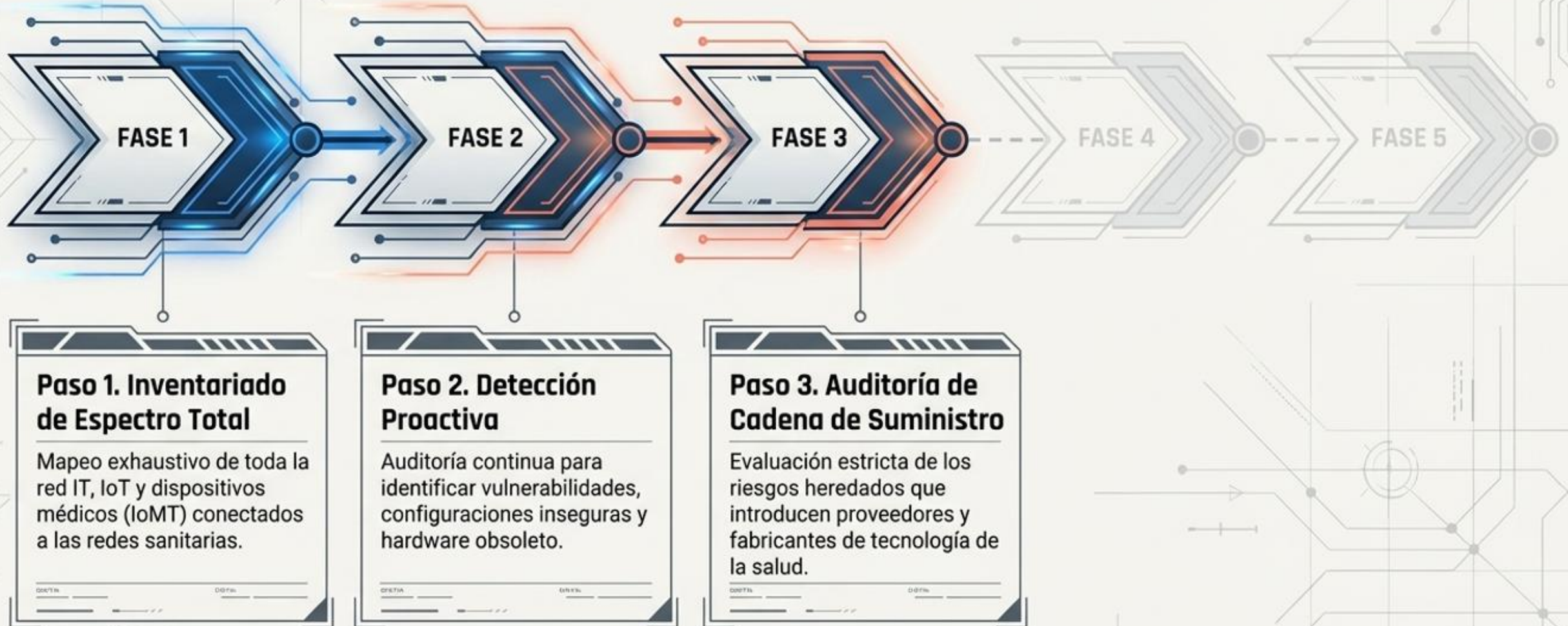


ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

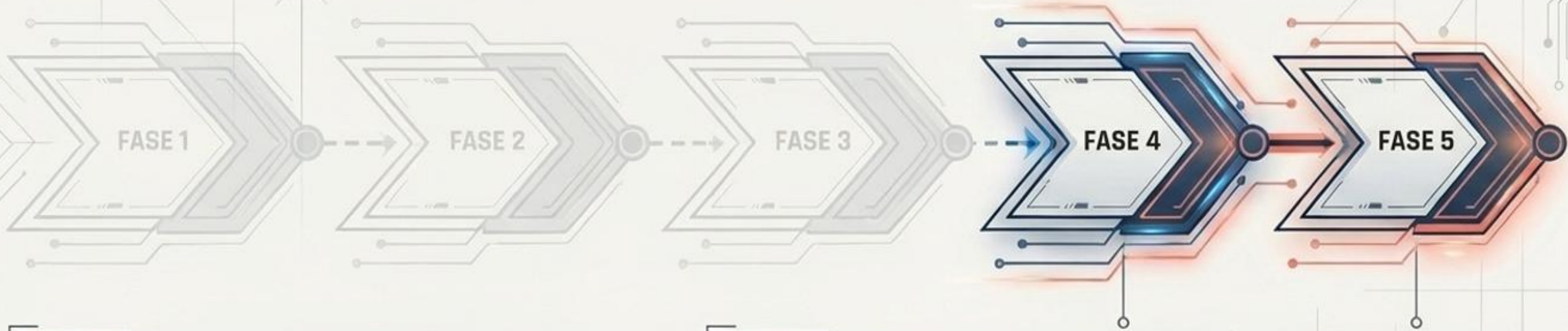


GOBIERNO
de
CANTABRIA
CONSEJERÍA DE SALUD

El Playbook C-SHIELD: Fases de Despliegue Táctico (1/2)



El Playbook C-SHIELD: Fases de Despliegue Táctico (2/2)



Paso 4. Mitigación en Entorno Aislado (Cyber Range):

Diseño y ejecución de pruebas de estrés sobre las soluciones diseñadas antes de su pase a producción.

Paso 5. Empaquetado y Cooperación:

Creación de una metodología estandarizada y repetible para compartir con otras redes sanitarias a nivel nacional y europeo.

La Innovación Estructural: El “Cyber Range” Sanitario

Diseñar y probar medidas de mitigación en un entorno seguro antes de su despliegue real.

Hospital Físico Clínico



Gemelo Digital
(Universidad de Cantabria)



Escenario 1:
Campañas de phishing masivo.



Escenario 2: Propagación de malware a través de equipos médicos (IoMT).



Escenario 3:
Estrés de red y caídas de disponibilidad.

Pruebas de estrés extremo con cero impacto en la actividad clínica real.

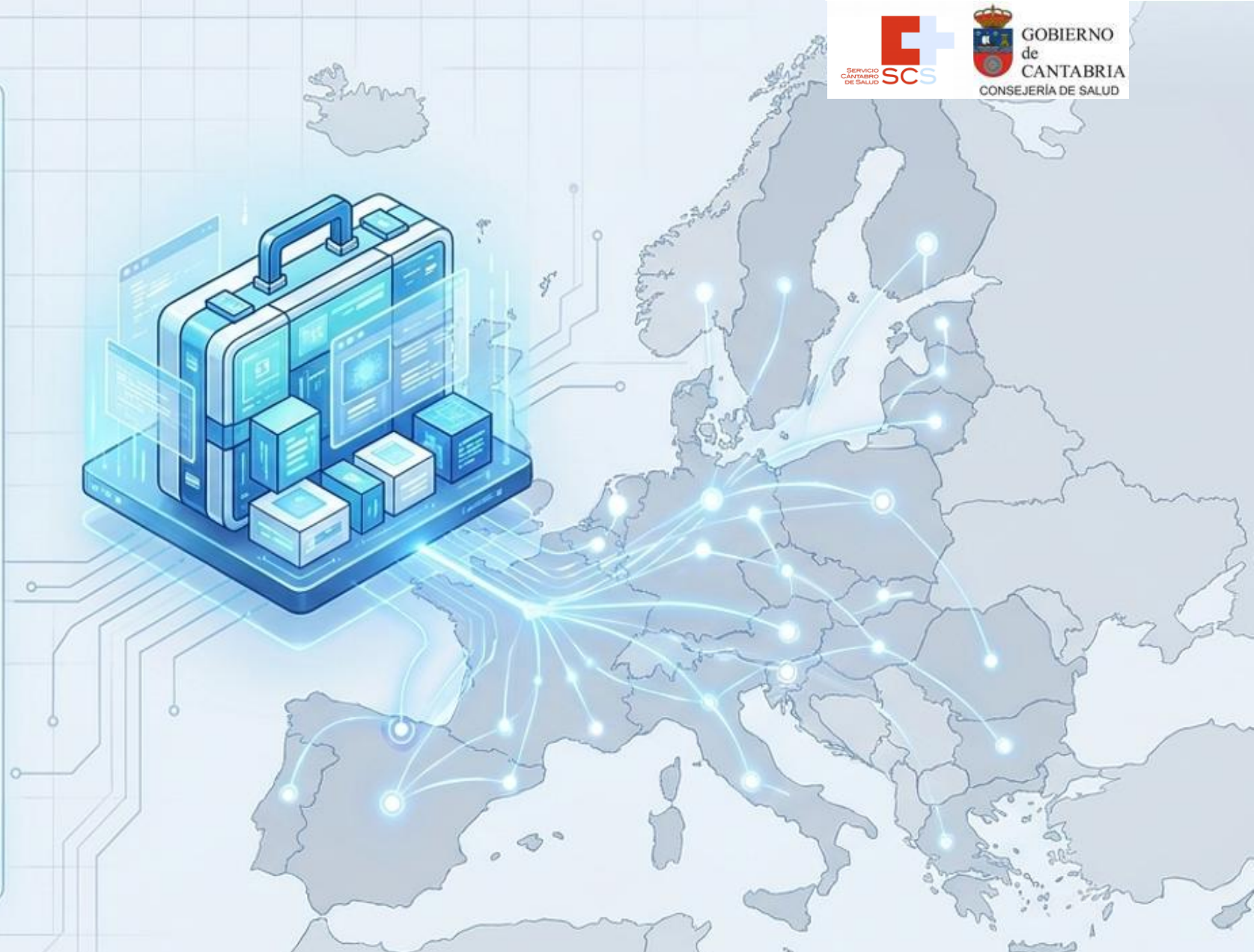
Impacto Europeo: El Paquete de Replicabilidad



El objetivo final de C-SHIELD no termina en Cantabria.

El proyecto entregará un **Paquete de Replicabilidad** metodológico integral.

Diseñado específicamente para que otras regiones de la Unión Europea puedan adoptar, de forma **sostenible sostenible y repetible**, el modelo de Cantabria para proteger sus propias infraestructuras hospitalarias.



El horizonte europeo:

Paquete de **Soberanía Tecnológica** (Junio 2026).
La resiliencia local requiere independencia continental.

Reglamento de Chips 2.0

Impulso masivo a la producción y diseño de semiconductores críticos directamente en suelo europeo.



Ley de Computación en la Nube y IA



Plan de Acción «Continente de IA»:
Objetivo de triplicar la capacidad de los centros de datos en Europa en 5-7 años.

Estrategia Open Source



Reducción de la dependencia de cajas negras de software propietario mediante estándares de código abierto.

El cambio real exige que la financiación llegue tanto a la industria como a las Administraciones Públicas para la renovación tecnológica.

El diseño clínico está trazado; la ejecución es nuestra responsabilidad.

Gracias por su atención

María del Mar Ortiz Marqués