

Despliegue de un Centro de Operaciones de Ciberseguridad en un entorno sanitario crítico

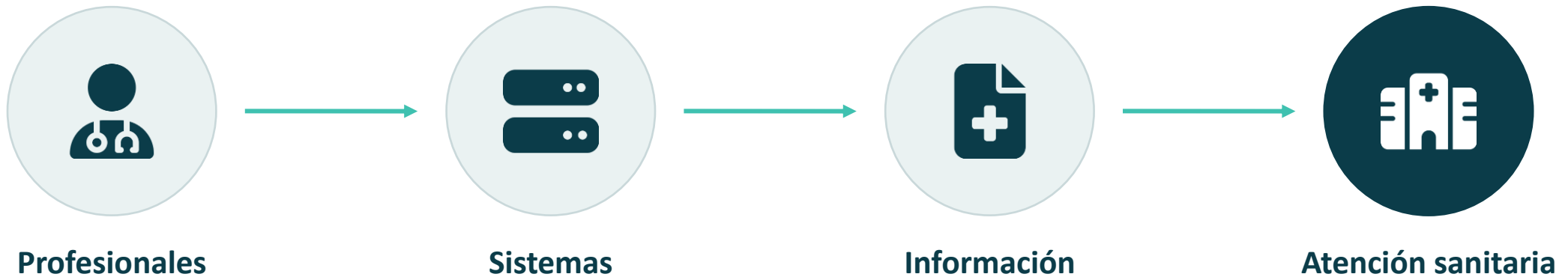
Experiencia y retos del Servicio Extremeño de Salud

Chesco Romero Ciborro

Responsable de Seguridad y de la Oficina de Ciberseguridad
Servicio Extremeño de Salud

15 de octubre de 2026
Escuela de Administración Pública de Extremadura

La ciberseguridad sostiene la asistencia



Continuidad · Confianza · Resiliencia

En sanidad, un incidente de ciberseguridad puede convertirse en un problema asistencial.

Qué es el COC del SES



Acuerdo Marco regional de la Junta de Extremadura · SES, tenant principal

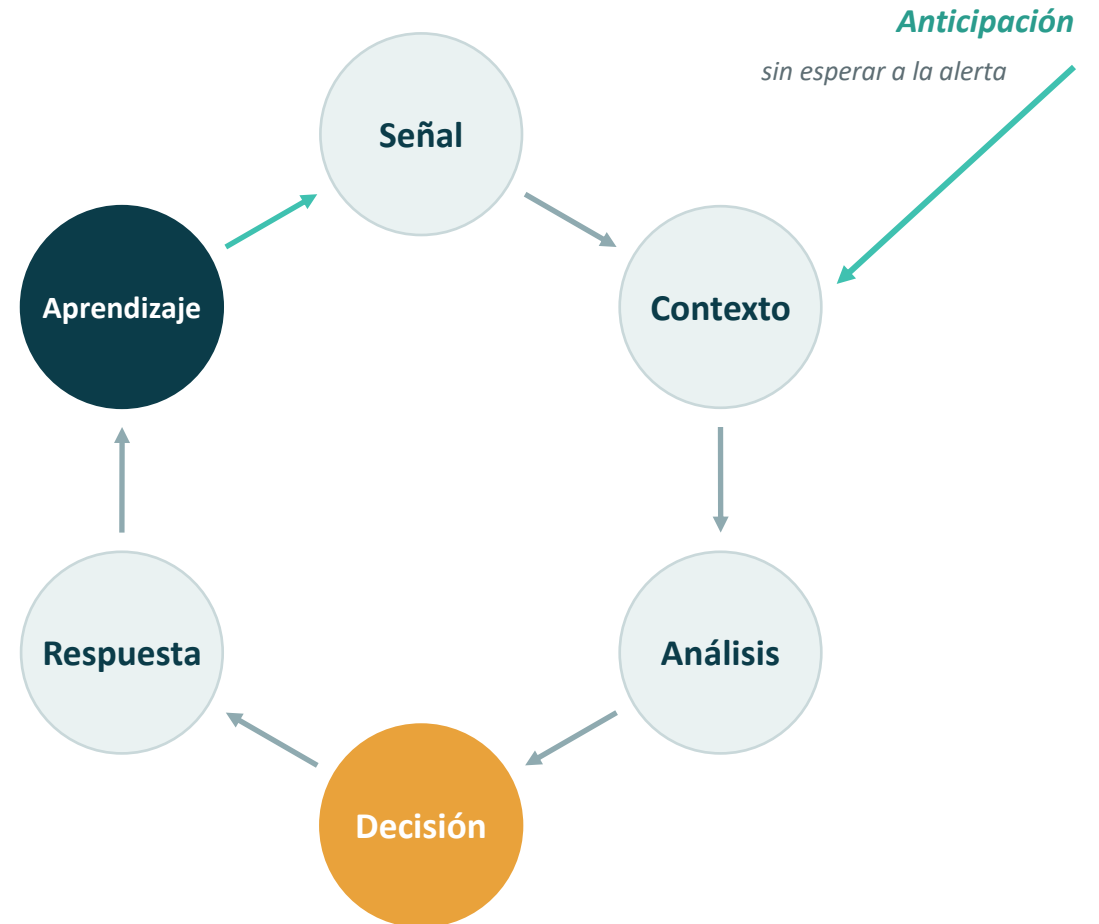
De la señal al aprendizaje

Detectar no es el final del proceso.

Es el comienzo de una decisión.

La respuesta se ejecuta según procedimientos y con autorización del SES.

Anticipación: inteligencia de amenazas · búsqueda proactiva · vigilancia digital



El SOC, núcleo operativo del COC



SOC

- Vigilancia continua 24x7
- Triage, análisis y escalado
- Coordinación técnica de la respuesta

COC

- El SOC y los servicios bajo demanda: respuesta a incidentes graves, soporte especializado
- Equipos del SES: sistemas, comunicaciones, aplicaciones
- Relación con el CCN y gobierno del conjunto

El SOC opera y coordina. El COC integra, gobierna y evoluciona.

Lo que estamos aprendiendo

01 Desplegar no es instalar

02 Migrar no es copiar

03 Recibir datos no es vigilar

04 El COC compite por los mismos recursos

05 La seguridad obliga a ordenar procesos

Externalizar servicios no es externalizar el gobierno

Se pueden contratar servicios.
No se puede contratar la responsabilidad.

Dirección y gobierno del SES

Coordinación y seguimiento

Operación y servicios especializados



¿Quién decide, autoriza, ejecuta y responde?



Trazabilidad de la alerta al cierre



Procedimientos que se ajustan mientras se usan



Conocimiento propio: formación y transferencia

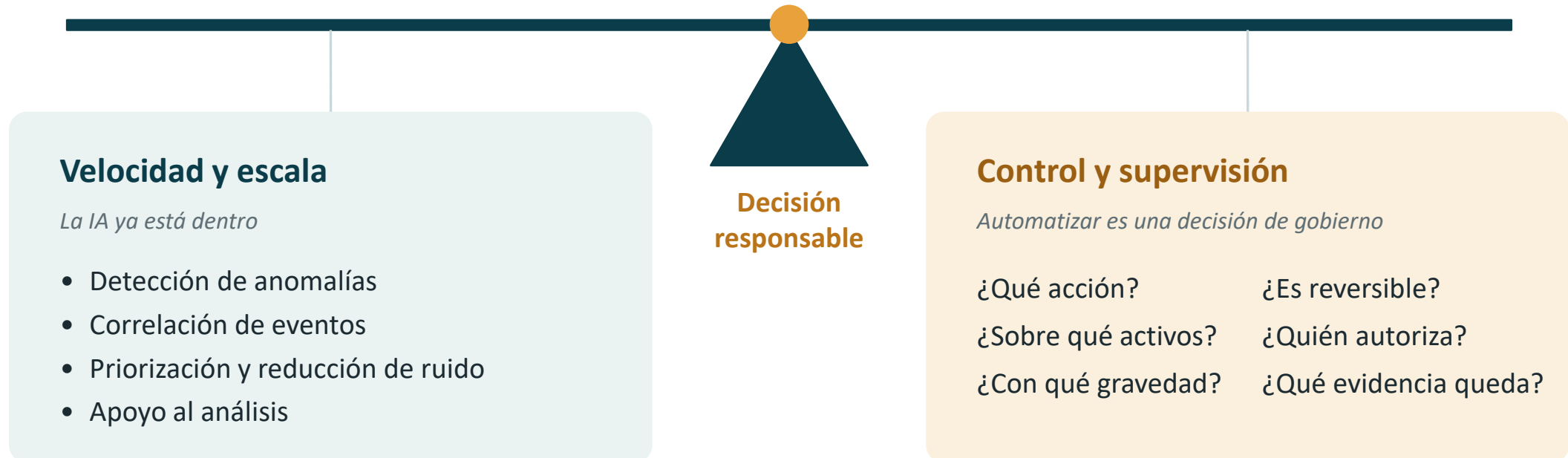


Datos personales protegidos también dentro del COC

Marco: Esquema Nacional de Seguridad (RD 311/2022)

IA y automatización bajo gobierno

La IA multiplica la capacidad humana. **No sustituye la responsabilidad.**



Cinco retos y una finalidad



El objetivo no es gestionar más alertas. **Es proteger la continuidad de la asistencia.**