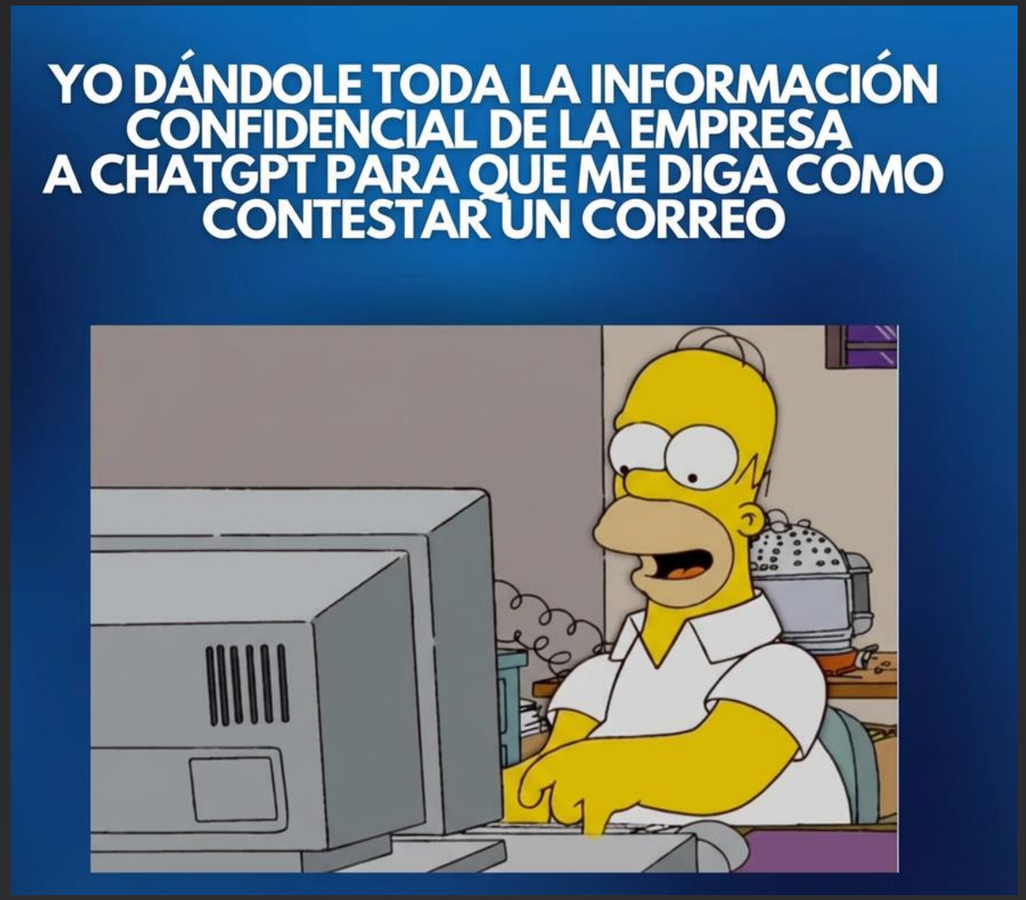
¿Está preparada la Sanidad para los retos de la IA y la nueva ciberamenaza?



Un enfoque continuo y estratégico para la protección de servidores en el Sistema Nacional de Salud

INTRODUCCIÓN

El desafío de la seguridad continua

Como Administradora de Sistemas en el ámbito sanitario, la ciberseguridad no es un producto que se adquiere una vez y se olvida. Es un proceso vivo, dinámico y circular que requiere vigilancia constante.

La seguridad efectiva se basa en la práctica diaria, la monitorización activa y la mejora continua de nuestros sistemas críticos.

Como Administradora de Bases de Datos, el mantenimiento y seguridad no son tareas puntuales. El proceso continuo de optimización, respaldo y protección de la información crítica.

La integridad y disponibilidad de los datos dependen de la vigilancia constant y las mejores practices.

La mejor Forma de minimizar riesgos es previniendolos, y eso comienza por una formación y concienciación con los usuarios.

INFRAESTRUCTURA

El Contenedor: Disponibilidad y Defensa

La estrategia del SNS establece requisitos específicos para garantizar la seguridad de nuestra infraestructura crítica.

Virtualización segura

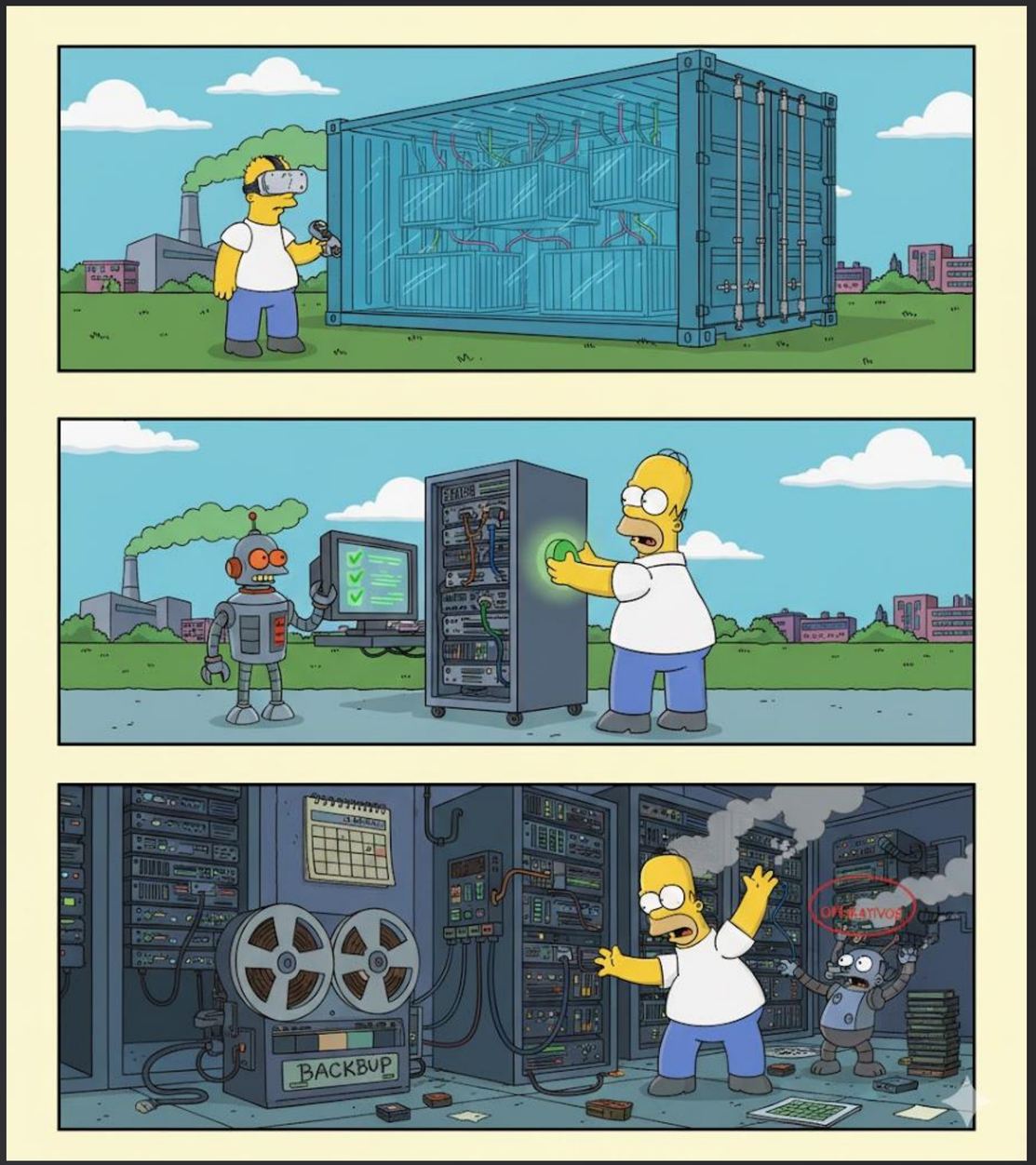
La Estrategia del SNS enfatiza la importancia de la segmentación como barrera fundamental de defensa

Despliegues seguros

Ningún sistema se despliega sin superar los checks de seguridad establecidos por el SNS

La última frontera: Backup

La estrategia nacional nos obliga a mantener planes de recuperación ante desastres (DRP) operativos



La Estrategia del SNS 2025-2028 como motor de mejora

En lugar de ver la nueva estrategia como un conjunto de reglas restrictivas, debemos concebirla como el motor de mejora continua que impulsa la excellences operativa en nuestros sistemas sanitarios.

Gobernanza

Definir claramente quién hace qué cuando un servidor crítico falla

Vigilancia

Mirar hacia fuera para identificar amenazas y hacia dentro para detectar vulnerabilidades

Cultura

Conseguir que cada professional entienda que un USB conectado amenaza nuestros servidores

⚠ ALERTA CRÍTICA

El Caballo de Troya: IA y privacidad de datos

Términos y condiciones: El peligro de la IA "gratuita"

Cuando el servicio es gratis, el historial clínico de los pacientes es el precio

El mejor USB de usuario es aquel que no se conecta y el Dato más protegido aquel que no reside en ninguna IA.

Comparativa de modelos de IA en entornos sanitarios

IA Abierta

Modelo: "Tus datos entrenan mi modelo global"

Conclusión: Inviable en el SNS por exposición de datos sensibles

IA Enterprise

Modelo: "Tus datos están aislados y protegidos"

Conclusión: Requiere contrato específico con garantías legales y técnicas

IA en VM Local

Modelo: "El dato nunca sale del hospital"

Conclusión: Nuestra apuesta estratégica para cumplir con el SNS

Pilares de la Estrategia Nacional

01

Gobernanza efectiva

Estructura clara de responsabilidades y toma de decisiones

02

Vigilancia activa

Monitorización proactiva de amenazas internas y externas

03

Cultura de seguridad

Concienciación transversal en toda la organización sanitaria

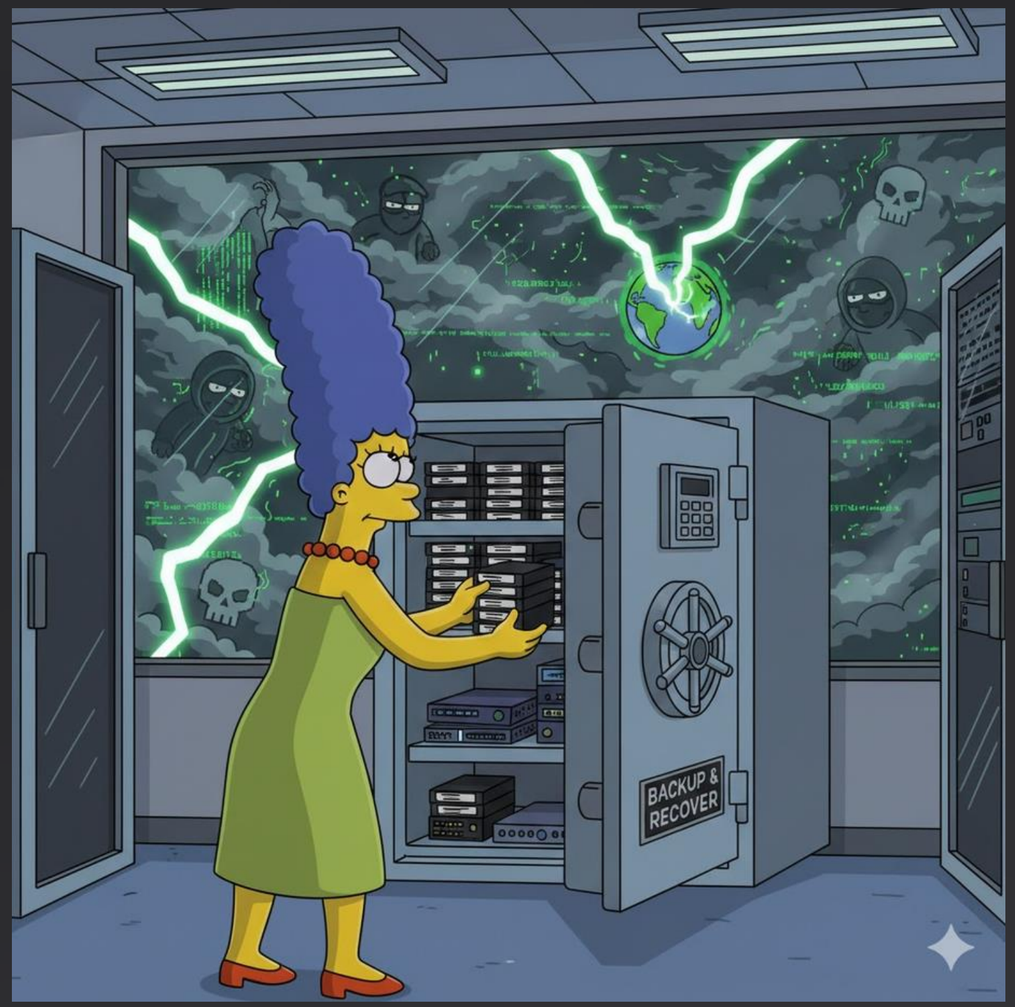
04

Concienciación Integral

Formación efectiva en todos los niveles para los diferecntes USUARIOS.

La última frontera: Backup

Un BACKUP no es un plan de continuidad; es solo una herramienta. El plan es saber qué hacer cuando la "tormenta de hackers" golpea la Puerta. La Improvisación para el mundo del Teatro.



No se trata de guardar los datos, sino de cuánto tardas en volver a trabajar.

- **RTO** (Recovery Time Objective): ¿Cuánto tiempo puede estar Springfield sin luz antes del caos?

- **RPO** (Recovery Point Objective): ¿Cuántos datos estamos dispuestos a perder? (¿Los últimos 5 minutos o todo el día de trabajo?).

Conclusiones: La seguridad como ejercicio continuo

La Ciberseguridad es un proceso, no un producto

Requiere vigilancia constante, actualización continua y compromiso organizacional

La Estrategia del SNS 2025-2028 es nuestra hoja de ruta

Gobernanza, vigilancia, concienciación y cultura son los pilares de nuestra defensa

La IA requiere soluciones locales y controladas

Solo así garantizamos la privacidad absoluta de los datos sanitarios de nuestros pacientes