

## CASO DE USO

SALUD

# PROTECCIÓN DE HISTORIALES MÉDICOS

El caso de un centro hospitalario: protección de los historiales de los pacientes, consultados desde un parque de clientes ligeros.



ZONECENTRAL



## REQUISITOS

Según impone un decreto, solo los titulares de una tarjeta de profesional sanitario pueden acceder a los historiales médicos. Este centro quería ir más allá y **proteger también los datos contra el robo y las filtraciones y, por lo tanto, proteger los datos en sí mismos.**

La solución debe adaptarse a un sistema de información compuesto de **45 servidores de Windows, varios SAN, dos directorios AD, 20 servidores Citrix™ y varios cientos de clientes ligeros Wyse.**

Las limitaciones de rendimiento y de capacidad de carga son primordiales. De hecho, las torres de servidores Citrix™ **albergan sesiones de usuarios simultáneamente:** los clientes ligeros Wyse, instalados en todo el hospital, **disponen de un lector de tarjetas con microprocesador** para autenticar al personal sanitario y permitirle acceder a los historiales médicos de los pacientes. La solución debe **segmentar los datos en un entorno multiusuario**, según la función y el rol del individuo (personal sanitario o administrativo). El producto debe ser independiente de la tecnología de almacenamiento.

## SOLUCIÓN

Así, el cliente eligió el producto **ZONECENTRAL** por:

- + Su **compatibilidad con la arquitectura Citrix™:** a pesar de picos de carga con hasta 120 usuarios simultáneos en una misma zona de cifrado, la solución es perfectamente estable.
- + Su respuesta a la **necesidad de un cifrado multiusuario.**

## EXPERIENCIA

Se aplicó una serie de procedimientos con el fin de **garantizar la separación de las funciones:**

- + El DSI gestiona los certificados.
- + Los profesionales gestionan el derecho a saber.
- + El responsable informático tiene acceso a las zonas de cifrado para su mantenimiento, pero no tiene acceso al contenido legible que contienen.

## + VENTAJAS

Ahora el establecimiento no solo puede respetar la obligación de controlar el acceso a los datos médicos, sino que también puede perfeccionar la separación de roles gracias al cifrado: los datos solo serán accesibles al personal autorizado y su manipulación estará supervisada.

La recuperación, una etapa crucial, también está muy controlada: ningún administrador puede descifrar los datos por sí solo. Para ello, será necesario implicar al jefe de Seguridad de la Información (para acceder a los datos de recuperación), el servicio médico (para el código PIN de la tarjeta de recuperación) y a la dirección (titular de la tarjeta de recuperación, pero no del código asociado).