

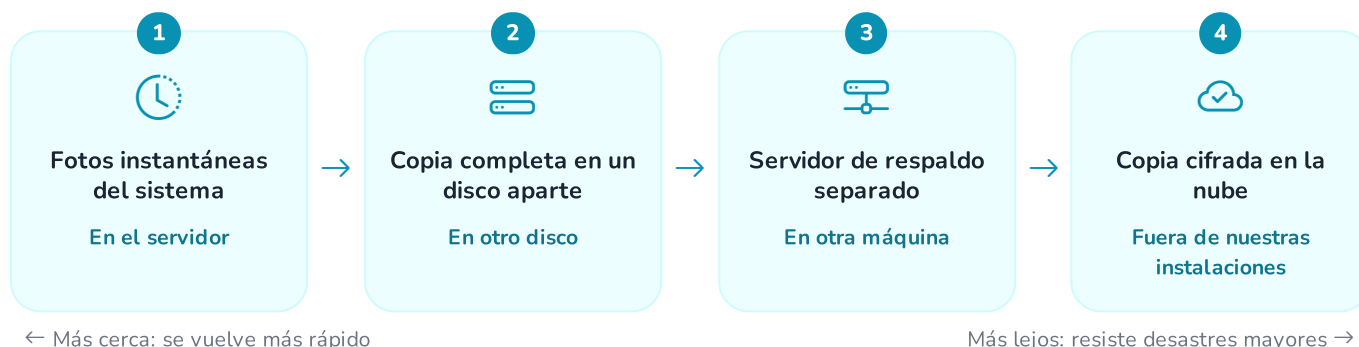


Cómo cuidamos tus datos

CitMed · Copias de seguridad y recuperación

Los datos de CitMed —**las historias clínicas**, los estudios y archivos adjuntos— se copian solos, varias veces por día y en lugares distintos. Si algo sale mal, volvemos atrás en minutos. Y lo probamos de verdad: **una copia que nunca se probó no es una copia.**

Cuatro capas, cada una más lejos



Qué guarda cada capa

Capa	Cada cuánto	Hasta cuándo atrás	Te protege de...
1 Fotos instantáneas del sistema	Cada 15 minutos, cada hora y cada día	Hasta 7 días	Un borrado por error o una actualización que salió mal.
2 Copia completa en un disco aparte	Todos los días, de madrugada	Últimos 7 días	Que fallen los discos principales.
3 Servidor de respaldo separado	Todos los días, verificadas cada semana	Hasta 6 meses (diarias, semanales y mensuales)	Que se rompa el servidor entero.
4 Copia cifrada en la nube	Bases de datos: todos los días. Aplicación completa con los estudios y archivos adjuntos: una vez por semana	Bases: 30 días · Completa: 4 semanas	Un incendio, un robo o un desastre en el lugar.



Y antes de todo eso, discos en espejo: el servidor guarda todo en dos discos a la vez. Si uno se rompe, el otro sigue trabajando y no se nota ningún corte.



Copias cifradas: lo que sale de nuestras instalaciones viaja y se guarda cifrado. Ni el proveedor de la nube puede leerlo.

Lo más cerca, para volver rápido. Lo más lejos, para que nada lo alcance.



¿Qué pasa si...?



Se borró algo por error, o una actualización salió mal

Volvemos al estado de minutos antes del problema con las fotos instantáneas (capa 1).

Minutos
se pierde como máximo
¼ de hora



Se rompe un disco del servidor

Los discos trabajan en espejo: el otro sigue funcionando. Cambiamos el disco roto sin cortar el servicio.

Sin corte



Se rompe el servidor entero

Recuperamos el sistema completo desde el servidor de respaldo (capa 3) o el disco aparte (capa 2).

Se recupera hasta la copia de esa madrugada.

16 minutos
medido en un simulacro
real



Incendio, robo o desastre en el lugar

Reinstalamos todo en otro equipo con la copia cifrada de la nube (capa 4), que está fuera de nuestras instalaciones.

Los datos vuelven hasta la copia del día; los estudios y archivos adjuntos, hasta la última copia semanal.

En el día
algunas horas

Además



Vigilancia permanente

El sistema se controla solo cada pocos minutos. Si una copia falla, los dos responsables nos enteramos al instante por WhatsApp y por mail.



Resumen semanal

Cada semana recibimos el estado de todas las copias. Si un resumen no llega, también es una señal de alarma.



Recuperación probada

Hacemos simulacros de restauración: sabemos cuánto tardamos en volver, no lo suponemos.



Acceso protegido

Conexión cifrada, contraseña propia de cada usuario y permisos por rol: cada institución ve solo lo suyo.

Lo que podés hacer vos

Tu parte también cuenta:

- Que cada persona entre con **su propio usuario**, y no compartir contraseñas.
- Cerrar la sesión en computadoras de uso compartido.
- Si algo se borró o se ve raro, **avisanos cuanto antes**: mientras más rápido, más cerca del momento justo podemos volver.

¿Dudas?

Escribinos: **Nestor Guerra** · WhatsApp +54 9 2355 47-4212 · **Federico Sanchez** · WhatsApp +54 9 2355 51-3172