



RIESGOS DE SEGURIDAD EN INSTITUCIONES DE SALUD Y CÓMO AFRONTARLOS

Hospitales, clínicas y laboratorios son un blanco atractivo para los atacantes porque manejan información personal, financiera y médica de sus pacientes. Pero el malware y los ataques dirigidos no son los únicos riesgos que enfrentan, ya que los empleados (actuales o antiguos) también pueden ser causantes de incidentes de seguridad, debido al desconocimiento o uso irresponsable de la tecnología en el trabajo.

Se deben resguardar

- + Historias clínicas y datos médicos
- + Datos personales y bancarios de pacientes y personal
- + Patentes y fórmulas de medicamentos

¿Cómo protegerlos?

- + **Doble autenticación:** evita accesos no autorizados creando claves temporales únicas
- + **Cifrado:** protege los datos haciéndolos ilegibles a terceros no autorizados
- + **Backup:** respaldo de información y sistemas que permite recuperar su disponibilidad
- + **Servicios profesionales:** ayudan a cumplir con las normativas y mejorar el desempeño

¿Qué los pone en peligro?

- + **Dispositivos médicos** con vulnerabilidades
- + **Equipos modernos** con sistemas obsoletos
- + **Información fácilmente accesible** para muchos
- + **Negligencia del personal** al compartir datos y fotos de pacientes por SMS y WhatsApp
- + **Uso de redes compartidas** sin las precauciones adecuadas

60%

De las empresas sufrió una infección por malware en 2014

40%

De los ataques fueron causados por descuidos de los empleados

Fuente

* Encuestas de ESET Latinoamérica realizadas durante 2014 en eventos corporativos de seguridad informática

* Encuesta sobre el estado de la seguridad global 2015 de PWC, CIO y CSO entre marzo y mayo del 2014