



DESDE LA NUBE:
SEGURIDAD DE IMÁGENES MÉDICAS
EN LA ERA DIGITAL



Introducción

La seguridad de las imágenes médicas es un desafío crítico para hospitales, clínicas y centros de diagnóstico. Estos archivos contienen información sensible que debe estar disponible en tiempo real, protegida contra accesos no autorizados y en cumplimiento con regulaciones internacionales.

La digitalización ha permitido avances importantes en el acceso y análisis de estas imágenes, pero también ha traído riesgos. Ciberataques dirigidos al sector salud, pérdida de datos por infraestructuras obsoletas y la necesidad de cumplir con regulaciones cada vez más estrictas han convertido la seguridad en un factor clave en la transformación digital del sector.

Las soluciones en la nube, combinadas con inteligencia artificial (IA), están abordando estos desafíos. Infraestructuras certificadas, cifrado de datos avanzado y herramientas de monitoreo inteligente están permitiendo que las instituciones de salud adopten nuevos modelos de almacenamiento sin comprometer la privacidad ni la integridad de la información.

Este documento explora los riesgos actuales, las soluciones disponibles y cómo las organizaciones de salud pueden implementar estrategias efectivas para garantizar la protección de datos sin afectar la eficiencia operativa.

Los desafíos de la seguridad en imágenes médicas

Las imágenes médicas son herramientas esenciales para el diagnóstico y tratamiento, pero su almacenamiento y acceso presentan retos complejos.

Ciberataques y accesos no autorizados

El sector salud es uno de los más atacados a nivel global. Según estudios recientes, el 60% de las brechas de seguridad en hospitales involucran datos de imágenes médicas.

- Ataques de ransomware: Organizaciones de salud han sido blanco de ataques donde los hackers cifran los datos y exigen pagos para su recuperación.
- Filtraciones de datos sensibles: Accesos no autorizados pueden exponer información privada de pacientes, generando riesgos legales y pérdida de confianza en las instituciones.
- Amenazas internas: No todos los riesgos provienen de ataques externos. Errores de configuración o accesos indebidos por parte del personal también pueden comprometer la seguridad de los datos.

Pérdida o corrupción de datos

Las imágenes médicas deben mantenerse disponibles a largo plazo, pero sin una infraestructura adecuada, pueden perderse o deteriorarse.

- Sistemas locales con almacenamiento limitado: Muchos hospitales aún dependen de servidores físicos con capacidad reducida, lo que obliga a eliminar archivos antiguos o migrar datos manualmente, aumentando el riesgo de errores.
- Fallas en el respaldo de datos: Sin un protocolo adecuado de copias de seguridad, una interrupción o falla técnica puede provocar la pérdida irreversible de información médica crítica.



Cumplimiento normativo

Las regulaciones internacionales imponen estrictos requisitos sobre la gestión de datos médicos.



AI Act en Europa:

Exige transparencia en el uso de IA en salud, asegurando que los sistemas sean seguros y no generen sesgos en los diagnósticos.



RGPD de la Unión Europea:

Que afecta a todos los profesionales que operan en el sector sanitario y vela por la protección de los datos personales relativos a la salud.



Reglamento sobre el EEDS:

Con el objetivo de establecer un marco común para el uso y el intercambio de datos de salud electrónicos en toda la UE, entra en vigor este 26 de marzo de 2025 y es un hito importante en tanto que mejora el acceso de las personas a sus datos de salud electrónicos personales y su control de dichos datos, al tiempo que permite que determinados datos se reutilicen con fines de interés público, apoyo a las políticas e investigación científica OMS y regulaciones en LATAM.

Países de América Latina están adaptando sus normativas a modelos europeos y estadounidenses, estableciendo estándares para el almacenamiento y acceso seguro a imágenes médicas.

Soluciones tecnológicas para la seguridad de imágenes médicas

Las tecnologías más avanzadas están permitiendo mejorar la seguridad y la eficiencia sin generar cargas operativas adicionales.

Infraestructura en la nube con certificaciones internacionales

Los sistemas de almacenamiento en la nube han evolucionado para ofrecer entornos seguros y certificados para la gestión de imágenes médicas.

- **AWS y cumplimiento normativo:** AWS proporciona una infraestructura con certificaciones internacionales como HIPAA, GDPR y AI Act, asegurando que los datos sean protegidos bajo los estándares más estrictos.
- **Almacenamiento distribuido:** La replicación de datos en múltiples ubicaciones permite evitar la pérdida de información en caso de fallas en un servidor.

Inteligencia Artificial aplicada a la seguridad

La IA no solo mejora la precisión diagnóstica, sino que también juega un papel clave en la seguridad de las imágenes médicas.

- **Análisis de accesos sospechosos:** Algoritmos de machine learning identifican patrones inusuales en el uso de imágenes médicas, alertando sobre posibles intentos de acceso no autorizado.

- **Automatización de anonimización:** La IA permite anonimizar imágenes antes de compartirlas con investigadores o especialistas, asegurando el cumplimiento normativo sin afectar la colaboración médica.
- **Optimización del diagnóstico:** Herramientas de IA permiten analizar grandes volúmenes de imágenes en segundos, reduciendo el tiempo de diagnóstico y minimizando el riesgo de errores humanos.

Estrategias de ciberseguridad avanzadas

Un entorno seguro debe integrar múltiples capas de protección para garantizar que las imágenes médicas estén resguardadas en todo momento.

- **Cifrado de datos en tránsito y en reposo:** Impide que la información sea interceptada durante su transmisión o almacenamiento.
- **Autenticación multifactor:** Requiere múltiples métodos de verificación para acceder a sistemas sensibles, evitando accesos no autorizados.
- **Monitoreo constante:** La supervisión en tiempo real permite detectar amenazas y responder de manera inmediata ante cualquier incidente de seguridad.

Resultados en números: impacto de una estrategia bien ejecutada

Las cifras muestran la diferencia entre seguir con infraestructuras obsoletas y adoptar soluciones modernas:

70%

menos incidentes de seguridad en hospitales que han migrado a plataformas certificadas.

40%

de reducción en tiempos de diagnóstico gracias a IA aplicada en imágenes médicas.

30%

de ahorro en costos operacionales, eliminando servidores locales y costos de mantenimiento.

Mayor interoperabilidad: acceso inmediato a imágenes desde cualquier ubicación y colaboración fluida entre especialistas.



Caso de éxito

Implementación de seguridad y eficiencia en imágenes médicas

Un hospital en Latinoamérica enfrentaba problemas con su infraestructura tradicional de imágenes médicas:

- Sistemas locales con almacenamiento limitado.
- Dificultad para compartir imágenes entre especialistas.
- Ausencia de protocolos de seguridad avanzados.

Tras adoptar una plataforma en la nube con IA integrada, se implementaron mejoras significativas:

- Infraestructura segura y escalable: Reducción del riesgo de pérdida de datos y acceso inmediato a imágenes.
- Análisis automatizado de imágenes: IA aceleró tiempos de diagnóstico y redujo el margen de error en interpretaciones médicas.
- Cumplimiento normativo asegurado: Auditorías automatizadas y cifrado robusto garantizaron alineación con estándares internacionales.



70% de reducción en incidentes de seguridad.



30% de ahorro en costos operacionales.



Acceso a imágenes desde cualquier ubicación.



Dedalus

Conclusión:

La seguridad de imágenes médicas es un desafío que requiere un enfoque estratégico. Las instituciones de salud no pueden depender de infraestructuras obsoletas ni de medidas de seguridad básicas.

Las soluciones en la nube y la IA han demostrado ser efectivas para garantizar el acceso seguro a imágenes médicas sin comprometer la eficiencia operativa.

Dedalus, en alianza con deepcOS y AWS ha desarrollado plataformas que cumplen con los más altos estándares de seguridad, integrando tecnologías avanzadas para optimizar la gestión de imágenes médicas y garantizar el cumplimiento normativo.

Para el sector salud, la seguridad no es una opción, es una necesidad. La adopción de estrategias modernas marcará la diferencia entre una gestión eficiente y una vulnerabilidad constante.

