

Alerta ID:	126
Fecha del reporte:	21/07/2026
Entidad:	Todas las entidades del ecosistema digital
Título:	Exposición de sistemas PACS/DICOM y riesgo de acceso no autorizado a información médica
Herramienta de detección	N/A
Activo involucrado:	Sistemas PACS/DICOM de almacenamiento, gestión y transmisión de imágenes médicas
Tipo de alerta:	Alerta
Nivel de riesgo:	Alto

Objetivo:

Informar a las organizaciones del sector salud en Colombia sobre la identificación de una condición crítica de exposición asociada a sistemas **PACS/DICOM**, utilizados para el almacenamiento, transmisión y gestión de imágenes médicas. Esta situación puede permitir accesos no autorizados a información clínica sensible, comprometiendo la confidencialidad, integridad y disponibilidad de los datos de pacientes, así como afectar procesos asistenciales relacionados con diagnóstico por imagen.

El propósito de esta alerta es que las organizaciones del sector salud validen la exposición y configuración de sus plataformas **PACS/DICOM**, incluyendo infraestructura propia, servicios administrados por terceros, ambientes en la nube y soluciones integradas con sistemas de información hospitalaria. Esta validación debe contemplar la revisión de inventarios



tecnológicos, controles de autenticación, mecanismos de cifrado, segmentación de red y accesos externos asociados a servidores de imágenes médicas.

Asimismo, se recomienda que las instituciones verifiquen la existencia de servicios DICOM publicados directamente en internet, versiones de software sin soporte, configuraciones inseguras o mecanismos de acceso no autorizados que puedan facilitar la extracción, modificación o indisponibilidad de estudios diagnósticos y datos asociados a los pacientes.

Descripción:

La exposición de sistemas **PACS (Picture Archiving and Communication System)** y servicios **DICOM (Digital Imaging and Communications in Medicine)** representa una condición crítica de seguridad que puede afectar la infraestructura tecnológica utilizada por las organizaciones del sector salud para el almacenamiento, transmisión y consulta de imágenes médicas. Estos sistemas son fundamentales para la operación de servicios como radiología, tomografía, resonancia magnética, ecografía y otras áreas relacionadas con el diagnóstico clínico.

El estándar **DICOM** permite la comunicación entre equipos médicos, estaciones de trabajo y plataformas de almacenamiento de imágenes, facilitando el intercambio de estudios diagnósticos entre diferentes dispositivos y sistemas hospitalarios. Sin embargo, cuando estos servicios se encuentran expuestos directamente a internet, configurados sin controles adecuados de autenticación, utilizando protocolos sin cifrado o ejecutando versiones desactualizadas del software, pueden convertirse en puntos de entrada para accesos no autorizados por parte de actores maliciosos.

Esta condición puede permitir que un atacante realice actividades como la identificación de servidores PACS expuestos, consulta no autorizada de estudios médicos, extracción de imágenes diagnósticas, recopilación de información personal asociada a pacientes o



manipulación de archivos médicos almacenados en estas plataformas. La exposición de estos sistemas representa un riesgo significativo debido a que las imágenes médicas suelen contener información clínica sensible vinculada a datos personales, diagnósticos y antecedentes médicos de los usuarios.

El impacto puede extenderse a las organizaciones del sector salud que utilizan infraestructura propia, servicios administrados por terceros, soluciones alojadas en la nube o plataformas integradas con Sistemas de Información Hospitalaria (SIH), Sistemas de Información Radiológica (RIS) y otros componentes tecnológicos utilizados durante la atención del paciente.

Actualmente, diferentes investigaciones de seguridad han identificado múltiples implementaciones PACS/DICOM accesibles desde internet con configuraciones deficientes, incluyendo servicios sin mecanismos robustos de autenticación y sistemas que permiten conexiones no autorizadas. Esta situación incrementa la posibilidad de incidentes relacionados con exposición de información clínica, afectación de la continuidad operativa y compromiso de la seguridad del paciente.

Por lo anterior, las organizaciones del sector salud deben realizar una revisión inmediata de sus plataformas PACS/DICOM, verificando los mecanismos de protección implementados, controles de acceso, segmentación de red, actualización de componentes tecnológicos y exposición de servicios hacia redes externas.

Consecuencias de la explotación

La explotación de configuraciones inseguras o exposiciones no controladas en sistemas **PACS/DICOM** puede generar consecuencias graves para las organizaciones del sector salud, debido a que estas plataformas almacenan y gestionan información clínica crítica utilizada



durante los procesos de diagnóstico y atención médica. Entre las principales consecuencias se encuentran:

1. Acceso no autorizado a información médica sensible

La exposición de servidores PACS/DICOM puede permitir que actores maliciosos accedan sin autorización a estudios diagnósticos almacenados en estas plataformas, incluyendo imágenes médicas, datos personales de pacientes e información clínica asociada.

Este acceso indebido puede comprometer la confidencialidad de la información protegida, generando riesgos relacionados con la privacidad de los pacientes y posibles incumplimientos de las obligaciones establecidas en materia de protección de datos personales en Colombia.

2. Compromiso de la confidencialidad de los datos de los pacientes

Los estudios médicos almacenados en sistemas PACS suelen contener información identificable del paciente, incluyendo nombres, identificadores, fechas de nacimiento, datos clínicos y detalles relacionados con procedimientos diagnósticos.

La extracción no autorizada de esta información podría ocasionar filtraciones de datos sensibles, afectando la privacidad de los usuarios y exponiendo a las instituciones a consecuencias legales, regulatorias y reputacionales derivadas de una posible brecha de seguridad.



3. Alteración o manipulación de imágenes médicas y datos asociados

Un atacante que logre acceso a un sistema PACS/DICOM podría modificar, eliminar o reemplazar información almacenada, afectando la integridad de los estudios diagnósticos.

La manipulación de imágenes médicas representa un riesgo crítico debido a que estos elementos pueden ser utilizados como soporte para la toma de decisiones clínicas. Cualquier modificación no autorizada podría generar interpretaciones incorrectas, retrasos en diagnósticos o afectaciones en los procesos asistenciales.

4. Interrupción de servicios críticos de diagnóstico

La afectación de plataformas PACS/DICOM puede ocasionar indisponibilidad de imágenes médicas necesarias para la atención de pacientes, impactando servicios como radiología, urgencias, hospitalización, consulta externa y unidades de cuidado crítico.

La interrupción del acceso a estudios diagnósticos puede retrasar procedimientos médicos, generar reprocesos operativos y afectar la continuidad de los servicios esenciales de salud.

5. Uso del sistema comprometido como punto de entrada hacia la red institucional

Un sistema PACS/DICOM comprometido puede ser utilizado como punto inicial para realizar movimientos laterales dentro de la infraestructura tecnológica de la organización.



Desde un servidor de imágenes afectado, un atacante podría intentar acceder a otros sistemas conectados, como Sistemas de Información Hospitalaria (SIH), Sistemas de Información Radiológica (RIS), bases de datos institucionales, servidores administrativos o plataformas integradas con la operación clínica.

Esta situación incrementa el alcance del incidente y puede convertir una exposición específica de imagenología en un compromiso general de la infraestructura tecnológica institucional.

6. Impacto reputacional, regulatorio y económico

La exposición de información médica o la interrupción de servicios asociados a diagnóstico por imágenes puede afectar la confianza de pacientes, profesionales de salud y entidades relacionadas con la organización.

Adicionalmente, un incidente de seguridad puede generar costos asociados a la investigación, recuperación de sistemas, análisis forense, notificación de afectados, fortalecimiento de controles de seguridad y posibles procesos administrativos derivados del incumplimiento de normas de protección de información..

Modo de explotación del ataque

La explotación de sistemas **PACS/DICOM** expuestos ocurre principalmente cuando estos servicios se encuentran accesibles desde redes externas sin los controles de seguridad



adecuados. Los actores maliciosos pueden aprovechar configuraciones deficientes, mecanismos de autenticación insuficientes, software desactualizado o una segmentación inadecuada de la infraestructura para obtener acceso no autorizado a plataformas utilizadas para la gestión de imágenes médicas.

A continuación, se describe el ciclo general mediante el cual puede producirse un compromiso de este tipo:

Identificación de servicios PACS/DICOM expuestos

El atacante realiza actividades de reconocimiento orientadas a identificar sistemas de imagenología médica accesibles desde internet o conectados a redes externas.

Durante esta etapa pueden ser identificados servicios relacionados con plataformas PACS/DICOM, servidores de almacenamiento de imágenes, visores médicos o componentes asociados que presenten configuraciones inseguras o controles de acceso insuficientes.

La exposición innecesaria de estos servicios aumenta la superficie de ataque y facilita que actores maliciosos determinen posibles objetivos dentro del ecosistema tecnológico de una institución de salud.

Acceso no autorizado a la plataforma PACS/DICOM

Una vez identificado un sistema vulnerable, el atacante puede intentar aprovechar debilidades de configuración, credenciales comprometidas, ausencia de autenticación robusta o controles de seguridad insuficientes para acceder a los servicios de imágenes médicas.



Cuando una plataforma no cuenta con mecanismos adecuados de protección, existe el riesgo de que usuarios no autorizados puedan consultar información almacenada, acceder a estudios diagnósticos o interactuar con componentes críticos del sistema.

Consulta y extracción de información clínica

Después de obtener acceso al sistema comprometido, el atacante puede intentar acceder a los repositorios donde se almacenan imágenes médicas y datos asociados a los pacientes.

La información comprometida puede incluir:

- Estudios radiológicos.
- Datos identificativos del paciente.
- Información clínica asociada.
- Metadatos contenidos en archivos DICOM.

Esta información puede ser utilizada para actividades ilícitas como exposición de datos, fraude, extorsión o comercialización no autorizada de información sensible.

Alteración o afectación de la integridad de los estudios médicos

En escenarios donde el atacante logra permisos suficientes dentro del sistema, podría intentar modificar o eliminar información almacenada en la plataforma.

La alteración de imágenes diagnósticas o datos asociados representa un riesgo crítico debido a que estos elementos pueden influir en procesos de evaluación médica y toma de decisiones clínicas.



Uso del sistema comprometido para movimientos laterales

Cuando los sistemas PACS/DICOM no se encuentran adecuadamente segmentados dentro de la infraestructura institucional, un atacante podría utilizar el acceso inicial como punto de entrada hacia otros componentes tecnológicos conectados.

Entre los posibles objetivos se encuentran:

- Sistemas de Información Hospitalaria (SIH).
- Sistemas de Información Radiológica (RIS).
- Servidores administrativos.
- Bases de datos institucionales.
- Servicios internos de autenticación.

Esta situación puede ampliar el impacto inicial y convertir una afectación localizada en un incidente de seguridad de mayor alcance.

Acciones posteriores al compromiso

Después de obtener acceso, los atacantes pueden intentar mantener persistencia dentro del entorno comprometido mediante modificaciones no autorizadas, creación de accesos adicionales o aprovechamiento de otros sistemas conectados.

Entre las acciones posteriores pueden presentarse:

- Extracción continua de información clínica.
- Interrupción de servicios de imagenología.
- Eliminación o alteración de registros.
- Uso de infraestructura comprometida para afectar otros sistemas institucionales.



Explotación masiva y afectación al ecosistema sanitario

Debido a que múltiples instituciones de salud utilizan plataformas PACS/DICOM de diferentes fabricantes y versiones, una configuración insegura replicada en varios ambientes puede aumentar el alcance de la amenaza.

La exposición de servicios de imagenología médica requiere una gestión permanente de vulnerabilidades, revisión de configuraciones, control de accesos y monitoreo continuo para reducir la posibilidad de compromiso de sistemas críticos.

vulnerabilidades asociadas
Exposición de servicios PACS/DICOM hacia internet**Descripción:**

Una de las principales condiciones de riesgo corresponde a la publicación directa de servicios PACS/DICOM hacia redes externas sin controles adecuados de restricción de acceso. Algunas organizaciones pueden mantener servidores de imágenes médicas accesibles desde internet para facilitar conexiones remotas, integración con proveedores o intercambio de estudios diagnósticos, sin aplicar mecanismos suficientes de protección.

La exposición pública de estos servicios incrementa la superficie de ataque institucional, permitiendo que actores no autorizados puedan identificar sistemas de imagenología disponibles y evaluar posibles debilidades de seguridad.

Impacto:

La exposición de servidores PACS/DICOM puede facilitar accesos no autorizados a plataformas de almacenamiento de imágenes médicas, generando riesgos de filtración de información clínica, consulta indebida de estudios diagnósticos y compromiso de la confidencialidad de los datos de los pacientes.



Ausencia de mecanismos robustos de autenticación y control de acceso**Descripción:**

Algunas implementaciones PACS/DICOM pueden presentar configuraciones donde los controles de autenticación son insuficientes, utilizan credenciales predeterminadas, manejan permisos excesivos o no aplican adecuadamente políticas de control de acceso basadas en roles.

Esta situación puede permitir que usuarios no autorizados interactúen con los sistemas de imagenología o accedan a información que debería estar restringida únicamente a personal autorizado.

Impacto:

La falta de controles adecuados puede ocasionar acceso indebido a imágenes médicas, información clínica asociada y datos personales de pacientes, afectando la privacidad, seguridad de la información y cumplimiento de las obligaciones institucionales de protección de datos.

Falta de cifrado en las comunicaciones DICOM**Descripción:**

El protocolo DICOM fue diseñado principalmente para facilitar la interoperabilidad entre equipos médicos y sistemas de información clínica. Sin embargo, algunas implementaciones pueden operar sin mecanismos adecuados de cifrado, permitiendo que la información transmitida entre dispositivos médicos, servidores PACS y estaciones de trabajo viaje sin una protección suficiente.

Cuando las comunicaciones no se encuentran protegidas, un atacante con acceso a la red podría intentar interceptar información durante la transmisión.

Impacto:

La ausencia de cifrado puede permitir la exposición de imágenes diagnósticas, datos



identificativos del paciente y otra información clínica transmitida entre componentes tecnológicos, comprometiendo la confidencialidad de la información médica.

Uso de software PACS/DICOM desactualizado o sin soporte

Descripción:

Las plataformas PACS, servidores DICOM y componentes asociados requieren actualizaciones periódicas para corregir fallas de seguridad identificadas por fabricantes y comunidades técnicas.

El uso de versiones antiguas, componentes sin soporte o sistemas que no reciben actualizaciones de seguridad puede mantener vulnerabilidades conocidas dentro de la infraestructura institucional.

Impacto:

Los sistemas desactualizados pueden ser aprovechados por atacantes para comprometer servidores de imagenología, ejecutar acciones no autorizadas, afectar la disponibilidad de los servicios o utilizar estos equipos como punto de entrada hacia otros sistemas institucionales.

Configuración insegura de permisos y servicios asociados

Descripción:

Las configuraciones incorrectas en servidores PACS/DICOM, bases de datos asociadas, visores médicos o servicios complementarios pueden generar accesos innecesarios, exposición de información administrativa o permisos superiores a los requeridos para usuarios y aplicaciones.

Una configuración inadecuada puede permanecer durante largos periodos debido a la complejidad de los ambientes clínicos y la necesidad de mantener disponibilidad permanente de los servicios.

Impacto:

Los permisos excesivos o configuraciones inseguras pueden facilitar que un atacante obtenga mayor control sobre la plataforma, acceda a información clínica sensible o afecte la operación de los servicios de diagnóstico por imagen.



Falta de segmentación de red en infraestructura de imagenología**Descripción:**

Los sistemas PACS/DICOM suelen integrarse con múltiples componentes tecnológicos, incluyendo equipos médicos, estaciones clínicas, sistemas RIS, HIS y otros servicios institucionales.

Cuando estos sistemas no se encuentran adecuadamente segmentados mediante controles de red, un compromiso inicial en una plataforma de imagenología podría permitir desplazamientos hacia otros activos críticos de la organización.

Impacto:

La ausencia de segmentación puede ampliar el alcance de un incidente de seguridad, permitiendo que una afectación localizada en imagenología evolucione hacia un compromiso de sistemas administrativos, clínicos o bases de datos institucionales.

Deficiencias en monitoreo y auditoría de accesos**Descripción:**

Los sistemas PACS/DICOM requieren mecanismos de registro y seguimiento de actividades para identificar accesos inusuales, consultas masivas de estudios, modificaciones no autorizadas o comportamientos anómalos dentro de la plataforma.

La ausencia de monitoreo continuo limita la capacidad institucional para detectar oportunamente actividades maliciosas.

Impacto:

La falta de auditoría puede retrasar la identificación de incidentes, aumentar el tiempo de exposición de información clínica y dificultar las investigaciones posteriores para determinar el alcance del compromiso



Recomendaciones de detección y mitigación

Para detectar y mitigar eficazmente los riesgos asociados con la exposición de sistemas **PACS/DICOM**, es fundamental que las organizaciones del sector salud implementen medidas orientadas a identificar servicios expuestos, fortalecer los controles de acceso, proteger la información clínica y garantizar la continuidad de los servicios relacionados con diagnóstico por imagen.

A continuación, se presentan las recomendaciones principales:

1. Identificación y revisión de infraestructura PACS/DICOM

Las organizaciones deben realizar una revisión inmediata de sus activos tecnológicos relacionados con imagenología médica, identificando:

- Servidores PACS implementados dentro de la institución.
- Servicios DICOM asociados a equipos médicos.
- Visores de imágenes utilizados por personal asistencial.
- Integraciones con sistemas RIS, HIS y Sistemas de Información Hospitalaria.
- Servicios administrados por terceros o alojados en ambientes externos.

Es importante mantener actualizado el inventario tecnológico institucional, incluyendo fabricante, versión del sistema, ubicación, responsables técnicos y conexiones existentes.

2. Validación de exposición de servicios DICOM hacia internet

Se recomienda verificar si existen servicios PACS/DICOM publicados directamente hacia redes externas sin controles adecuados.



Las entidades deben evaluar:

- Conexiones externas habilitadas.
- Accesos remotos utilizados por proveedores.
- Puertos y servicios innecesariamente expuestos.
- Reglas de firewall asociadas a servidores de imagenología.

Los servicios DICOM deben permanecer accesibles únicamente para usuarios, dispositivos y redes autorizadas.

3. Fortalecimiento de mecanismos de autenticación y control de acceso

Implementar controles de acceso estrictos para reducir la posibilidad de accesos no autorizados.

Se recomienda:

- Eliminar credenciales predeterminadas.
- Aplicar políticas de contraseñas seguras.
- Implementar autenticación multifactor cuando la plataforma lo permita.
- Asignar permisos según funciones laborales.
- Aplicar el principio de mínimo privilegio.

Los usuarios administrativos de las plataformas PACS deben ser limitados y monitoreados debido al nivel de acceso que poseen sobre información clínica sensible.



4. Implementación de cifrado en comunicaciones DICOM

Las instituciones deben verificar que las comunicaciones entre equipos médicos, servidores PACS y estaciones de consulta utilicen mecanismos seguros de transmisión.

Se recomienda:

- Habilitar configuraciones DICOM Secure cuando sean soportadas.
- Utilizar protocolos cifrados para conexiones remotas.
- Evitar transmisión de información clínica sin mecanismos adecuados de protección.
- Revisar certificados digitales asociados a servicios médicos.

La protección de las comunicaciones permite reducir el riesgo de interceptación de información clínica durante su transferencia.

5. Actualización y gestión de vulnerabilidades en plataformas PACS/DICOM

Las organizaciones deben mantener actualizados los componentes tecnológicos relacionados con imagenología médica.

Se recomienda:

- Aplicar actualizaciones de seguridad proporcionadas por fabricantes.
- Revisar boletines técnicos de proveedores PACS.
- Retirar componentes obsoletos o sin soporte.
- Evaluar riesgos asociados a versiones antiguas de software.

La gestión periódica de vulnerabilidades permite reducir la posibilidad de explotación de fallas conocidas.



6. Segmentación y protección de redes de imagenología

Los sistemas PACS/DICOM deben permanecer aislados de otros segmentos de red mediante controles adecuados.

Se recomienda:

- Separar redes clínicas y administrativas.
- Implementar reglas de firewall internas.
- Restringir comunicaciones únicamente a servicios necesarios.
- Controlar conexiones provenientes de equipos externos.

Una adecuada segmentación limita la posibilidad de movimiento lateral en caso de compromiso de un sistema de imagenología.

7. Monitoreo continuo y revisión de registros

Las instituciones deben establecer mecanismos de monitoreo para detectar comportamientos anómalos dentro de las plataformas PACS/DICOM.

Se recomienda revisar:

- Registros de autenticación.
- Consultas masivas de estudios.
- Descargas inusuales de imágenes.
- Cambios administrativos.
- Modificaciones o eliminación de información.



El análisis periódico de eventos permite identificar accesos sospechosos y responder oportunamente ante posibles incidentes.

8. Auditorías periódicas de seguridad

Se recomienda realizar evaluaciones técnicas periódicas sobre la infraestructura de imagenología.

Estas auditorías deben incluir:

- Evaluación de configuraciones PACS.
- Revisión de controles de acceso.
- Análisis de exposición externa.
- Validación de cumplimiento de políticas institucionales.
- Pruebas de seguridad autorizadas.

Las auditorías permiten identificar condiciones de riesgo antes de que sean aprovechadas por actores maliciosos.

9. Capacitación del personal técnico y asistencial

Es necesario fortalecer el conocimiento del personal involucrado en la administración y uso de sistemas de imagenología.

La capacitación debe incluir:

- Manejo seguro de credenciales.
- Identificación de accesos sospechosos.
- Reporte oportuno de incidentes.



- Buenas prácticas en protección de información clínica.

La seguridad de los sistemas PACS/DICOM requiere la participación coordinada de áreas de tecnología, ingeniería biomédica, radiología y seguridad del paciente.

10. Implementación de planes de continuidad operativa

Las instituciones deben contar con procedimientos definidos ante una posible indisponibilidad de las plataformas PACS/DICOM.

Se recomienda establecer:

- Procedimientos alternos para consulta de imágenes.
- Copias de seguridad verificadas.
- Responsables de respuesta ante incidentes.
- Protocolos de comunicación interna.

Esto permite reducir el impacto operacional y garantizar la continuidad de la atención médica ante eventos de seguridad.

Recomendaciones de respuesta ante compromiso

Si se identifica o sospecha que un sistema PACS/DICOM ha sido comprometido, las organizaciones del sector salud deben ejecutar acciones inmediatas orientadas a contener el incidente, proteger la información clínica, preservar evidencia digital y garantizar la continuidad de los servicios asistenciales relacionados con diagnóstico por imagen.

A continuación, se describen las acciones recomendadas:

- Aislamiento del sistema afectado



- Desconectar o restringir la conectividad del sistema comprometido

El primer paso ante un posible compromiso de una plataforma PACS/DICOM consiste en limitar la exposición del sistema afectado para evitar accesos adicionales, extracción de información o propagación hacia otros componentes tecnológicos institucionales.

Las acciones recomendadas incluyen:

- Restringir temporalmente conexiones externas hacia el servidor PACS.
- Bloquear accesos no autorizados identificados durante la investigación.
- Aislar el sistema dentro del segmento de red correspondiente.
- Mantener coordinación con radiología, ingeniería biomédica y tecnología para evitar afectaciones innecesarias sobre la atención clínica.

Cuando sea posible, el aislamiento debe realizarse preservando la evidencia necesaria para el análisis posterior del incidente.

Análisis y confirmación del compromiso

Revisión de registros y actividad del sistema

Se debe realizar una revisión detallada de los eventos registrados en la plataforma PACS/DICOM con el objetivo de identificar comportamientos anómalos relacionados con accesos no autorizados o actividades inusuales.

La revisión debe incluir:

- Registros de autenticación.



- Usuarios con accesos administrativos.
- Consultas inusuales de estudios médicos.
- Descargas masivas de imágenes.
- Cambios en configuraciones del sistema.
- Modificaciones o eliminación de estudios.

El análisis debe permitir determinar:

- Fecha aproximada del acceso no autorizado.
- Sistemas involucrados.
- Información potencialmente comprometida.
- Alcance del incidente.

Análisis forense de la infraestructura afectada

Cuando exista evidencia de compromiso, se recomienda realizar un análisis técnico especializado sobre los componentes involucrados.

Este análisis debe contemplar:

- Servidor PACS.
- Bases de datos asociadas.
- Servidores DICOM.
- Estaciones de trabajo relacionadas.
- Registros de red.



- Sistemas conectados mediante RIS o HIS.

El objetivo es identificar mecanismos utilizados para obtener acceso, determinar si hubo extracción o modificación de información y establecer medidas correctivas.

Contención del incidente

Revocación de accesos comprometidos

Si se identifican usuarios, cuentas o credenciales comprometidas, se deben aplicar acciones inmediatas:

- Deshabilitar cuentas sospechosas.
- Restablecer credenciales administrativas.
- Revisar permisos asignados.
- Retirar accesos innecesarios.
- Implementar autenticación multifactor cuando sea posible.

Estas medidas reducen la posibilidad de que el atacante conserve acceso sobre la plataforma.

Restricción temporal de servicios afectados

Cuando sea necesario, se recomienda limitar temporalmente funcionalidades específicas del sistema mientras se realiza la investigación.

Estas acciones pueden incluir:

- Suspensión de accesos externos.
- Bloqueo de conexiones no autorizadas.



- Restricción de integraciones con terceros.
- Revisión de conexiones con otros sistemas institucionales.

Las medidas deben ejecutarse coordinadamente para evitar impactos innecesarios sobre la operación clínica.

Erradicación de la amenaza

Corrección de configuraciones inseguras

Una vez identificado el origen del compromiso, se deben corregir las condiciones que permitieron la exposición.

Las acciones pueden incluir:

- Eliminación de accesos innecesarios.
- Corrección de permisos excesivos.
- Cierre de servicios expuestos sin justificación.
- Fortalecimiento de configuraciones de seguridad.
- Aplicación de controles adicionales de autenticación.

Actualización de plataformas y componentes tecnológicos

Se debe verificar que todos los componentes relacionados con PACS/DICOM se encuentren soportados y actualizados.

Las acciones recomendadas incluyen:

- Aplicación de parches de seguridad.



- Actualización de servidores PACS.
- Actualización de visores médicos.
- Revisión de componentes integrados.
- Validación de compatibilidad con equipos biomédicos.

Eliminación de accesos persistentes no autorizados

Los atacantes pueden intentar mantener acceso mediante modificaciones dentro del sistema comprometido.

Por esta razón se debe revisar:

- Usuarios creados recientemente.
- Cambios administrativos no autorizados.
- Configuraciones modificadas.
- Servicios desconocidos.
- Integraciones no reconocidas.

Restauración del sistema

Recuperación desde respaldos confiables

Cuando la integridad del sistema haya sido afectada, se debe evaluar la restauración desde copias de seguridad verificadas.

Antes de realizar una recuperación se recomienda:

- Confirmar que los respaldos no estén comprometidos.



- Validar la integridad de las imágenes médicas almacenadas.
- Verificar disponibilidad de estudios clínicos críticos.
- Documentar las acciones realizadas.

Validación antes del retorno a operación

Antes de habilitar nuevamente la plataforma PACS/DICOM, se debe confirmar:

- Corrección de la vulnerabilidad identificada.
- Eliminación de accesos no autorizados.
- Funcionamiento adecuado de las integraciones clínicas.
- Disponibilidad de imágenes médicas.
- Correcto funcionamiento para usuarios asistenciales.

Comunicación y notificación

Notificación interna

El incidente debe ser comunicado al personal responsable para coordinar la respuesta institucional.

Se recomienda involucrar:

- Seguridad de la información.
- Tecnología de la información.
- Ingeniería biomédica.
- Servicio de radiología.



- Seguridad del paciente.
- Dirección institucional.

Evaluación de notificación externa

Cuando exista compromiso de información personal o datos clínicos de pacientes, la organización debe evaluar las obligaciones de notificación establecidas por la normativa colombiana aplicable en protección de datos personales y gestión de incidentes.

También debe considerarse la comunicación con:

- Proveedores tecnológicos involucrados.
- Fabricantes de plataformas PACS.
- Entidades regulatorias cuando corresponda.

Prevención a largo plazo

Después de controlar el incidente, las organizaciones deben fortalecer sus capacidades de seguridad para evitar recurrencias.

Se recomienda:

- Realizar auditorías periódicas de infraestructura PACS/DICOM.
- Mantener actualizado el inventario tecnológico.
- Implementar gestión continua de vulnerabilidades.
- Revisar accesos privilegiados.
- Fortalecer segmentación de red.



- Ejecutar ejercicios de respuesta ante incidentes.
- Capacitar al personal técnico y asistencial

Conclusiones



La exposición de sistemas **PACS/DICOM** representa una condición de riesgo significativo para las organizaciones del sector salud debido a que estas plataformas almacenan, procesan y transmiten información clínica sensible utilizada durante los procesos de diagnóstico y atención de los pacientes. Una configuración insegura, una exposición innecesaria hacia internet o la ausencia de controles adecuados de seguridad pueden permitir accesos no autorizados que comprometan la confidencialidad, integridad y disponibilidad de la información médica.

Las instituciones de salud que utilizan sistemas PACS/DICOM dentro de su infraestructura tecnológica, mediante servicios tercerizados o plataformas administradas por proveedores externos, deben considerar estos componentes como activos críticos debido a su relación directa con la operación asistencial. La afectación de estos sistemas puede generar exposición de imágenes diagnósticas, alteración de información clínica, interrupción de servicios de radiología y retrasos en procesos fundamentales para la atención de los pacientes.

La implementación de controles de seguridad adecuados es fundamental para reducir la posibilidad de compromiso. Entre las principales medidas se encuentran la revisión permanente de configuraciones, restricción de accesos externos, fortalecimiento de mecanismos de autenticación, aplicación de actualizaciones de seguridad, segmentación de redes clínicas y monitoreo continuo de eventos relacionados con las plataformas de imagenología.



En caso de identificar una posible exposición o compromiso de un sistema PACS/DICOM, las organizaciones deben actuar de manera inmediata mediante el aislamiento del componente afectado, análisis de registros, identificación del alcance del incidente, protección de la información clínica y coordinación entre las áreas de tecnología, ingeniería biomédica, radiología y seguridad del paciente.

La protección de los sistemas de imagenología médica requiere una gestión integral que combine controles tecnológicos, procesos institucionales y capacitación del personal encargado de administrar y utilizar estas plataformas. La seguridad de la información clínica debe mantenerse como un elemento prioritario dentro de la continuidad operativa del sector salud.

Finalmente, se recomienda que las organizaciones realicen evaluaciones periódicas de sus ambientes PACS/DICOM, mantengan actualizados sus inventarios tecnológicos y fortalezcan sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad, con el propósito de reducir riesgos que puedan afectar la prestación segura y continua de los servicios de salud.

Fuentes:



DICOM Standard Committee. Digital Imaging and Communications in Medicine (DICOM) Standard. Disponible en: <https://www.dicomstandard.org/>

Health Sector Cybersecurity Coordination Center (HC3) – U.S. Department of Health and Human Services. Cybersecurity Threat Briefings for the Healthcare Sector. Disponible en: <https://www.hhs.gov/about/agencies/405d/index.html>



Cybersecurity and Infrastructure Security Agency (CISA). Healthcare and Public Health Cybersecurity Guidance. Disponible en: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/healthcare-and-public-health>

MITRE ATT&CK Framework for Enterprise. Disponible en: <https://attack.mitre.org/>

National Institute of Standards and Technology (NIST). Cybersecurity Framework (CSF) 2.0. Disponible en: <https://www.nist.gov/cyberframework>

Food and Drug Administration (FDA). Cybersecurity in Medical Devices. Disponible en: <https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity>

Trend Micro Research. Exposed DICOM Servers and the Risk to Patient Data. Disponible en: <https://www.trendmicro.com/vinfo/us/security/news/>

Rapid7 Research. Exposed DICOM Servers and Healthcare Security Risks. Disponible en: <https://www.rapid7.com/>

Health Sector Coordinating Council (HSCC). Health Industry Cybersecurity Practices (HICP). Disponible en: <https://healthsectorcouncil.org/>

Cybersecurity in Medical Imaging: A Review of Security Challenges and Solutions. Disponible en: <https://pmc.ncbi.nlm.nih.gov/>

En caso de dudas, inquietudes o requerir asistencia adicional relacionada con esta alerta de seguridad, puede comunicarse directamente con el **CSIRT Salud** a través de las líneas telefónicas **(+57) 316 893 1490 - 318 155 3570** o mediante el correo electrónico **csirtsalud@minsalud.gov.co**. Nuestro equipo está disponible para brindar el acompañamiento necesario.

