Bogotá D.C., 7 de Octubre del 2025 INT-HCC-036-25

Doctor
GUILLERMO MAYORGA
Representante Legal
UT HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA
Ciudad

ASUNTO: Requerimiento seguimiento recomendaciones RESPUESTA A OFICIO INT-HCC-020-25 COMPONENTE SISTEMAS (Imedical Cloud – Gestión de Activos TI)

Respetado Doctor,

En cumplimiento de nuestras obligaciones contractuales derivadas de la ejecución del contrato de interventoría No. SS-CM-INV-825-2025 cuyo objeto es *"REALIZAR, DESARROLLAR Y EJECUTAR LA INTERVENTORÍA TÉCNICA, JURÍDICA, ADMINISTRATIVA, FINANCIERA Y CONTABLE, EN REPRESENTACIÓN DE LA SECRETARÍA DE SALUD DEL DEPARTAMENTO DE CUNDINAMARCA COMO ENTIDAD CONTRATANTE DEL "CONTRATO DE CONCESIÓN NO. 002 DE 2003" CELEBRADO ENTRE LA SECRETARÍA DE SALUD Y LA UNIÓN TEMPORAL HOSPITAL CARDIOVASCULAR DEL NIÑO DE CUNDINAMARCA*" En cumplimiento de las obligaciones de supervisión y seguimiento establecidas.

En el marco de las actividades de auditoría y seguimiento adelantadas por esta interventoría, se realiza la revisión y análisis de los soportes remitidos en atención a las recomendaciones formuladas, con el propósito de emitir un concepto sobre el avance y cumplimiento de los lineamientos establecidos:

1. Seguridad en Imedical Cloud

   "(…) Oportunidad de mejora Encriptación de datos en tránsito y reposo: Se identificó que el cifrado del tráfico entre los usuarios finales y las máquinas virtuales en la infraestructura de Azure no se encuentra habilitado por defecto. Si bien los mensajes entre centros de datos utilizan TLS con claves de al menos 128 bits, la protección extrema a extremo depende de la configuración manual por parte del cliente (…)".

   Respuesta Hospital Cardiovascular de Cundinamarca: "*En relación con la oportunidad de mejora planteada sobre la encriptación de datos en tránsito y en reposo, informamos que en la reunión del día 10 de septiembre de 2025, con presencia de la interventoría y en comunicación con el ingeniero Germán Cardona, CEO de iMedical, se aclaró que el cifrado del tráfico entre los usuarios finales y las máquinas virtuales sí se encuentra habilitado dentro de la infraestructura de iMedical Cloud.*

   En atención a esta confirmación, se procedió a actualizar el documento PT01 INF "Seguridad y Confidencialidad de la Historia Clínica iMedical Cloud V3", corrigiendo la información que se encontraba desactualizada. Dicho documento actualizado se adjunta

como evidencia en la presente respuesta".

Concepto: Revisada la información y las evidencias remitidas por el Hospital Cardiovascular de Cundinamarca, se confirma la actualización del documento PT01 INF "Seguridad y Confidencialidad de la Historia Clínica iMedical Cloud V3", en el cual se corrige la información relacionada con el cifrado de datos en tránsito y en reposo.

En consecuencia, la interventoría acepta la aclaración y la actualización realizada, considerando atendida la oportunidad de mejora planteada en relación con la configuración de cifrado en la infraestructura de iMedical Cloud.

2. Imedical Cloud Soporte de Servicios:

"*(…) Oportunidad de mejora Soporte Servicios: Durante la revisión de la plataforma se identificó que el control y seguimiento de los casos se realiza mediante un archivo en Excel, paralelo al registro en la plataforma iMedical Cloud. Si bien esta práctica permite mantener trazabilidad básica, presenta riesgos de duplicidad de información, falta de consolidación y retrasos en la gestión de cierres (…)"*

Respuesta Hospital Cardiovascular de Cundinamarca: "*En la actualidad, el control y seguimiento de los casos se realiza mediante un archivo en Excel administrado por el Departamento de Informática, lo cual permite mantener trazabilidad básica. Sin embargo, atendiendo a la recomendación de la interventoría y con el fin de fortalecer la gestión, se migrará este proceso al Centro de Asistencia de iMedical Cloud, que es la plataforma oficial del proveedor para la administración de tickets.*
A partir de la fecha, la gestión de casos se realizará directamente en iMedical Cloud, aprovechando sus funcionalidades de:

- Registro centralizado de tickets desde su apertura hasta el cierre.
- Descarga de reportes consolidados de todos los casos registrados.
- Búsqueda y filtrado de tickets por estado, fecha o número, lo que asegura un control oportuno y actualizado.
De esta manera, el Hospital asegurará que la totalidad del ciclo de vida de los casos (apertura, seguimiento y cierre) quede documentado en un único repositorio, reduciendo riesgos de duplicidad de información y mejorando la eficiencia en el cierre oportuno de requerimientos, adjunto base descargada".

Concepto: La interventoría revisó la evidencia documental remitida y la actualización informada respecto a la migración del control y seguimiento de casos hacia el Centro de Asistencia de iMedical Cloud, plataforma oficial del proveedor para la administración de tickets.
Se constata que la medida adoptada atiende la oportunidad de mejora señalada, al propender por un registro centralizado, trazable y con reportes consolidados, lo cual contribuye a la eficiencia en la gestión de requerimientos.
No obstante, la interventoría recomienda que este proceso se articule con la Coordinación de Sistemas del Hospital en lo correspondiente a la gestión de soportes de TI, asegurando que la operación del centro de asistencia se enmarque dentro de las buenas prácticas de ITIL,

particularmente en los procesos de gestión de incidentes y requerimientos de servicio. Con base en lo anterior, se acepta la respuesta presentada por el Hospital Cardiovascular de Cundinamarca, considerando atendida la oportunidad de mejora, con la recomendación descrita.

En lo que tiene que ver con "*Definir un procedimiento formal de gestión de casos en la plataforma iMedical Cloud, que establezca responsables, tiempos de respuesta y cierre documentado*".

Concepto: La interventoría revisó la información remitida y no se evidenció soporte que documente la existencia de un procedimiento formal de gestión de casos en la plataforma iMedical Cloud, que establezca responsables, tiempos de respuesta y criterios de cierre. En consecuencia, se recomienda formalizar dicho procedimiento, articulándolo con la Coordinación de Sistemas del Hospital, de manera que se enmarque dentro de las buenas prácticas de ITIL para la gestión de incidentes y requerimientos de servicio. La interventoría efectuará seguimiento en los próximas meses teniendo en cuenta la oportunidad de mejora dada al Servicio de Soporte de TI del Hospital.

3. Análisis del Plan de Contingencia frente a la Caída del Sistema (PT03 DA V3):

   (…) "Tras la revisión realizada al Plan de Contingencia frente a la Caída del Sistema (PT03 DA V3), se observa que en términos generales se encuentra bien estructurado (…)"

Concepto:
La interventoría revisó el documento PT03 DA "Plan de Contingencia frente a Caída del Sistema" V3 y evidenció que su contenido se centra en la gestión asistencial y administrativa durante una caída del sistema, estableciendo lineamientos para el diligenciamiento manual de los registros clínicos y la posterior carga de la información en el aplicativo.

No obstante, este documento no constituye un Plan de Continuidad del Negocio (PCN), ya que no incluye los componentes estratégicos y tecnológicos propios de dicho plan, tales como el análisis de impacto en el negocio (BIA), la definición de tiempos de recuperación (RTO/RPO), los procedimientos técnicos de restauración (DRP), ni los roles y responsabilidades para la recuperación de la infraestructura tecnológica.

En consecuencia, se recomienda elaborar un Plan de Continuidad del Negocio independiente, que integre tanto el componente operativo (ya descrito en este protocolo) como el Plan de Recuperación ante Desastres (DRP), en coordinación con la Coordinación de Sistemas y todos los proveedores del Hospital Cardiovascular de Cundinamarca, asegurando su alineación con las **buenas prácticas de ITIL y las normas ISO 22301 e ISO 27031**.

La interventoría hará seguimiento a la elaboración y adopción del Plan de Continuidad del Negocio, considerando que esta actividad requiere tiempo, planeación y coordinación interinstitucional.
En consecuencia, la oportunidad de mejora se mantiene abierta, hasta tanto se disponga del documento formal que integre los componentes de continuidad PCN y recuperación (DRP, RTO, RPO) y se evidencien pruebas o simulacros que validen su efectividad.

4. Control de Accesos:

"(…) Oportunidad de mejora: La matriz actual está bien como listado básico de roles activos, pero para ser evidencia sólida de seguridad de accesos en auditoría, debería complementarse con usuarios asociados, permisos, áreas y trazabilidad de cambios a continuación se sugiere (…)"

Respuesta Hospital Cardiovascular de Cundinamarca: (…) *Se descarga información de la base de datos y se genera archivo de Excel que adjunto llamado Rol Vs Usuarios en la cual se especifica qué usuario tiene asignado cada rol. Adicionalmente, en una segunda hoja del mismo archivo se documenta cada rol con su fecha de creación y la cantidad de usuarios activos asociados.*
Se realizó la solicitud al proveedor mediante el ticket N.° 89392, con el fin de obtener el detalle de los privilegios y permisos asociados a cada rol, Una vez el proveedor entregue la información detallada de roles y permisos, se procederá a vincular cada rol con el área o proceso correspondiente, así como a establecer y documentar las modificaciones.
Como parte del proceso de control interno, se efectúa una revisión semestral de usuarios y roles, validando la pertinencia de cada asignación según especialidad y función. En caso de encontrarse usuarios con roles no correspondientes, se procede a su inactivación inmediata (…)

Concepto: La interventoría revisó la información remitida, incluyendo el archivo "Rol vs Usuarios", en el cual se relacionan los usuarios activos y los roles asignados, así como la evidencia de la solicitud al proveedor (ticket N.º 89392) para obtener el detalle de los privilegios y permisos asociados.

Se reconoce el avance realizado en la estructuración de la matriz y en la implementación del control semestral de revisión de usuarios y roles. No obstante, aún se requiere complementar la información con la documentación del detalle de privilegios, áreas o procesos asociados a cada rol, así como el control de versionamiento, fechas y modificaciones realizadas, que permita garantizar la trazabilidad de los cambios en materia de seguridad de accesos.

En consecuencia, la recomendación se mantiene abierta, hasta tanto se consolide la matriz completa con los componentes mencionados y se formalice el mecanismo de actualización periódica y control de cambios.

5. Consentimientos Imedical Cloud:

(…) *Se evidenció que los consentimientos informados aún no están completamente implementados en la plataforma Imedical Cloudl, dado que gran parte del proceso continúa siendo gestionado de manera manual* (…).

Concepto:
La interventoría revisó la evidencia documental remitida, incluyendo la comunicación oficial del 22 de septiembre de 2025, mediante la cual el Hospital Cardiovascular de

Cundinamarca solicita al proveedor iMedicalCloud el desarrollo del módulo de consentimiento informado dentro de la plataforma, como parte del fortalecimiento de los registros clínicos electrónicos.

Esta gestión evidencia el inicio formal del proceso ante el proveedor; no obstante, a la fecha no se cuenta con la implementación ni las pruebas funcionales del módulo en operación.

En consecuencia, la oportunidad de mejora se mantiene abierta, y en lo que resta del proceso de interventoría se efectuará seguimiento al avance del desarrollo, implementación y validación del consentimiento informado electrónico, verificando la trazabilidad de las comunicaciones, los entregables técnicos y la puesta en marcha del módulo en la plataforma.

6. Prueba de consulta (no abordada durante la auditoría):

"*(…) se solicita al hospital informar si ya cuenta con algún avance en la adopción de la CIE-11 o un plan o proyección definido para el ajuste de sus sistemas de información, la capacitación del personal y la adaptación documental (…)".*

Respuesta Hospital Cardiovascular de Cundinamarca: *"(…) Dado que nuestra institución utiliza un software en la modalidad SaaS (Software as a Service), es el proveedor quien se encarga de la actualización y adaptación de la plataforma para dar cumplimiento a la normatividad vigente.*

En este sentido, conforme a la Resolución 1657 de 2025 del Ministerio de Salud, se amplió el plazo para la implementación de la CIE-11 a 36 meses, contados a partir del 14 de agosto de 2025. Esta resolución modifica los artículos 3 y 4 de la Resolución 1442 de 2024 y establece el tiempo máximo para que las entidades del sistema de salud adopten la CIE-11 como sistema oficial de codificación.

Por lo anterior, nuestra institución se encuentra a la espera de las actualizaciones que realizará el proveedor del software, en concordancia con los plazos definidos por el Ministerio de Salud, y gestionará los procesos internos de capacitación y adaptación documental conforme se avance en dicho plan".

Concepto:
La interventoría revisó la información remitida y confirma que la adopción de la CIE-11 depende de las actualizaciones que realice el proveedor iMedicalCloud, dado que el sistema opera bajo la modalidad SaaS (Software as a Service).

En concordancia con la Resolución 1657 de 2025, que amplió a 36 meses el plazo para la implementación de la CIE-11, la institución se encuentra dentro del periodo establecido por el Ministerio de Salud y Protección Social para su adopción.

Considerando que el cumplimiento de este requerimiento se encuentra en etapa normativa y técnica inicial, y que su ejecución trasciende la vigencia del contrato de interventoría, este

aspecto se dejará como un punto abierto al cierre del proceso, a fin de que la entidad continúe con la gestión correspondiente ante el proveedor y con la planeación interna requerida para la futura adopción.

7. Gestión de la información de terceros
    - *"Si bien la interoperabilidad con las plataformas externas (Lumier para imágenes diagnósticas y Enterprise para laboratorio clínico) funciona de manera operativa, se identificó que actualmente no existe un seguimiento formal a las actividades del proveedor respecto a la gestión de respaldos (backups), planes de recuperación y esquemas de seguridad asociados a la información transmitida.*

    - *Adicionalmente, no se dispone de una arquitectura documentada que describa el flujo de datos, la infraestructura utilizada y los controles aplicados en estos servicios, lo que representa un vacío en la trazabilidad y en la gestión de riesgos tecnológicos.*

    - *En este sentido, se recomienda que el Hospital:*
        - *Exija a los proveedores la entrega periódica de evidencias sobre la ejecución de respaldos y planes de recuperación de la información.*
        - *Documente una arquitectura técnica que integre los servicios de laboratorio e imágenes con iMedical, de forma que se tenga claridad sobre los puntos críticos de interoperabilidad y sus medidas de seguridad.*
        - *Incorpore estas validaciones en la matriz de riesgos tecnológicos para asegurar un control integral."*

Concepto:
La interventoría revisó la información remitida, incluyendo los contratos suscritos con los proveedores Lumier y Enterprise, los cuales sustentan la relación contractual vigente.

Sin embargo, se observa que las acciones presentadas no atienden de manera directa las recomendaciones formuladas, dado que no se evidencian avances en la implementación de controles técnicos, ni en la documentación de la arquitectura de interoperabilidad, planes de respaldo o esquemas de seguridad asociados a la información gestionada por terceros.

En este sentido, se solicita tener en cuenta las recomendaciones emitidas por la interventoría, orientadas a fortalecer la gestión de riesgos tecnológicos y la trazabilidad de la información.

Adicionalmente, como sugerencia de mejora, se recomienda diseñar e implementar un checklist de verificación técnica transversal a los proveedores, que permita consolidar

de forma estandarizada las evidencias sobre respaldo, recuperación, seguridad de la información y los que el hospital considere.

Mientras se implementan las acciones sugeridas, este aspecto permanecerá en estado abierto.

8. Proceso de TI (Sistemas)

   (…) Se identificó que el área de Sistemas carece de una definición y mapeo formal de los procesos de TI, así como de documentación organizacional que respalde la estructura de funciones (organigramas, roles y responsabilidades). Esta situación puede generar riesgos en la continuidad operativa, la asignación clara de responsabilidades y el control efectivo de los activos tecnológicos(…)".

Concepto:
La interventoría reconoce el esfuerzo del Hospital en la elaboración del Manual de Procesos de TI, el cual constituye un avance importante respecto a la observación formulada. El documento aporta una primera formalización de los procesos y roles del área de Sistemas, contribuyendo a la estructuración organizacional y al cumplimiento de los lineamientos de la norma ISO/IEC 27001:2022.

No obstante, el manual aún requiere fortalecimiento para consolidarse como evidencia completa de gestión de TI. Se recomienda:

- Ampliar el detalle de los procesos incorporando flujogramas, entradas, salidas, controles, métricas e interrelaciones.
- Integrar una matriz RACI que asigne responsabilidades y dependencias funcionales.
- Vincular los procesos documentados con los controles aplicables de la ISO/IEC 27001:2022 (por ejemplo, A.5.9 Gestión de Activos, A.6.1 Gestión de Incidentes, A.5.23 Gestión del Cambio).
- Consolidar los procedimientos operativos y políticas de TI como anexos o documentos complementarios, garantizando su trazabilidad.

El avance es valorado positivamente; sin embargo, el punto se mantiene en desarrollo, hasta que se consolide la documentación completa y validada en el marco de los estándares de gestión de seguridad de la información y continuidad operativa.

9. *"Se revisó el inventario de equipos de cómputo presentado en Excel por el área de Sistemas y se verificó la existencia de la plataforma QSystem, informada por el hospital como el repositorio oficial de activos de la entidad:*

   Oportunidades de mejora:

   - *Inventario en Excel*
     - *El archivo incluye columnas básicas (Piso, Ubicación, Tipo, Placa y Observaciones), pero su nivel de detalle es limitado.*
     - *Carece de información técnica (marca, modelo, serial, fecha de adquisición, estado operativo) y de trazabilidad (usuario responsable, historial de mantenimiento).*

- *La columna Observaciones no aporta información diferenciada.*

- *Uso de QSystem como plataforma oficial*

  - *La institución informó que el inventario centralizado se gestiona en QSystem.*

- *Datos incompletos en el ejemplo:*
  - *Varios campos no tienen información (ej. observaciones, tipo de mantenimiento, criticidad, frecuencia de mantenimiento).*
  - *Esto refleja que, aunque la plataforma tiene la capacidad, los registros no están siendo diligenciados completamente.*
- *Ubicación física poco detallada:*
  - *En el formulario aparece "Torre, Piso, Servicio, Ubicación", pero en este ejemplo solo está diligenciado Piso 4 / Servicio Sistemas. Se recomienda siempre registrar la dependencia exacta o responsable asignado.*
- *Trazabilidad de responsables:*

  - *No se evidencia un campo para el usuario final o área responsable del equipo. Este dato es clave para auditoría y control patrimonial.*

- *Inconsistencias y vacíos:*
  - *Algunos campos aparecen con "N/A", lo cual puede restar confiabilidad (ej. seriales, placas duplicadas o vacías).*
  - *Esto refleja que la información no está completa o no fue actualizada de manera uniforme.*
- *Estandarización de datos:*

  - *Las áreas no siempre siguen el mismo formato (ej. "CONSULTA EXTERNA" vs "CONSULTA EXTERNA ASTRID VEGA").*
  - *Se observa mezcla de roles y nombres en algunas columnas que deberían ser más uniformes.*
- *Control de duplicidad:*
  - *En la columna de Placa y Serial debería garantizarse que no existan duplicados, ya que cada equipo debe tener un identificador único.*
- *Gestión de criticidad:*
  - *No se observa un campo para evaluar la criticidad del equipo (muy importante en hospital: un PC en admisiones no tiene el mismo riesgo que uno en facturación o en sistemas biomédicos).*
- *Auditoría de comodato:*
  - *El archivo indica que son equipos en comodato, pero no incluye la referencia al contrato de comodato, proveedor, ni condiciones de renovación/devolución.*
  - *Esto limita la trazabilidad legal/contractual de los activos.*

Concepto:
La interventoría revisó la aclaración presentada por el Hospital, en la que se informa que el inventario oficial de activos se administra a través del software SIIGO, y no en QSystem como se había reportado inicialmente.

Si bien esta precisión aclara la plataforma oficial de consulta, la información suministrada no evidencia cumplimiento integral de los controles de gestión de activos establecidos de acuerdo con las buenas prácticas de la norma ISO/IEC 27001:2022, particularmente en lo referente a la identificación, trazabilidad, mantenimiento y criticidad de los activos tecnológicos.

Se observa que los registros presentan niveles de detalle limitados e inconsistentes, carecen de campos técnicos obligatorios y no permiten garantizar una gestión integral ni un control efectivo de duplicidad o criticidad.

Adicionalmente, no se evidenció información sobre la marcación o etiquetado físico (marquillas) de los activos, lo cual constituye un control esencial para asegurar la trazabilidad, propiedad y fácil verificación durante auditorías o inventarios físicos.

En este sentido, se recomienda fortalecer el inventario de activos de TI, asegurando su integración con el área de Sistemas y el cumplimiento de los siguientes aspectos mínimos:

- Definir campos técnicos obligatorios (marca, modelo, serial, responsable, ubicación exacta, fecha de adquisición, estado, criticidad, contrato).
- Implementar mecanismos de control de duplicidad y validación periódica.
- Incorporar una matriz de criticidad y trazabilidad de responsables.
- Garantizar la marcación física estandarizada (marquillas) de los activos con códigos únicos vinculados al inventario digital.
- Alinear el registro con los controles A.5.9 (Inventario de activos), A.5.10 (Propiedad de activos) y A.5.11 (Uso aceptable de activos) de la norma ISO/IEC 27001:2022.

Como sugerencia de mejora, se propone desarrollar un checklist de validación de activos transversal a todas las áreas responsables, que asegure consistencia, trazabilidad y actualización continua de la información registrada en SIIGO.

Actualmente, el proceso se considera en etapa de fortalecimiento, hasta que se evidencie la consolidación del inventario con los campos, controles y marcación física correspondientes, la oportunidad de mejora continua abierta.

- Inventario de software:
  "*(…) no obstante, este inventario se limita a describir el modelo de contratación y el área responsable de la administración, sin contemplar aspectos clave de licenciamiento, control de versiones, criticidad, ni estado de autorización formal*

de uso. Adicionalmente, se observó que el inventario no incluye aplicativos de escritorio o software utilitario (ej. sistemas operativos, suite ofimática, software open source, freeware o desarrollos internos menores), salvo el licenciamiento documentado de Windows y Office.

Esta situación genera una visión fragmentada del ecosistema tecnológico institucional y dificulta la gestión integral de riesgos, la planeación de actualizaciones y el cumplimiento normativo en materia de software.

Concepto:
La interventoría revisó el documento "Listado de Sistemas de Información y Apps – F06 SIS Versión 01", en el que se relacionan los principales sistemas institucionales y programas utilizados por el Hospital Cardiovascular de Cundinamarca, diferenciando su propiedad y funcionalidad.
Este formato representa un avance frente a la observación formulada, al consolidar en un solo documento los sistemas clínicos, administrativos y de soporte operativo.
No obstante, el inventario aún presenta limitaciones frente a los controles de gestión de activos de software definidos en la norma ISO/IEC 27001:2022, dado que no incluye información sobre:

- Licenciamiento: tipo de licencia, número, vigencia y titularidad.
- Control de versiones y actualizaciones.
- Estado de autorización formal de uso (aprobado, en prueba, descontinuado).
- Criticidad o impacto operativo de cada sistema.
- Responsable funcional y técnico asignado.

Adicionalmente, se observa que el listado no incorpora sistemas operativos, aplicaciones utilitarias y desarrollos menores internos o freeware, lo cual genera una visión parcial del ecosistema tecnológico institucional y limita la trazabilidad del cumplimiento normativo en materia de licenciamiento y control de software.
En este sentido, se recomienda actualizar y ampliar el inventario de software, incorporando los elementos anteriores y alineando su estructura con los controles A.5.9 (Inventario de activos), A.5.10 (Propiedad de activos) y A.8.32 (Gestión del ciclo de vida del software) de la norma ISO/IEC 27001:2022.
Como sugerencia de mejora, se propone complementar el formato con una matriz de licenciamiento y control de versiones, que incluya responsables, fechas de renovación y estado de actualización, para fortalecer la planeación tecnológica y la gestión de riesgos asociados al uso de software institucional.

Con el propósito de dar continuidad al proceso de mejora y fortalecimiento institucional, se solicita presentar en un plazo máximo de diez (10) días hábiles los planes de trabajo correspondientes a los puntos en estado abierto, especificando acciones, responsables y fechas previstas de cumplimiento.

La interventoría acompañará la revisión de dichos planes para verificar su alineación con los objetivos de gestión tecnológica y de seguridad de la información.

Agradecemos su colaboración y la entrega de la información solicitada en un plazo no mayor a tres (3) días hábiles, contados a partir de la fecha del presente oficio.

Cordialmente,



CARLOS ALBERTO YEPEZ GOMEZ
Representante Legal
RYF CONSULTORIA SAS BIC