Bogotá D.C., 8 de Septiembre del 2025 INT-HCC-020-25

Doctor
GUILLERMO MAYORGA
Representante Legal
UT HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA
Ciudad

**ASUNTO: PRESENTACIÓN OPORTUNIDADES DE MEJORA PLATAFORMA IMEDICAL Y ACTIVOS DE INFORMACIÓN DE 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.

Esta interventoría se permite presentar las oportunidades de mejora identificadas sobre la plataforma de Imedical de Historias Clínicas y el proceso de activos de información de TI del Hospital Cardiovascular Navarro, actividad realizada en el mes de agosto 2025.

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.

   La no habilitación del cifrado en la comunicación entre usuarios y máquinas virtuales puede exponer la información a interceptaciones o accesos no autorizados, comprometiendo la confidencialidad de los datos en tránsito.

   Se recomienda habilitar de manera obligatoria el cifrado de tráfico entre usuarios finales y máquinas virtuales, asegurando que toda comunicación cuente con protección criptográfica extremo a extremo, reduciendo así el riesgo de exposición de información sensible.

### 10.3 PROTECCIÓN CRIPTOGRÁFICA DE MENSAJES

Para proteger los mensajes de control que se envían entre los centros de datos de Windows Azure y entre los clústeres de un centro de datos dado, se utiliza TLS con claves criptográficas de al menos 128 bits. Los clientes tienen la opción de habilitar el cifrado del tráfico entre los usuarios finales y las máquinas virtuales.

Documento: 7. PT01 INF SEGURIDAD Y CONFIDENCIALIDAD DE LA HISTORIA CLÍNICA IMEDICALCLOUD V3

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.
En particular, se evidenció un total de 599 casos, de los cuales 70 (12%) permanecen abiertos, sin documentación de cierre, incluyendo reportes acumulados de los años 2022, 2023, 2024 y 2025. Esta situación refleja una falta de cierre oportuno y control en la gestión de requerimientos.

| Año | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|
| No. Ticket | 1 | 7 | 7 | 55 |

Se recomienda al Hospital consolidar en la plataforma iMedical Cloud la totalidad del ciclo de vida de los casos (apertura, seguimiento y cierre), eliminando gradualmente la dependencia de archivos Excel y correos electrónicos como mecanismos de control, por lo que se sugiere:

- Definir un procedimiento formal de gestión de casos en la plataforma iMedical Cloud, que establezca responsables, tiempos de respuesta y cierre documentado.
- Configurar reportes automáticos en la plataforma para reemplazar los controles en Excel, garantizando así un único repositorio de información, actualizado en tiempo real.
- Ejecutar un plan de depuración y cierre de casos pendientes, priorizando los 70 casos abiertos (12% del total histórico), con énfasis en aquellos que datan de 2022 y 2023.

Con estas acciones, se optimizaría la trazabilidad, se minimizarían riesgos de duplicidad y retrasos, y se garantizaría la confiabilidad de la información para la toma de decisiones operativas.

Documento Tickets iMedical.xls.

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.

   Oportunidades de mejora

   - Pruebas periódicas del plan: No se evidencia la realización de simulacros o pruebas de recuperación. Es necesario definir cómo y cada cuánto se validará la efectividad del plan.
   - Tiempos de recuperación (RTO/RPO): Aunque se establece un umbral de 2 horas para activar formatos físicos, no se precisan tiempos objetivos de recuperación (RTO) ni el punto máximo de pérdida de datos tolerable (RPO).
   - Gestión de comunicaciones: Se recomienda incluir un protocolo de comunicación interna y externa que contemple cómo informar oportunamente a usuarios, proveedores, entidades de control o pacientes en caso de una caída prolongada.
   - Matriz de riesgos tecnológicos: Sería pertinente relacionar este plan con la matriz de riesgos informáticos, de modo que se identifiquen vulnerabilidades críticas y controles asociados.
   - Seguimiento post-incidente: No se establece un proceso formal para documentar, analizar y generar lecciones aprendidas tras el restablecimiento del servicio.

   El plan constituye una guía inicial adecuada y cumple con requisitos normativos básicos (Resoluciones 3100 de 2019, 1995 de 1999 y 0839 de 2017). Sin embargo, para evolucionar hacia un Plan de Continuidad de Negocio y Recuperación de Desastres (BCP/DRP) robusto, requiere complementarse con pruebas periódicas, definición formal de RTO/RPO, integración con respaldos, protocolos de comunicación y mecanismos de retroalimentación post-incidente e inclusión de proveedores o terceros

   Documento 1.PT03 DA PLAN DE CONTINGENCIA FRENTE A CAIDA DEL SISTEMA V3.pdf.

.

4. Control de Accesos: Cada usuario se autentica con su cuenta asignada, creada a solicitud, formal de las áreas responsables. Los perfiles determinan los permisos de lectura, escritura o impresión.

   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:

   - Usuarios asignados: Cuántos y quiénes tienen ese rol (Ejemplo: Rol “Auxiliar de Archivo” 3 usuarios activos).
   - Nivel de privilegio / permisos asociados Qué puede hacer ese rol (consultar, editar, eliminar, aprobar, administrar).

- Fecha de creación y última actualización del rol Para garantizar trazabilidad.
- Área o proceso al que pertenece Vincular el rol con el área (ej. Contabilidad, Enfermería, TI).
- Segregación de funciones Una nota que indique si el rol requiere controles adicionales para evitar conflictos (ej. “Super Usuario” debería estar muy restringido).
- Periodicidad de revisión Cada cuánto se revisan los roles y accesos (ej. semestralmente).
- Solicitar al proveedor la creación del reporte de roles y permisos.

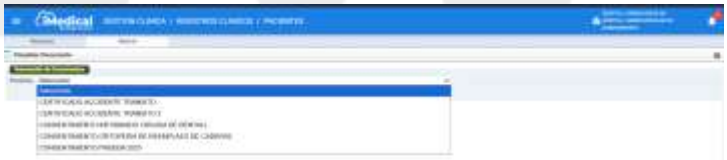
5. Consentimientos Imedical Cloud: De acuerdo con la revisión realizada frente a los criterios de la Ley 1995 de 1999 se identificó:

- Oportunidad de Mejora: 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.

  La gestión manual de los consentimientos puede generar incumplimientos en los requisitos legales y éticos relacionados con la autonomía, la decisión informada del paciente y la trazabilidad de la aceptación. Asimismo, incrementa la posibilidad de errores administrativos o pérdida de documentos.

  Se recomienda avanzar en la digitalización e integración completa de los consentimientos informados en la plataforma institucional, asegurando así cumplimiento normativo, mayor seguridad en el manejo documental y una mejor experiencia para el paciente.

Consentimientos cargados en la plataforma Imedical Cloud



- Se identificó que, aunque los consentimientos informados diligenciados manualmente son posteriormente cargados a la plataforma digital, no se observó con claridad sobre la gestión de los documentos físicos originales ni sobre su proceso de custodia, archivo o disposición final.

  La falta de lineamientos claros puede generar riesgos en la trazabilidad, duplicidad de registros, pérdida o deterioro de documentos originales, afectando la validez legal y probatoria de los consentimientos.

Se recomienda establecer y documentar un procedimiento formal que defina el manejo de los consentimientos informados físicos una vez digitalizados, asegurando su adecuada custodia y cumplimiento con la normatividad vigente sobre archivo clínico y conservación documental.

Se solicita presentar evidencias sobre la custodia y resguardo de esta información.

6. Prueba de consulta (no abordada durante la auditoría): Durante la ejecución de la auditoría no se revisó la implementación de la nueva normatividad relacionada con la adopción de la CIE-11 (Resolución 1442 de 2024 y Resolución 1657 de 2025). Sin embargo, considerando que la regulación establece la obligatoriedad de la codificación dual (CIE-10 y CIE-11) y un periodo de transición de 36 meses, se recomienda validar en futuras auditorías el grado de avance de la institución en este proceso.

   Sin embargo, 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

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.

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.

Se recomienda documentar y formalizar los procesos de TI en concordancia con las buenas prácticas y estándares internacionales como ISO/IEC 27001:2022, incorporando en los organigramas y manuales de funciones la estructura del área de Sistemas, roles, responsabilidades y relaciones de dependencia, de manera que se fortalezca la trazabilidad, la gestión de riesgos y el aseguramiento de la continuidad operativa.

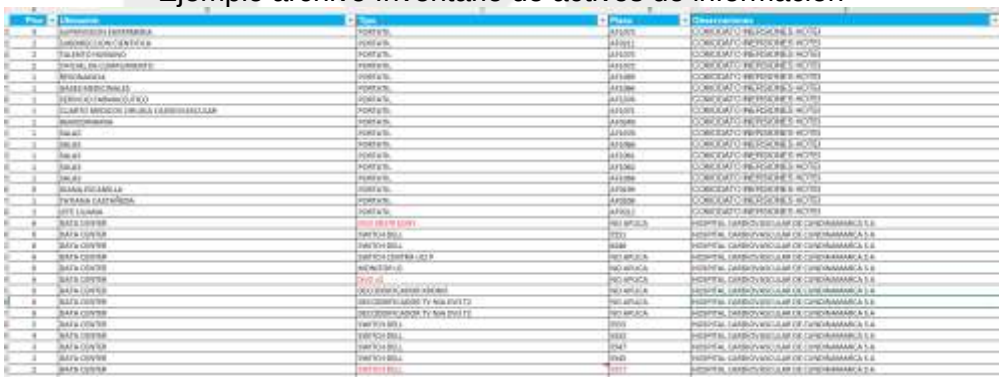
Por lo anterior, la interventoría tomó como punto de partida el proceso de Gestión de Activos, en la medida en que constituye uno de los pilares fundamentales dentro de la gestión de TI y está directamente contemplado en la norma ISO/IEC 27001:2022 (controles A.5.9 y A.5.10).

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.

Ejemplo archivo Inventario de activos de información



- Uso de QSystem como plataforma oficial

  - La institución informó que el inventario centralizado se gestiona en QSystem.
  - Sin embargo, se evidenció que la información registrada en la plataforma no está actualizada, lo cual compromete la confiabilidad de los datos y limita su utilidad como fuente oficial de control, como se observa en la siguiente imagen:

Consulta de activo AF0398 en QSytem



Como parte de la verificación realizada en la plataforma Qsystem al activo de información AF1061 se identificó:

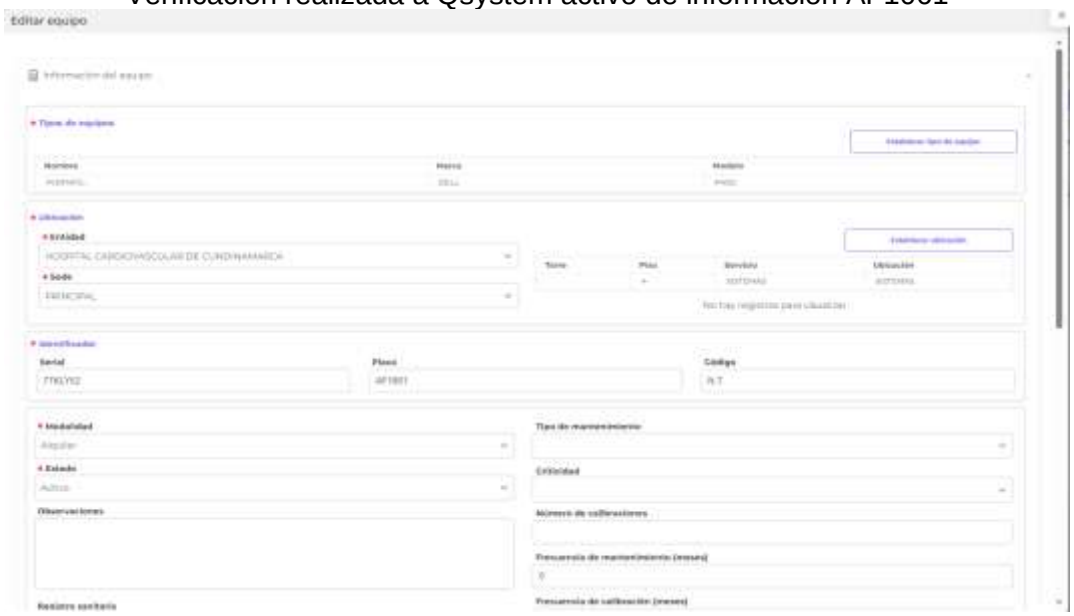
Fortalezas del registro

- Campos completos y estructurados: Incluye tipo de equipo, marca, modelo, serial, placa, código interno, modalidad (ej. alquiler), estado, ubicación (sede, piso, servicio, dependencia).
- Rastreo de mantenimientos y calibraciones: El sistema contempla campos para tipo de mantenimiento, frecuencia, número de calibraciones y criticidad, lo que aporta trazabilidad.
- Trazabilidad institucional: Relaciona el equipo con la entidad (Hospital Cardiovascular de Cundinamarca) y la sede específica, lo cual permite consolidar información por ubicación.
- Modalidad de adquisición: Permite registrar si es alquiler, comodato o propiedad, clave para la gestión contractual.
- Estado del activo: El campo “Activo” diferencia equipos disponibles, dados de baja o en mantenimiento.

Oportunidades de mejora

- 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.

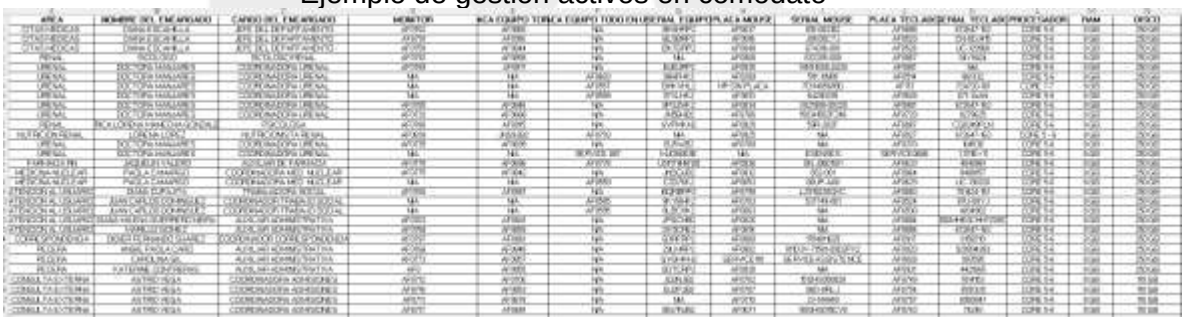
Verificación realizada a Qsystem activo de información AF1061




La plataforma QSystem ofrece las funcionalidades adecuadas para un inventario robusto de activos de TI, con campos técnicos, administrativos y de mantenimiento. Sin embargo, el análisis del registro evidencia que no se están diligenciando todos los campos disponibles, lo que genera información incompleta y pérdida de valor de la herramienta.
En otras palabras: la plataforma es adecuada, pero la debilidad está en el proceso de registro y actualización de la información.

Revisión de inventario de equipos en comodato:

Ejemplo de gestión activos en comodato



Aspectos positivos

- Detalle de la información: Este formato es mucho más completo que el Excel inicial. Incluye: área, encargado, cargo, placa, serial, RAM, disco duro, IP, usuario, fecha de instalación y de mantenimiento.
- Asignación de responsables: Cada equipo está relacionado con un área y un encargado, lo que facilita la trazabilidad.

- Datos técnicos incluidos: Se registra memoria RAM, disco, procesador, serial y dirección IP, información clave para gestión técnica.
- Control de fechas: Se incluyen fechas de instalación y de mantenimiento, lo cual permite auditar periodicidad y cumplimiento de mantenimientos.
- Clasificación por área/departamento:La tabla muestra equipos distribuidos en diferentes servicios hospitalarios (citas médicas, renal, medicina nuclear, farmacia, atención al usuario, etc.).

Oportunidad de mejora

- 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.

El archivo de inventario de equipos en comodato constituye un avance significativo frente al primer formato revisado, ya que contiene información técnica, administrativa y de fechas de instalación/mantenimiento.
Sin embargo, presenta inconsistencias, campos incompletos y ausencia de estandarización, lo cual afecta la confiabilidad como inventario oficial. Además, no incluye la relación contractual del comodato, un aspecto clave para auditoría.

10. Inventario de software: Se evidenció que el Hospital Cardiovascular de Cundinamarca cuenta con un inventario de sistemas de información y aplicativos contratados con terceros o de desarrollo propio, dentro del cual se incluyen plataformas como iMedical Cloud, Almera, Lumier, G-Suite Workspace, Enterprise, Delfín, Geovictoria, Siigo, QSystem, Firewall PFSense, OpenMediaVault, entre otros.

    Oportunidad de mejora: 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.

Se recomienda fortalecer el inventario existente de sistemas de información incorporando todos los aplicativos en uso dentro de la organización, independientemente de su origen o modelo de contratación. Dicho inventario debería incluir como mínimo:

- Nombre del aplicativo y proveedor.
- Tipo de licenciamiento (comercial, suscripción, open source, freeware, interno).
- Modelo de contratación (propio, terceros).
- Área responsable de la administración.
- Usuarios asignados y número de licencias adquiridas (cuando aplique).
- Versión instalada y fecha de última actualización.
- Nivel de criticidad para la operación institucional.

Así mismo, se recomienda establecer un procedimiento formal para la evaluación, autorización y registro de cualquier nuevo aplicativo, garantizando así control, trazabilidad y cumplimiento frente a políticas de TI y normativa aplicable.

Clasificación sugerida de aplicativos
Para organizar el inventario y facilitar su gestión, los aplicativos podrían clasificarse en:

- Sistemas de información contratados con terceros (ejm: iMedical Cloud, Almera, Lumier, Geovictoria, Siigo).
- Sistemas de información propios (ejm: Página web institucional).
- Software licenciado y de suscripción comercial (ej.: Windows, Office, mysql, oracle).
- Software open-source o freeware (ejm: pdf, winzip, vnc entre otros.)
- Aplicativos desarrollados internamente (in-house o por terceros a la medida).

Cada categoría debería contar con lineamientos de uso, control de versiones, validación de seguridad y criterios de mantenimiento para garantizar la confiabilidad y seguridad de los servicios de TI.

Como parte de la revisión, se efectuó un recorrido aleatorio por distintas dependencias del hospital con el propósito de validar la correspondencia entre las placas de identificación de los activos tecnológicos y la información registrada en el inventario oficial. Esta verificación permitió identificar coincidencias y posibles discrepancias entre los equipos observados en campo y los registros administrativos.

En el área de Informática se efectuó la revisión de tres equipos tipo ‘todo en uno’, identificándose que uno de ellos no contaba con placa de identificación institucional que permitiera distinguirlo como activo de la compañía o en condición de comodato. Esta situación dificulta el control patrimonial y la trazabilidad de los activos tecnológicos dentro de la organización.

Equipo ubicado en informática



Por otra parte, se validó el equipo identificado con la placa AF0388 y 0004 frente al inventario de activos proporcionado por el hospital y el reporte exportado desde QSystem, sin evidenciarse el registro de dichos activos en ninguno de estos controles. Esta situación refleja inconsistencias en la administración del inventario, lo que puede generar dificultades en el control patrimonial, seguimiento y trazabilidad de los activos tecnológicos.



Por otra parte, durante la visita al servicio de Atención en Ventanilla de Cardiología se identificó una impresora marca Lexmark. Se intentó realizar la validación de la placa del dispositivo frente a los inventarios institucionales; sin embargo, no fue posible llevar a cabo dicha verificación debido a que el equipo no contaba con placa de identificación.

Impresora Atención en Ventanilla de Cardiología



Se realizó visita al Datacenter Principal del Hospital Cardiovascular encontrando diferentes activos clasificados así:

- Se evidenció que el SWITCH DELL6247 se encuentra registrado en el inventario institucional; no obstante, durante la validación física se observó que el equipo cuenta con dos placas de identificación de activo con diferente numeración. Esta situación puede generar confusión en la trazabilidad, control y conciliación de la información entre el inventario y los activos físicos.



Análisis de activos identificados

- Etiquetado y control físico
  - Se observan equipos con etiquetas improvisadas (ejm “RAMIRO”, “COMPARTIDA”), lo cual no corresponde a placas oficiales de activos de la organización.
  - Varios equipos no cuentan con placa institucional formal de identificación (placa patrimonial o código de activo).

  La coexistencia de etiquetas manuales y la ausencia de placas oficiales generan riesgo de pérdida de trazabilidad y dificultan la conciliación con el inventario oficial.

- Equipos visibles en Data Center
  - Servidor Dell – identificado como “Servidor de carpetas compartidas”.
  - PC HP – usado como “Servidor proveedor Lumier”.
  - Servidor Lenovo ST550 identificado como “Servidor firewall hospital”.
  - Se observa además un servidor Dell adicional y un chasis HP que no parecen tener registro de placa en el inventario proporcionado.

- Inventario proporcionado (fragmento Excel)
  - Los tres activos listados (Dell, HP, Lenovo ST550) aparecen en el inventario bajo la ubicación “Data Center Principal”.
  - En el campo “Placa” aparece como “NO APLICA”, lo cual refleja que estos activos no tienen asignación de número de inventario formal o que no fue registrada.
  - En observaciones, todos figuran como pertenecientes al *Hospital Cardiovascular de Cundinamarca S.A.*

  - Oportunidades de mejora:
    - Inconsistencia en la identificación: equipos con placas improvisadas y ausencia de placas institucionales.
    - Registro incompleto: el inventario no consigna número de placa oficial (“NO APLICA”), lo cual limita el control patrimonial.
    - Dependencia de observaciones manuales: la información de propiedad se consigna en observaciones, no en un campo formal de control.

    Riesgo de duplicidad/confusión: etiquetas como “COMODATO” no permiten distinguir si el activo realmente pertenece al hospital, está en comodato o es de un tercero.

Equipos físicos Datacenter Principal





Inventario Activos Servidores

| Piso | Ubicación | Tipo | Placa | Observaciones |
|---|---|---|---|---|
| 1 | DATA CENTER PRINCIPAL | SERVIDOR CARPETA1 COMPARTIDAS - DELL | NO APLICA | HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S.A. |
| 1 | DATA CENTER PRINCIPAL | PC SERVIDOR PROVEEDOR «UNIR - HP | NO APLICA | HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S.A. |
| 1 | DATA CENTER PRINCIPAL | SERVIDOR FIREWALL HOSPITAL LENOVO ST550 | NO APLICA | HOSPITAL CARDIOVASCULAR DE CUNDINAMARCA S.A. |

Durante la validación física en el Data Center se identificó un servidor que no presta ningún servicio, se encuentra apagado y no dispone de placa de identificación institucional. Esta situación impide establecer con certeza su trazabilidad, propiedad y estado dentro del inventario oficial de activos tecnológicos.



Este proceso no debe limitarse a un inventario estático de equipos, sino que requiere un enfoque integral que abarque:

- Identificación y clasificación de todos los activos tecnológicos (hardware, software, licencias, redes, servicios en la nube, información crítica).

- Asignación de responsables claros para cada activo, asegurando trazabilidad y control.
- Ciclo de vida de los activos: adquisición, operación, mantenimiento, transferencia y disposición final, con criterios de seguridad de la información en cada fase.
- Relación entre activos y procesos de negocio, de manera que se conozca el impacto de cada activo en la operación institucional.
- Controles de seguridad y confidencialidad, garantizando que el acceso y uso de los activos esté alineado con la política de seguridad de la organización.

De esta manera, se busca trascender de un inventario descriptivo hacia un sistema formal de gestión de activos, que permita mitigar riesgos, optimizar recursos y garantizar la continuidad operativa.

La información solicitada deberá remitirse a esta interventoría en un plazo no mayor a diez (10) días hábiles.

**Cordialmente,**



**CARLOS ALBERTO YEPEZ GOMEZ**
**Representante Legal**
**RYF CONSULTORIA SAS BIC**