RYF S.A.S
Consultoría, Auditoría e Interventoría

ACTA DE REUNIÓN No. 8

RESPONSABLE DE LA REUNIÓN: Carolina Romero

(En caso de ser presencial):

FECHA: 19 septiembre 2025 VIRTUAL: _____ PRESENCIAL: X LUGAR: Hospital Cardiovascular de Cundinamarca

OBJETIVO DE LA REUNIÓN: Revisión Proceso de Soporte Técnico

HORA DE INICIO: 9_00 am HORA DE FINALIZACIÓN: __12:00 pm_____

ASISTENTES:

NOMBRE	ENTIDAD o DEPENDENCIA	CARGO	CORREO ELECTRÓNICO	TELÉFONO	FIRMA
Andrés Cruz	Hospital Cardiovascular de Cundinamarca	Coordinador Sistemas	Sistemas@hccsa.com.co	3209795384	
Nicolas Rojas Sánchez	Hospital Cardiovascular de Cundinamarca	Sistemaas	Sistemas@hccsa.com.co	3197941890	Nicolas Rojas
Carolina Romero	RYF SAS	Interventor TI	Trabajo.interventoria@gmial.com	3184050702	

1. TEMAS A TRATAR

Se llevó a cabo la revisión del proceso de soporte técnico, verificando la gestión de incidentes, tiempos de respuesta, canales de atención disponibles y cumplimiento de los acuerdos de servicio establecido.

2. DESARROLLO DE LA REUNION O DESCRIPCION DE ACTIVIDADES REALIZADAS

- **Canales de atención**:
  El proceso de soporte técnico dispone de los siguientes canales de atención: a través de WhatsApp al número 310 217 9101 y mediante la línea telefónica (601) 592 2979, extensiones 402 y 703, con disponibilidad permanente 7x24.

- **Registro de solicitudes:**
  Se evidenció que las incidencias y requerimientos actualmente se registran en una bitácora en Excel, donde se consigna información básica como fecha, usuario, departamento, tipo de incidente, técnico asignado, estado y observaciones. No obstante, este mecanismo no constituye un sistema formal de gestión de tickets, lo que limita la trazabilidad, el seguimiento y la generación de reportes.

  Por otra parte, se observó que el Hospital Cardiovascular de Cundinamarca dispone de un documento "*Gestión de servicios TIC HCC*" donde se pudo evidenciar:

  Fortalezas identificadas
  - Definición de canales claros: WhatsApp corporativo y línea telefónica interna, ambos con disponibilidad 24/7.
  - Orientación al usuario: Se enfatiza en garantizar una comunicación rápida y efectiva, incluso con la posibilidad de enviar fotos o capturas para agilizar el diagnóstico.
  - Priorización según criticidad: Se contempla un esquema de atención diferenciada para incidentes de baja, media y alta prioridad, lo cual es positivo en un entorno hospitalario.
  - Cobertura permanente: Se garantiza continuidad en los servicios hospitalarios gracias a la disponibilidad ininterrumpida.

  Vacíos o debilidades
  - Ausencia de un sistema formal de tickets: Aunque se mencionan los canales, no se evidencia un sistema automatizado para el registro, seguimiento y cierre de casos. Esto limita la trazabilidad.
  - Flujo de gestión poco detallado: El documento enuncia pasos generales de atención (recepción, asignación, atención remota/presencial), pero no especifica tiempos de respuesta (SLA) ni responsables de escalamiento.
  - Falta de métricas o indicadores: No se definen indicadores de desempeño como tiempo promedio de atención, tasa de resolución en primer contacto, o satisfacción del usuario.
  - Políticas generales: Aunque se definen horarios y disponibilidad, no se detallan protocolos de escalamiento ni niveles de servicio documentados.

  Hallazgo:
  El documento constituye una guía básica de atención de casos en el área de Sistemas del Hospital Cardiovascular de Cundinamarca, enfocada en la comunicación ágil con los usuarios y en la disponibilidad 24/7. Sin embargo, presenta debilidades en cuanto a formalización de procesos, trazabilidad y control, lo que se traduce en un hallazgo relevante desde el punto de vista de auditoría y gestión de calidad.

Riesgos asociados

- Baja trazabilidad: Al no existir un sistema de tickets, los registros dependen de controles manuales (Excel, bitácoras), lo que puede generar pérdida de información.
- Falta de control y auditoría: Sin métricas ni reportes, es difícil medir el cumplimiento y eficacia del soporte.
- Dependencia de canales informales: WhatsApp es ágil, pero no garantiza confidencialidad ni formalidad en la gestión de incidencias.

Documento: Bitacora de Soportes - Sistemas HCC.xls
Gestion de servicios TIC HCC.docx.pdf

- **Priorización de incidentes y Tiempos de atención y resolución (SLA):**
Aunque en el documento de gestión de servicios TIC del Hospital Cardiovascular de Cundinamarca se contempla la clasificación de incidentes por niveles de criticidad (alta, media y baja)

  En el documento de Gestión de servicios TIC HCC.docx.pdf en la práctica no se evidenció su aplicación en los registros ni en la atención de los casos. Adicionalmente, dichos niveles no cuentan con tiempos de respuesta y solución definidos.

  En la revisión de la bitácora de soporte y de los mecanismos de atención, se constató que no se documenta la categoría de criticidad en los incidentes reportados ni se relacionan tiempos de respuesta asociados a cada nivel.

  Riesgo:
  La falta de aplicación y de tiempos definidos por nivel de criticidad limita la efectividad de la priorización de incidentes, lo que puede generar demoras en la atención de casos críticos y afectar la continuidad de los servicios hospitalarios.

- **Escalamiento de incidentes**:
No se evidenció la existencia de un procedimiento formal de escalamiento para los incidentes que no pueden ser resueltos en la primera línea de soporte técnico.

  En la documentación revisada sobre la gestión de servicios TIC y en la práctica de atención de casos, no se encontraron lineamientos, responsables ni tiempos definidos para el escalamiento de incidentes hacia niveles superiores de soporte.

  La ausencia de un procedimiento de escalamiento puede ocasionar retrasos en la solución de incidentes complejos o críticos, dependencia de la discrecionalidad del personal de soporte y afectaciones a la continuidad operativa del hospital.

- **Evidencias de resolución y cierre de casos:**
No se evidencian procedimientos ni registros que documenten las evidencias de resolución y el cierre formal de los casos atendidos por el área de soporte técnico.

  En la revisión de la bitácora de soportes y en la documentación de gestión de servicios TIC, no se encontraron mecanismos que respalden de manera verificable la resolución ni el cierre de las incidencias registradas.

  Riesgo:
  La falta de evidencias de resolución y de un cierre formal de los casos limita la trazabilidad y transparencia del proceso, dificulta la validación de la efectividad de las soluciones aplicadas y puede derivar en reincidencia de incidentes o en reclamos por parte de los usuarios sin soporte documental.

- **Reportes periódicos**
  No se generan reportes periódicos de la gestión de soporte técnico, bajo el argumento de que todos los casos son atendidos el mismo día.
  En la revisión de la bitácora de soportes, correspondiente al periodo 26 de junio de 2025 a 25 de septiembre de 2025 (240 registros), se observó lo siguiente:
  - De los casos con fechas de solicitud y solución válidas (136 registros), 133 (98%) se reportan como resueltos el mismo día.
  - Existen 3 registros (2%) con diferencias en las fechas, incluyendo inconsistencias como solución anterior a la solicitud.
  - 104 registros (43% del total) no consignan fecha de solución, lo que impide confirmar la atención real de los incidentes.
  - No se identificaron reportes de consolidación o análisis periódico que permitan verificar tendencias, tiempos de atención promedio o reincidencias.

  Riesgo:
  La ausencia de reportes periódicos y la existencia de registros incompletos/inconsistentes limitan la capacidad de verificar de manera objetiva la oportunidad en la atención, afectan la trazabilidad del proceso y dificultan la implementación de acciones de mejora basadas en datos confiables.

- **Evaluar el control de acceso al WhatsApp corporativo y confidencialidad en la atención.**
  No se evidenció la existencia de controles de acceso, políticas de uso ni lineamientos formales que regulen la confidencialidad de la información gestionada a través del canal de WhatsApp corporativo para la atención de incidentes y requerimientos.

  En la revisión documental y de la práctica operativa, no se encontraron procedimientos que definan:
  - Usuarios autorizados para administrar el canal de WhatsApp corporativo.
  - Políticas de confidencialidad y protección de la información tratada en este medio.
  - Reglas de seguridad relacionadas con conservación, respaldo o auditoría de la información transmitida.

  Riesgo:
  La ausencia de controles de acceso y políticas de confidencialidad en el canal de WhatsApp corporativo puede derivar en riesgos de exposición de información sensible, manipulación no autorizada, pérdida de trazabilidad y vulneración de principios de seguridad de la información (confidencialidad, integridad y disponibilidad).

- **Retroalimentación y mejora**
  No se evidenció la existencia de actividades de capacitación, espacios de retroalimentación ni aplicación de encuestas de satisfacción a los usuarios sobre el servicio de soporte técnico.

  En la revisión de la documentación de gestión de servicios TIC y de los registros de soporte, no se encontraron planes de capacitación a usuarios, mecanismos de retroalimentación formal ni reportes de encuestas de satisfacción que midan la percepción del servicio.

  Riesgo:
  La falta de capacitación y retroalimentación limita la capacidad de los usuarios para prevenir incidentes recurrentes, impide identificar oportunidades de mejora en el servicio y debilita la medición de la satisfacción del usuario, lo que puede afectar la calidad percibida y la eficiencia del soporte técnico.

3. CONCLUSIONES DE LA REUNIÓN

Recomendaciones

1. Gestión de Incidentes (ITIL v4 – Service Operation)
    - Implementar un sistema formal de gestión de tickets que permita registrar, clasificar y dar seguimiento a cada incidente y requerimiento desde su apertura hasta su cierre.
    - Recomendación técnica: considerar el uso de GLPI (open source), que ofrece funcionalidades de gestión de tickets, base de conocimientos, SLA y reportes. Alternativamente, pueden evaluar otras soluciones en función de su presupuesto y necesidades.
2. Clasificación y Priorización de Incidentes
    - Definir de manera formal la matriz de criticidad (alta, media, baja) con criterios claros y tiempos de atención/resolución (SLA) asociados.
    - Configurar en el sistema de tickets el flujo automático de priorización, garantizando que los incidentes críticos sean atendidos en menor tiempo y con visibilidad gerencial.
3. Gestión de Escalamiento (ITIL v4 – Incident Management & Problem Management)
    - Documentar un procedimiento de escalamiento (funcional y jerárquico) que defina responsables, niveles de soporte y tiempos de escalamiento.
    - Incluir estos pasos en el sistema de tickets para que el proceso sea automático y trazable.
4. Evidencias de resolución y cierre de casos
    - Establecer la obligatoriedad de documentar la evidencia de resolución (capturas, reportes técnicos, logs) antes del cierre del ticket.
    - Configurar en el sistema de tickets un flujo de cierre formal, con validación del usuario cuando aplique.
5. Generación de reportes e indicadores (ITIL v4 – Continual Improvement)
    - Definir un esquema de reportes periódicos (mensuales/trimestrales) con indicadores de desempeño (KPI):
        - Tiempo promedio de atención y resolución.
        - % de incidentes resueltos en primer nivel.
        - Número de incidentes por categoría.
        - Niveles de satisfacción del usuario.
    - Se recomienda que estos reportes sean presentados a la dirección para análisis y mejora continua.
6. Gestión de la Seguridad de la Información (alineado con ITIL v4 y ISO 27001)
    - Formalizar controles de acceso al canal de WhatsApp o sustituirlo progresivamente por el uso del sistema de tickets.
    - En caso de mantener WhatsApp como canal complementario, definir:

- Usuarios autorizados.
- Políticas de confidencialidad.
- Procedimiento de respaldo y trazabilidad de la información recibida.

7. Gestión de la Experiencia del Usuario (ITIL v4 – Service Desk)

   - Implementar encuestas automáticas de satisfacción al cierre de los tickets.

   - Desarrollar un plan anual de capacitaciones y retroalimentación para los usuarios, con el fin de:
     - Reducir incidentes recurrentes.
     - Mejorar la percepción del servicio.
     - Fortalecer la relación entre usuarios y área de TI.

8. Gestión de proveedores y servicios tercerizados (ITIL v4 – Supplier Management / Service Level Management)

   - Centralizar en el mismo sistema de tickets (GLPI u otro ITSM) todos los incidentes y requerimientos relacionados con plataformas tercerizadas, aunque su resolución dependa del proveedor externo.

   - Establecer un procedimiento de registro y seguimiento de los casos tercerizados, incluyendo:
     - Identificación del proveedor responsable.
     - Tiempo de escalamiento hacia el proveedor.
     - Monitoreo de cumplimiento de los SLA contratados.

   - Configurar el sistema de tickets para que permita clasificar incidentes internos y tercerizados, manteniendo trazabilidad de todos los casos en un repositorio único.

Concepto

Adoptar un sistema como GLPI u otro aplicativo de ITSM permitirá:

- Formalizar la gestión de incidentes y requerimientos.
- Asegurar trazabilidad y cumplimiento de SLA.
- Generar indicadores clave para la mejora continua.
- Reducir la dependencia de canales informales como WhatsApp.
- Se elimina la dispersión de la información.
- Se asegura que la dirección tenga visibilidad completa de los servicios críticos (internos y tercerizados).
- Se fortalece la gestión de proveedores y el cumplimiento de acuerdos contractuales

Esto alinea el proceso de soporte técnico con las mejores prácticas de ITIL v4, mejora la gobernanza de TI y fortalece la seguridad de la información institucional.

Nota: Las recomendaciones aquí presentadas se enmarcan en las buenas prácticas de ITIL v4 y en la necesidad de fortalecer la trazabilidad y el control del proceso de soporte técnico. El Hospital Cardiovascular de Cundinamarca es libre de adoptar la metodología y la herramienta tecnológica (ejm. GLPI u otra solución ITSM) que considere más adecuada a sus necesidades y recursos.

COMPROMISOS O ACTIVIDADES PENDIENTES

No aplica

COMPROMISOS DE LA REUNIÓN

ITEM	ACTIVIDAD	RESPONSABLE	FECHA DE ENTREGA
1			
2			