22 de septiembre de 2025

Doctor
CARLOS ALBERTO YEPEZ GOMEZ
Representante Legal
RYF CONSULTORIA SAS BIC

Carolina Romero
Interventora componente Sistemas
RYF CONSULTORIA SAS BIC

Asunto: Contestación Requerimiento – Componente Sistemas

En atención al requerimiento formulado por la interventoría, el Departamento de Informática del Hospital Cardiovascular de Cundinamarca presenta a continuación la respuesta correspondiente al punto 4, relacionado con la seguridad en la plataforma iMedical Cloud.

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.

Respuesta: 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.

Cordialmente,



Malitson Torres
Coordinadora de Informática
Hospital Cardiovascular de Cundinamarca