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

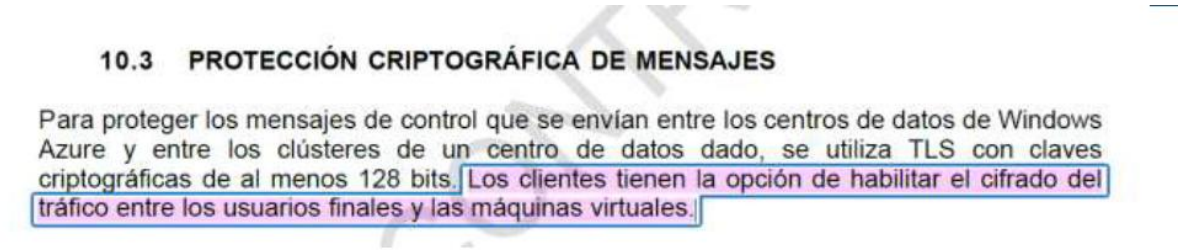
Asunto: Contestación Requerimiento – Componente Sistemas

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 1, relacionado con la seguridad en la plataforma iMedical Cloud.

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

Respuesta: 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.

Cordialmente,



Malitson Torres
Coordinadora de Informática
Hospital Cardiovascular de Cundinamarca