LICITACION PUBLICA N° 26/24
PLIEGO TÉCNICO
LICITACION PÚBLICA DE LABORATORIO
HOSPITALES SAN MIGUEL ARCÁNGEL, SANTA MARÍA Y LARCADE

OBJETO: El presente pliego, tiene por objeto la adquisición de software de gestión para los laboratorios de los hospitales Larcade, San Miguel Arcángel y Santa María por 10 meses.

SECCIÓN N° 7: SOFTWARE
Red Informática, Hardware y LIS.

SOFTWARE DE GESTIÓN
Se solicita el alquiler de un software de Gestión de Laboratorio que realice el seguimiento de muestras y resultados incorporando etapas preanalíticas, analíticas y postanalíticas y que incorpore conceptos de calidad y seguridad de última generación. El sistema debe integrar los instrumentos y aplicaciones de laboratorio y permitir gestionar e intercambiar datos entre las distintas secciones. Deberá contar con la cantidad de usuarios necesarios para la gestión de todas las secciones, según demanda del laboratorio.
El OFERENTE deberá proveer, instalar y configurar un Sistema Informático de Laboratorio, que permita la integración tanto con aparatos automatizados existentes y/o por instalarse en el laboratorio posibilitando el intercambio de datos en forma bidireccional, como con el Sistema Informáticos Hospitalario / Clínico existente o que pueda funcionar en la institución, debe contemplar también los desarrollos necesarios que deriven de mejoras en el sistema hospitalario y clínico existente. Así también, deberá ofrecer interfaces de interoperabilidad para su integración en sistemas existentes y futuros, teniendo como base la carga automática de las órdenes de laboratorio generadas desde el sistema de salud y la visualización en ese sistema de los resultados de todos los análisis realizados en el laboratorio que estén validados en forma parcial o completa. El api debe enviar al sistema de laboratorio las órdenes de laboratorio generadas por el profesional médico, que se cargarán como pendientes en el sistema de laboratorio. Una vez finalizadas, desde el sistema de salud se debe mostrar -para el paciente consultado- el listado de todos los análisis que se le practicaron; al seleccionar uno, mostrará las determinaciones realizadas, con los valores obtenidos.
Las integraciones deben cumplir con los requisitos de seguridad definidos por la Dirección de Seguridad Informática del municipio y devolver los parámetros según lo establecido en la documentación técnica adjuntada sobre el servicio. Se adjunta requerimientos funcionales del servicio de integración.
El plazo de instalación y puesta en marcha no podrá superar los 30 días corridos a partir de la fecha de emisión de la OC.
La empresa responsable del software deberá realizar la configuración de todos los analíticos, valores de referencia, y todo lo necesario para la puesta en marcha del sistema, limitando las tareas del personal de laboratorio a controlar los datos ingresados y brindar la información necesaria para la configuración (valores de referencia, tipos de muestra, etc.) del sistema.
Se debe realizar la homologación y vinculación automática de los códigos de las determinaciones del sistema Markey y el sistema de laboratorio, facilitando el intercambio de información entre los sistemas, utilizando el Nomenclador Bioquímico único.

Al momento de la instalación se configurarán la cantidad de puestos de trabajo según necesidad del servicio.

El Curso de Capacitación debe ser dictado por dos o más Profesionales Capacitados. Debe durar no menos de cinco (5) días corridos (de lunes a viernes) en caso de ser presencial, y no exceder los diez (10) días en caso de ser remoto. El curso debe estar configurado para ser teórico práctico, y el Laboratorio deberá poder operar sin asistencia al momento de concluir la capacitación. La capacitación debe permitir al personal del laboratorio trabajar sin la necesidad de intervención del Proveedor, debe poder realizar el alta, baja y modificación de prácticas de laboratorio, así como configurar y modificar equivalencias de análisis para ajustarse al trabajo con los instrumentos.

Las actualizaciones y nuevas versiones del producto dentro del período de contratación deben ser SIN COSTO ADICIONAL, quedando a cargo del PROVEEDOR de la solución los costos de movilidad o viáticos.

La conexión directa o a través de la interface al sistema informático del servicio de Laboratorio, deberá proveerse sin costo adicional para el Hospital, y conjuntamente con la entrega del equipo adjudicado, dicha conexión deberá ser aclarada en el pliego. Será responsabilidad del oferente del sistema informático garantizar dicha conexión como también la necesaria con el sistema médico instalado actualmente en los hospitales y sus futuras modificaciones (incluidos cambios de sistema médico)

DEL SISTEMA:

El sistema de gestión debe ser un software de gestión integral para laboratorio, que contemple las áreas, preanalítica, analítica y postanalítica, desde la llegada del paciente/muestra al laboratorio hasta el retiro de los resultados, o el envío de los mismos por Correo o hacia una Aplicación Mobile. El software deberá poder administrar múltiples laboratorios en forma integral. Deberá cumplir con las siguientes características:

Se deberá entregar usuario y contraseña tanto para la administración de los servidores como de las DB

Se guardarán los datos unificados en una única base de datos, alojada en un servidor dentro de la red municipal. Dicha base de datos deberá contar con licencia.

El Sistema debe permitir la gestión integral y en una única plataforma de los procesos en las etapas preanalíticas, analíticas y postanalíticas, así mismo que integre la gestión de los tubos (tracking) con la gestión de los pacientes, sus resultados y los resultados de QC.

El Entorno Windows Server y/o servidores Linux deberá ser provisto, conectado y mantenido por el oferente. El mismo deberá asesorar técnicamente respecto al manejo de dicho sistema de gestión, el cual deberá ofrecer una conexión vía red para los siguientes sectores:

- Secretaría y admisión de muestras
- Hematología
- Hemostasia
- Química Clínica
- Orinas y Parasitología
- Endocrinología y Marcadores tumorales
- Inmunoserología
- Bacteriología
- Guardia

Deberá contar con lo siguiente:

Módulo de Microbiología
Módulo de Urgencias
Módulo de consulta remota para todos los servicios médicos fuera del laboratorio (entorno web).
Módulo de seguimiento de QC de todos los instrumentos conectados. (no excluyente)
Conexión de todos los instrumentos al Sistema de Gestión.
Ejecución de repeticiones de análisis automatizados desde el mismo LIS. (no excluyente)
Página web para el Laboratorio.
Aplicación web de consulta de resultados para pacientes.

Aplicación web de consulta de resultados para servicios médicos.
Aplicación web de consulta de resultados para eventuales derivantes.
Envío de resultados por mail
Paneles de control con estadísticas de autovalidación, análisis de volumen, análisis de carga de trabajo de muestras, repetición de análisis, revisiones de resultados atípicos, plazos del proyecto, procesamiento de las muestras, análisis del TAT.
Módulo de control de stock y proveedores que permitan generar ingresos de mercadería en forma automática con remito y correlacionar stock versus producción.
Módulo estadístico que provea datos de consumo, frecuencia y predictivos, tanto numéricos como gráficos, accesibles desde cualquier computadora conectada al LIS, análisis de resultados por poblaciones, de análisis de métodos manuales y automatizados
Módulo estadístico para Microbiología que provea cantidad y detalle de muestras, aislados, medios utilizados, pruebas, antibióticos, resultados, entre otros.
Sistema de turnos programables.
Monitoreo en tiempo real de las diferentes áreas de trabajo.
Sistema de pre peticiones a instalar en servicios médicos a designar por el Laboratorio
Guardia IT las 24 horas
Aplicación Mobile en App Store y Play Store que permita de manera personalizada la visualización de resultados de cada paciente.
En caso de no contar con alguno de los módulos requeridos, se deberá especificar el tiempo para su desarrollo e implementación, el costo debe estar incluido en la propuesta.
El oferente deberá hacer una demo del software ofertado en un entorno de prueba y asegurar las condiciones de interoperabilidad con nuestro sistema de gestión
El sistema de gestión informático deberá contar con las siguientes utilidades:
Mediante el software se deberá llevar a cabo la gestión integral para todas las secciones detalladas.
El sistema se debe entregar con manual completo en español, en su última versión, impreso y digitalizado.
En el caso de que la empresa adjudicada en todas las áreas del laboratorio, sea diferente a la de la licitación anterior
(Sistema de Gestión de Laboratorio), el proveedor de software deberá garantizar el desarrollo de una interfase que permita el acceso a los históricos de pacientes en el formato que el sistema previo determine.
La firma oferente deberá proveer e instalar un antivirus OEM y sus actualizaciones correspondientes, durante el periodo de la licitación, compatible con el sistema de gestión
Será evaluado favorablemente que el software sea de producción nacional.

El oferente deberá entregar un listado con no menos de 3 (tres) instalaciones en el ámbito nacional de similar envergadura a la nuestra donde se encuentre funcionando con al menos 5 secciones de laboratorio interconectadas y con más de 1 año de antigüedad.

Características del sistema:

1- Turnos e ingresos de pacientes y muestras

a) El sistema debe contar con un módulo de turnos, que forme parte del mismo sistema, para que permita el manejo de toda la información inherente al paciente al momento de dar o modificar un turno. Dicho módulo debe poder definir límites de cantidades de pacientes a citar y manejar excepciones para aumentar o disminuir temporariamente la cantidad de pacientes; debe definir los días festivos para no ser considerados al citar a los pacientes y debe poder anular franjas completas de trabajo durante las cuales no se puedan dar turnos. El módulo de turnos debe permitir ingresar solo los datos demográficos y el tipo de prestación, o incorporar también las prestaciones (pre ingresos).
b) El ingreso de pacientes deberá incluir: datos demográficos, grupo poblacional, médico solicitante, origen, cobertura y otros datos adicionales de los pacientes a requerimiento del laboratorio.
c) La identificación del paciente debe incluir, además de tipo y número de documento, criterios adicionales de identificación como ser número de internación, número de historia clínica, número de afiliado; los cuales podrán utilizarse para búsquedas y filtros de información.
d) La numeración de las peticiones deberá ser correlativa, sin posibilidad de reutilizar números de peticiones que fueran anuladas previamente.
e) Deberá permitir emitir en forma impresa, recomendaciones de toma de muestra del análisis al paciente y al extraccionista.
f) Deberá permitir informar al paciente la fecha de entrega de resultados teniendo en cuenta: definición de días de proceso de cada prueba, contemplando tanto demoras normales como urgentes. El sistema debe proveer la opción de pactar una entrega parcial de los resultados para aquellos casos en que existan diferentes fechas de entrega.
g) Para el caso de entrega de muestras en forma tardía, deberá permitir la recepción de las mismas, conservando el mismo número de identificación primario, por ejemplo: orina entregada al día siguiente con el mismo número de petición.
h) El módulo debe poder mostrar en pantalla la cantidad de turnos dados para un día determinado, la cantidad de turnos cumplidos y la cantidad de turnos que no se cumplieron para cada día en que se ha dado un turno, utilizando los registros de Ingresos de Pacientes.
i) El módulo de turnos debe poder mostrar en un esquema de calendario la saturación y presentismo de no menos de cuatro (4) meses, de forma de poder analizar la posible concurrencia en los próximos 30/60 días.
j) Con la carga del Turno, el sistema debe utilizar la información ya cargada a la hora de atender al Paciente el día de la Extracción, el sistema debe automáticamente generar el ingreso con la información cargada en el Turno.

2 - El sistema deberá generar etiquetas de código de barras para la total automatización de las tareas. Todos los resultados se podrán imprimir en diferentes impresoras con formatos configurables por el laboratorio. Se podrán generar hojas de trabajo, informes, estadísticas con formatos múltiples y configurables por el laboratorio.

a) Permitir que el usuario pueda definir el formato de impresión.
b) Permitir que se incorpore a la etiqueta información adicional como el origen de la muestra, tipo de la muestra, área de trabajo, análisis solicitados, nombre o identificación codificada del paciente, etc.
c) Permitir que se pueda definir la cantidad de etiquetas por tipo de muestra, incluyendo la no impresión de determinada etiqueta.
d) Permitir que se puedan definir etiquetas adicionales de control, para garantizar la correcta correlación entre la orden emitida por el médico y las etiquetas de códigos de barra de las muestras.
e) Permitir la reimpresión de etiquetas en su totalidad, sólo de un área o tipo de muestra o sólo la de control.
f) En caso de tratarse de una muestra de Urgencia, la etiqueta debe poder generarse con un indicador URG para que sea claramente identificado el tubo de Urgencia

3- El sistema debe soportar versionado tanto de Prestaciones como de Determinaciones. Significa que en caso de cambiar el grupo de determinaciones que componen una prestación esto generará una nueva versión de la prestación sin necesidad de crear una nueva. En el caso de las Determinaciones, significa que en caso de modificar tanto los métodos o valores normales, no será necesario generar una nueva determinación. El sistema seguirá reflejando para cada pedido en el tiempo la versión de prestación y determinación correspondiente en cada caso. Esto impedirá sobrecargar innecesariamente tanto el listado de prestaciones como determinaciones por cambio de tecnología, metodología de procesamiento de las muestras o cambios en la manera de informar.

4- El sistema debe ajustarse a las Ley Nacional de SIDA 23.798 y su decreto reglamentario 1.244/91, y a la Ley de Identidad de Género 26.743.

a) Sin necesidad de hacer una doble carga, o doble ingreso de paciente, el Sistema debe gestionar de forma autónoma la impresión de Resultados Protegidos, para las prestaciones que determine el Laboratorio. Se debe poder generar el protocolo no codificado con la leyenda que el Laboratorio determine y el Codificado por Ley sobre el mismo Ingreso de Muestra.

b) El Sistema debe permitir, de ser necesaria, la impresión de Sobres con la Codificación de Pacientes y datos del Ingreso según lo que solicita la Ley Nacional de SIDA, para la entrega de resultados positivos.

c) El sistema debe contemplar el registro de Sexo y Género, la información impresa del paciente debe ser consistente con lo que dictamina la ley y, para uso interno, los valores de referencia sean consistente con la biología del paciente.

5) El sistema debe contar con un control de sobre prestaciones; para ello deberá alertar que un análisis se ha solicitado nuevamente, si es que aún existe un pedido previo sin informar, o que se lo está repitiendo en un intervalo de tiempo innecesario. También deberá alertar si el estudio requiere autorización médica de nivel superior.

6) El sistema deberá contar con un módulo para registrar la extracción y recepción (check in) de muestras, indicando extraccionista, condiciones de la muestra, datos adicionales obtenidos al momento de la extracción, indicaciones para el extraccionista, y la eventual no concurrencia del paciente al box de extracciones para dejar sin efecto el ingreso.

7) Deberá permitir el control de resultados en base a antecedentes visibles del paciente en el momento de la validación, permitir al Laboratorio la posibilidad de definir reglas lógicas que realicen distintas acciones sobre los datos del paciente en función de los datos demográficos de la petición y de los resultados del mismo.

8) Resultados y validación

a) El sistema debe permitir el ingreso de diferentes tipos de resultados: numéricos, carácter, codificados, textos adicionales que conviven con el resultado, y permitir ingresar resultados tipo carácter donde habitualmente se espera un número.

b) A los efectos de facilitar la labor bioquímica de validar los resultados del paciente, el sistema deberá permitir visualizar en forma rápida y eficiente (a continuación del mismo en la misma ventana o pantalla), resultados anteriores, si los tuviese, para cada una de las determinaciones en ese paciente.

c) El sistema deberá contemplar la opción de resaltar mediante diferentes colores o similar, cuando se presenten valores fuera de los rangos especificados por el laboratorio o de existir diferencia con resultados anteriores. El delta check deberá poder ser modificado para cada determinación según el criterio del laboratorio.

d) Deberá permitir validar los datos del paciente por: grupo poblacional, resultados anteriores, delta check, por edad, sexo, método, y rechazar automáticamente aquellos resultados que se encuentren fuera del criterio de validación definido por el laboratorio, no permitiendo validar datos incompatibles con la vida. La validación deberá ser sectorizada, impidiendo que usuarios de un sector modifiquen o validen resultados de otro sector.

e) El sistema debe permitir, al momento de ingreso de resultados, solicitar pruebas adicionales sobre las muestras solicitadas desde la misma pantalla, solicitar nuevas muestras para repetición o recitar pacientes en los casos que fuera necesario.

f) El sistema debe permitir visualizar en el ingreso de resultados la última ubicación conocida de una muestra y poder consultar las muestras procesadas por instrumento en todo momento.

g) Además de la validación por cada sector, el sistema debe permitir la firma electrónica del informe en su totalidad, punto de revisión final antes de ser liberado al paciente. Este firmado debe realizarse no de forma genérica, sino que debe presentar la firma del bioquímico autorizado a tal efecto.

h) El sistema deberá contemplar múltiples modos de ingreso de resultados (por orden, por paciente, por origen de las muestras, por sector del laboratorio, por análisis, por determinación, instrumento, planilla de trabajo, sector, médico solicitante, etc.)

i) Deberá permitir la trazabilidad de los resultados informados, permitiendo conocer quién ingresó, participó en los diferentes estadios/repeticiones de un resultado, validó, imprimió y entregó los resultados y la metodología utilizada.

j) Deberá tener la posibilidad de ser accedido a través de un navegador web, para la consulta de resultados desde los consultorios de la institución, en el caso de requerir cableado adicional el proveedor deberá hacerse cargo de dicha instalación. En el caso de no requerir cableado, el oferente deberá especificar el tipo de tecnología a utilizar. Los resultados confidenciales solo podrán ser accedidos por personal especialmente autorizado. Este acceso web debe permitir la impresión de los Protocolos Firmados por el Personal, de forma idéntica a como se entregan desde el Laboratorio Central.

k) Todos los resultados incorporados en el sistema deben quedar registrados de forma inalterable, de manera de mantener una trazabilidad total de todos los datos incorporados en el sistema. En el caso de tener que realizar corrección y cambio de resultados el sistema debe mantener cada ocurrencia del resultado.

l) Deberá proveer mecanismos múltiples de ordenamiento y filtrado de la información, de manera de poder visualizar los resultados por al menos los siguientes criterios: estado de los resultados, rangos (normales/fuera de lo normal/patológicos), sector, instrumento.

9) Alertas y Urgencias Médicas

a) El Sistema debe contar con un módulo de Urgencias que, en un período de tiempo a determinar por el Laboratorio, se evalúe automáticamente si se debe informar de alguna Alerta Médica evaluando los resultados de los pacientes de una clase, categoría, origen o procedencia. El envío de las alertas debe ser totalmente automático sin la necesidad de intervención alguna de personal del Laboratorio u otras partes.

b) El Sistemas debe contar con una Aplicación Mobile de Urgencias Médicas que permita al laboratorio enviar mensajes y resultados de Urgencia directamente a los Médicos Autorizados.

10) Guardias Médicas

a) El sistema debe contar con una Aplicación Mobile de Guardias Médicas para que los Médicos autorizados por el laboratorio puedan acceder a los resultados desde su Smartphone. Esta aplicación debe funcionar dentro y fuera de la Institución.

b) Será potestad del laboratorio permitir o denegar a los Médicos el acceso a los resultados desde la Aplicación Mobile de Guardias Médicas.

c) La autorización o denegación de permisos para los Médicos deberá constar con un tiempo establecido, y será renovada por un período de tiempo que el Laboratorio decida.

11) El sistema debe poder, en base a condiciones lógicas definidas por el usuario, rechazar pruebas de acuerdo a criterios definidos por el laboratorio.

12) El sistema deberá contar con un módulo estadístico que brinde información de cantidad de determinaciones o pacientes según diferentes criterios: médico solicitante, grupo poblacional, servicio, grupo etario, sexo, área de trabajo, tipo de resultado o algún otro criterio que el laboratorio considere necesario. En caso de no contar con una estadística puntual, la misma puede ser solicitada al Proveedor de la Solución según los parámetros que el Laboratorio necesite.

Este sistema deberá contar con un registro de peticiones, talón de recepción y código de barras, hojas de trabajo, registro de peticiones diarias y previas, registro de historias clínicas, estadísticas y

posibilidad de conexión on-line a tiempo real vía a un software de gestión de muestras en la etapa preanalítica. El sistema deberá permitir realizar una auditoría completa del sistema de gestión por un supervisor en tiempo real.

El sistema deberá permitir dividir los circuitos del Laboratorio en, al menos, las siguientes etapas: origen de las peticiones, recepción y procesamiento de las peticiones, análisis, control, validación y entrega de informes.

13) Informes

a) La impresión de informes podrá realizarse en bloque o a demanda, incluyendo la firma del personal responsable de cada área interviniente. Las reimpresiones (copias) de informes sólo podrá realizarse si se cuenta con permisos especiales a tal fin.

b) Los informes podrán incorporar gráficos (por ejemplo, corrida electroforética, evolución de resultados anteriores, curvas de glucemia, etc.), a petición del usuario al momento de validar los resultados.

c) La impresión de informes podrá ser parcial o total según la necesidad del usuario, y en el caso de envío automático de resultados por correo electrónico, se podrá establecer que se envíen conforme se vayan completando los resultados.

d) A efectos de facilitar las tareas administrativo-contables de la institución, el sistema deberá poder exportar los datos de cada una de las secciones, por paciente, por grupo de pacientes, por sexo y otros, a formato Excel, csv u otro formato estándar.

e) El sistema deberá permitir la solicitud de informes epidemiológicos, demográficos y estadísticos según necesidades especiales de la institución.

f) Debe permitir en todos los informes la clasificación y búsqueda de acuerdo a: origen, servicio, unidad y médico.

g) Deberá permitir el envío de informes (resultados) por correo electrónico, en forma automática conforme lo configurado al recibir al paciente o preestablecido por médico u origen del paciente.

h) El sistema debe poder generar al final del proceso analítico un informe en formato PDF, que quede resguardado de cualquier tipo de cambio. En el caso de tener que generar más de un documento por entrega de parciales o correcciones, el sistema debe mantener todas las versiones del informe que se hayan generado.

i) El sistema debe contar con un sistema de Envío de Alertas automático por Mail para uso interno, cuyo uso en caso de ser requerido esté a disposición del Laboratorio para un grupo demográfico específico (ej. VDRL Positivas para Embarazadas, BACILOSCOPIA DIRECTA - ZIEHL NEELSEN POSITIVA)

14) El sistema debe contar con un módulo de indicadores de gestión relativa a la producción del laboratorio, la calidad de atención y la calidad de los resultados obtenidos. El sistema debe contar con la posibilidad de configurar Informes Automáticos por Correo Electrónico con el fin de establecer una dirección para enviar los resúmenes mensuales de forma automática.

15) El sistema debe permitir niveles de acceso definibles por un supervisor / administrador y contar con la posibilidad de configurar diferentes perfiles de usuarios. La seguridad del sistema, en base a perfiles de usuario, restringirá no solo a las pantallas sino también a las acciones relevantes de cada pantalla (consultar o modificar información, validar, rechazar, repetir, modificar estados, imprimir, etc.).

16) Deberá contar con un sistema de mensajería interno (no dependiente de Internet), para el aviso efectivo de situaciones particulares de un paciente (por ejemplo, solicitar nueva muestra, recitar al paciente, comunicarse con el médico, etc.) entre miembros del Laboratorio.
17) Deberá poseer un módulo de resguardo y permitir almacenar la información de forma manual o automática en diferentes medios de almacenamiento externos. El sistema deberá permitir hacer un backup de los resultados de manera sencilla y asegurar el resguardo de los mismos para poder realizar una copia en cualquier momento. El sistema deberá asegurar que los mismos no se perderán y se podrá acceder a ellos por al menos un período de 10 años.
18) El sistema deberá contar con un módulo específico para el laboratorio de guardia, que facilite la operación de todas las áreas desde un solo puesto de trabajo.
19) El sistema deberá contar con una base de datos abierta que permita la generación de reportes desde otras aplicaciones, con la debida autorización de laboratorio

DEL HARDWARE:

- Todos los analizadores y computadoras ofrecidos deberán ser provistos con UPS adecuadas, para evitar que haya posibilidad de daño a los mismos, deslindando responsabilidades por parte del Hospital, y previniendo así la pérdida de reactivos que
se estén utilizando en las corridas que están en proceso cuando se produzcan cortes del suministro eléctrico. Dichas UPS deberán estar sometidas a un mantenimiento preventivo y/o reposición por parte del proveedor del instrumento cuando su mal funcionamiento así lo requiera, sin gasto para el Laboratorio ni el Hospital.
Todas las computadoras deberán contar con el cableado de red desde el Laboratorio a las estaciones de trabajo
La firma oferente deberá proveer en calidad de comodato impresoras de código de barra con conexión USB a la red de laboratorio para cada Hospital. En el Hospital Santa María se deberán instalar 1 impresora de código de barras, 4 en el Hospital San Miguel Arcángel y 5 en el Hospital Larcade.
La firma oferente deberá proveer en calidad de comodato impresoras TIPO láser con conexión USB a la red de laboratorio para cada Hospital. En el Hospital Santa María se deberán instalar 4 impresoras, 6 en el Hospital San Miguel Arcángel y 8 en el Hospital Larcade.
Las impresoras deberán contar con el cableado de red desde el Laboratorio a las estaciones de trabajo con sus respectivas computadoras.
La Empresa proveedora será responsable de la realización del cableado entre el rack y los instrumentos y/o PCs según lo requiera el software de gestión, deberá ser patrimonio del Hospital una vez finalizada la licitación, dejando claramente constancia en la oferta. El cableado existente actualmente puede ser utilizado.

El server deberá ser de alguna de las siguientes características (tipo) o superior, acorde al buen funcionamiento del sistema de gestión del laboratorio:

Server: SR650/ 2U RACK / PROC SILVER 2 X8C/ 256GB RAM/ RAIDK 730 8I + 8 HDD 1,92TB SSD+ MIRRORING KIT 2X 1TB SSD / LOM 4 X 10GB BASE T + 4 PORT PCIE 10GB BASE T/ 2 X 750W/ WTY 3 AÑOS 7X 24 +YDYD / XCLARITY ENT/ XCLARITY PRO/ W. SVR STD 2019/+ HBA FC DUAL 16GB.

7X06CTO1WW - Server: ThinkSystem SR650 - 3yr Warranty
B4HT Intel Xeon Silver 4208 8C 85W 2.1GHz Processor - 2
B4H3 ThinkSystem 32GB TruDDR4 2933MHz (2Rx4 1.2V) RDIMM - 8
B4RQ ThinkSystem RAID 730-8i 2GB Flash PCIe 12Gb Adapter - 1
BQ1X ThinkSystem 2.5" 5400 PRO 1.92TB Read Intensive SATA 6Gb HS SSD - 8
AUMV ThinkSystem M.2 with Mirroring Enablement Kit - 1
WDS100T3B0B 1T WD SSD BLUE3D M.2 2280 SATA III - 2
B4PB ThinkSystem SR650 x16/x8/x16 PCIE Riser1- 1
AUKM ThinkSystem 10Gb 4-port Base-T LOM - 1
ATZV Emulex 16Gb Gen6 FC Dual-port HBA - 1
BMXB ThinkSystem Intel X710-T4L 10GBase-T 4-Port PCIe Ethernet Adapter - 1
AVWD ThinkSystem 750W(230/115V) Platinum Hot-Swap Power Supply - 2
6400 2.8m, 13A/100-250V, C13 to C14 Jumper Cord - 2
AUPW ThinkSystem XClarity Controller Standard to Enterprise Upgrade - 1
AXCA ThinkSystem Toolless Slide Rail - 1
5PS7A01558 Essential Service - 3Yr 24x7 4Hr Resp + YDYD SR650 - 1
7S05CTO3WW - Windows Server 2019 Standard (16 core) - MultiLang (not preinstalled)
5641PX3 - Lenovo XClarity Pro, Per Managed Endpoint w/3 Yr SW S&S- 1

MANTENIMIENTO Y SOPORTE TÉCNICO

El OFERENTE deberá hacerse cargo del servicio de mantenimiento preventivo y correctivo de la aplicación y sus componentes durante el período del contrato que incluya el desarrollo de adaptaciones particulares para el laboratorio, no pudiendo ofertarse software "enlatados" sin posibilidad de modificaciones.
La empresa responsable del software debe ser capaz de realizar per se las modificaciones necesarias sobre el mismo, incluyendo tareas de programación, para adaptarlo especialmente a las necesidades del laboratorio en tiempos razonables, (plazo máximo 3 meses).

1. Mantenimiento de Hardware
   a. Mantenimiento preventivo incluye una revisión periódica detallada del correcto funcionamiento de los equipos de hardware en todos sus componentes y estos serán pactados en entre JEFATURA del LABORATORIO y el PROVEEDOR.
   b. Mantenimiento correctivo incluye el costo de la mano de obra en la sustitución de los componentes tanto internos como externos que fallaran en los equipos.
   c. Incluye la instalación de otros dispositivos adicionales para la mejora del rendimiento operativo en general y de seguridad.

2. Mantenimiento de Software
   a. Mantenimiento preventivo del software instalado que incluye la revisión de los parámetros críticos de los equipos y de la red. Actualizaciones del sistema. Instalación y mantenimiento del sistema de copias de seguridad.
   b. Mantenimiento correctivo que incluye la reinstalación de software en el caso de anomalías en el funcionamiento. Recuperación de datos de copias de seguridad en caso de pérdidas de los mismos.
   c. Configuración del software ya instalado.
   d. Actualización e instalación de software adicional con licencia. Incluyéndose aquí tanto las actualizaciones del Sistema Operativo como aquellas de las diferentes aplicaciones instaladas en cada equipo.

3. Mantenimiento de Red
   a. Incluye mantenimiento de RED la configuración y optimización para el correcto funcionamiento de la comunicación entre los equipos y periféricos conectados en RED, solo incluye de los tramos de red de laboratorio; para cualquier modificación y/o corrección se debe comunicar previamente al LABORATORIO por cualquiera de las vías de contacto oportunamente informadas.

4. Los servicios se prestarán en la sede del Laboratorio, servicio presencial, y en todos los componentes de sus sistemas informáticos, en horario de 8:00 a 17:00 horas (pudiendo realizarse en otros horarios cuando fuere necesario) para realizar tareas de mantenimiento que requieran la presencia del personal técnico.

5. El OFERENTE monitorizará los sistemas principales: Servidores y componentes de la solución, Actualizaciones de todos los equipos, Antivirus y Copias de Seguridad de forma periódica de forma remota para alertar de cualquier situación.

6. El OFERENTE se obliga a prestar los servicios necesarios para el correcto funcionamiento del sistema informático del Laboratorio. Dichos servicios comprenden la realización de cuantas operaciones sean necesarias para el correcto funcionamiento de los equipos o sistemas incluidos en este contrato, siempre que no se deban a manipulaciones indebidas.

7. El OFERENTE ofrecerá un servicio de asistencia técnica en horario continuo donde se notificarán las incidencias que se produzcan. Todas las Ordenes de Atención deben enviarse de forma digital, ya sean presenciales o telefónicas.

8. Los problemas se resolverán en un período máximo variable según la naturaleza de la incidencia, su gravedad y complejidad, tal y como se detalla a continuación. De cualquier forma, el OFERENTE se compromete a seguir una política de máximo esfuerzo y utilizar todos los recursos a su disposición para solucionar cualquier incidencia en el menor tiempo posible.

a. Se entiende por incidencia crítica: las incidencias que, en el marco de la prestación de los Servicios, afectan significativamente al laboratorio, impidiendo el desarrollo de su labor asistencial. Por ejemplo, un fallo total de la solución que impida o dificulte en gran medida el desarrollo normal de una jornada laboral, como un fallo en el sistema de solicitudes e informes.

b. Se entiende por incidencia grave: las incidencias que, en el marco de la prestación de los Servicios, afectan moderadamente al laboratorio, dificultando de forma importante, pero no evitando, el desarrollo de su labor asistencial. Por ejemplo, un fallo en el servicio de turnos y que impide su realización mediante procesos informáticos, debiéndose realizar, de forma temporal, manualmente.

c. Se entiende por incidencia leve: las incidencias que se limitan a entorpecer la prestación de los Servicios y que pueden ser realizados por el laboratorio por medios alternativos sin que supongan una demora importante en el flujo de trabajo habitual.

9. El tiempo de respuesta (tiempo transcurrido entre la solicitud y la primera respuesta e inicio de las tareas necesarias por parte del OFERENTE) tendrá lugar en los siguientes períodos máximos.

a. Incidencia crítica: misma jornada laboral y dentro de las 2 hr, si el aviso es antes de las 17:00, pudiendo ser al día siguiente si el aviso es posterior.

b. Incidencia grave: misma jornada laboral y dentro de las 3 hr, si el aviso es antes de las 17:00, pudiendo ser al día siguiente si el aviso es posterior.

c. Incidencia leve: dentro de las siguientes 24 horas.

10. El tiempo de respuesta no puede garantizar el tiempo de finalización de las tareas (que siempre será el menor y estrictamente necesario) ya que este dependerá, salvo negligencia por parte del OFERENTE, de la disponibilidad de repuestos necesarios y la complejidad de la problemática surgida. El OFERENTE se compromete a explicar la naturaleza de la avería, el tiempo estimado de resolución y las tareas llevadas a cabo una vez resuelto el problema.

El Soporte Informático para el LIS deberá contar al menos con un número de Teléfono de Urgencias, número de Servicio de Mensajería Instantánea de Urgencia (WhatsApp, Telegram, etc.), dirección de Correo Electrónico de Urgencia. Cada interacción con esta línea e Soporte debe completarse con un Informe Digital de Trabajo Realizado que se debe enviar por mail (preferentemente de forma automática) de forma de dejar constancia completa de la trazabilidad y correcto funcionamiento del Sistema Informático de Laboratorio (LIS).

Requisitos de Seguridad Informática que debe cumplir el oferente, su alcance es para desarrollos y equipamiento provisto que tengan conexión a la red informática del Hospital:

- **Conformidad con Estándares de Seguridad:**
    - Los desarrollos deben cumplir con estándares de seguridad reconocidos, como OWASP (Open Web Application Security Project) para aplicaciones web o SEI CERT Secure Coding para desarrollo seguro en general.
- **Autenticación y Autorización:**
    - El desarrollo debe integrarse con Active Directory para la autenticación de los usuarios que operen con el mismo
    - La autorización debe basarse en la asignación de permisos a través de grupos, donde los usuarios con necesidades de autorización similares son agrupados y los permisos se otorgan en función del grupo al que pertenecen. Se prohíbe la asignación directa de permisos a usuarios individuales. Para garantizar un control de acceso efectivo, establecer un sistema granular que permite asignar permisos específicos a los grupos, limitando el acceso únicamente a las funcionalidades necesarias para cada grupo en particular.
    - Debe caducar la sesión del usuario transcurrido un cierto tiempo

- Los desarrollos deben contar con una consola para administración de permisos y parametría
- Contar con mecanismo para el bloqueo del acceso
- Las claves de máximo privilegio (administrador) deben ser cambiadas de configuración inicial y resguardas por Seguridad Informática.
- Las aplicaciones correrán con los mínimos privilegios (modo usuario) dentro de las estaciones de trabajo.
- Las aplicaciones que corran dentro de servidores deben correr en modo servicio con sus usuarios de servicio asignado para tal fin. Se prohíbe el uso de sesiones interactivas para mantener aplicaciones corriendo.
- Los usuarios de servicio (cuentas paara aplicaciones y servicios se ejecuten en segundo plano de manera continua y sin intervención humana) deberán contar con el mínimo privilegio posible y resguardados por la Dirección Seguridad Informática.

- **Terminales de operador (HMI: Interfaz humano-maquina):**

  - No deben poseer acceso libre a Internet
  - Solo correr las aplicaciones que controlan al equipo a operar y software de seguridad necesario
  - Segregación de Funciones:
  - Evitar que un solo usuario o rol tenga acceso a todas las funciones críticas. Separar las funciones y distribuir los privilegios según roles especializados
  - De soportarlo el fabricante, contar con un AntiVirus instalado y actualizado
  - Mantener el software y firmware actualizado con las últimas correcciones de seguridad.
  - Se unirán al dominio de Active Directory. En caso que los terminales no tengan dicho soporte se debe establecer políticas locales de control de acceso que limiten el acceso solo a usuarios autorizados.

- **Gestión de Identidad y Acceso:**

  - El acceso remoto del proveedor a la infraestructura del hospital debe realizarse mediante VPN provista por la Municipalidad de San Miguel
  - Los usuarios de Active Directory serán provistos por la Municipalidad de San Miguel con la nomenclatura ya definida.

- **Protección de Datos:**

  - Debe cumplir con la Ley de Protección de Datos Personales y leyes relacionadas con el tratamiento de datos
  - En caso que se requiera el almacenamiento de claves de usuarios, las mismas deben ser almacenadas mediante una función de hash (algoritmo matemática no reversible longitud fija). Se deben emplear funciones de hash robustas como SHA-2, bcrypt, argon2
  - Para la protección de datos sensibles almacenados en la base de datos, emplear cifrado de datos. Pudiendo aplicar cifrado a nivel de columna (field-level encryption) o cifrado de bases de datos completo.
  - Empleo de técnicas de tokenización de la información a fin de proteger datos sensibles y su disociación. En lugar de almacenar el dato real, se reemplaza por un "token" único, que es un identificador sin significado real.
  - Los motores de base de datos serán gestionados por la Municipalidad de San Miguel.

- La ubicación de los datos debe ser dentro del Centro de Datos de la Municipalidad de San Miguel.

- Se debe contar con un “diccionario de datos”, indicando la descripción detallada de los datos que se almacenan en la base de datos. Debe contar al menos con:

    - Nombre del Campo o Columna
    - Descripción del Campo, Uso y Significado
    - Tipo de Dato
    - Longitud y Precisión
    - Claves Primarias y Secundarias
    - Restricciones y Reglas
    - Relaciones
    - Origen de Datos

- **Validación de Datos:**

    - Contar con mecanismos de validación de entrada para prevenir ataques de inyección (como inyección de SQL y XSS).
    - Los mecanismos de validación de entrada deben encontrarse en la parte servidora
    - Contar mecanismos de validación y filtrado de datos de entrada antes de procesarlos.

    - Contar con una adecuada gestión de errores, evitando devoluciones no controladas o respuestas predeterminadas del servidor.

- **Manejo de Sesiones y Tokens:**

    - Empleo de tokens para la gestión de sesiones.
    - La generación de tokens debe utilizar algoritmos criptográficos fuertes como JWT con HMAC, PBKDF2, ECDSA, RSA, HMAC
    - El almacenamiento de tokens del lado del cliente debe emplear cookies seguras (atributos de HttpOnly y secure). Para el lado del servidor el almacenamiento debe ser cifrado.
    - Empleo de caducidad de tokens
    - Limitar las sesiones a una activa por usuario
    - Si el token contiene información sensible, como roles o permisos, esta información debe cifrarse para evitar la exposición no autorizada. Por ejemplo, utilizando JWT, puedes cifrar ciertas secciones del token.
    - Contar con mecanismos para renovar automáticamente los tokens antes de que expiren o solicitud al usuario que renueve su sesión de forma explicita
    - Evitar la reutilización de tokens para prevenir ataques de fijación de sesión

- **Auditoria y Registro:**

    - Contar con registros de auditoría para rastrear eventos y actividades críticas.
    - Documentación de los eventos que se registran
    - El registro de auditoría debe contar con los siguientes datos:
        - Cuando realizó la acción
        - Quien realizó la acción
        - Desde donde realizó la acción
        - Que acción realizó (Alta, Baja o Modificación)
        - Sobre que elemento realizó la acción
    - Deben tener la posibilidad de retención al menos de 9 meses y rotación para evitar archivos de registros de gran volumen.

- **Actualizaciones y Parches:**

    - Los desarrollos de aplicaciones deben ser compatibles con las actualizaciones del Sistema Operativo y de software base que corre dicha aplicación.
    - Para desarrollos de aplicaciones, deben dar prioridad de remediación en base criticidad de las vulnerabilidades reportadas
    - Los desarrollos deben poseer un versionado y documentado su historial de cambios. Cada nueva versión debe estar notificado la Subsecretaría de Modernización
- **Seguridad en API:**

    - Implementar métodos de autenticación como OAuth 2, JWT, OpenID o HMAC.
        - En caso que no sea viable técnicamente los métodos anteriores, utilizar API Key definiendo su complejidad la Dirección de Seguridad Informática al igual que su resguardo
    - Definir los niveles de autorización necesarios para acceder a diferentes recursos y funcionalidades en API mediante roles y permisos.
    - Aplicar un límite de consultas por segundo, a fin de evitar que se genere un abuso de la API
    - Para la interfaz con otras aplicaciones de salud se debe utilizar el estándar de HL7 (Health Level Seven International), en preferencia HL7 FHIR (Fast Healthcare Interoperability Resources)
    - En caso de requerir utilización de API de terceros alojadas fuera del Centro de Datos de la Municipalidad de San Miguel, se debe firmar acuerdo de confidencialidad con el tercero y especificar los a intercambiar.

- **Pruebas de Seguridad:**

    - Debe presentar el informe de una prueba de seguridad realizada por un tercero o disponer del código fuente a la Dirección de Seguridad Informática para su análisis.
    - Debe presentar plan de remediación para los hallazgos de riesgo medio, alto y crítico.

- El plazo de remediación se debe ser menor al vencimiento de la prestación del servicio y acordado con la Subsecretaría de Modernización.

- **Gestión de Incidentes:**

  - Presentación de informes mensuales de los incidentes detectados antes las áreas acordadas con la Municipalidad de San Miguel.
  - Debe prestar un punto de contacto y tiempo de respuesta.

- **Transmisión de Datos:**

  - Empleo de cifrado fuerte (TLS) para la transmisión de datos entre aplicaciones, APIs y, cuando sea técnicamente posible, equipamiento provisto.
  - Los servicios expuestos hacia Internet, deben pasar por un-Proxy Inverso (también conocido como Reverso)
  - Se permite solo servicios del tipo web expuesto a Internet, otros tipos de servicios deben ser validados con la Dirección de Seguridad Informática. Además, deben contar con su respectiva documentación describiendo el servicio.

- **Correo Electrónico:**

  - Debe emplear los servidores centralizado existentes para el envío de correo
  - Para volúmenes de gran tamaño (envíos masivos) se debe integrar con el software Mautic o emplear un servicio de envío masivo con cuenta a nombre de la Municipalidad de San Miguel

- **Protección contra Malware y Amenazas Externas:**

  - Los desarrollos deben ser compatibles con el software Antivirus (ESET) utilizado por la Municipalidad de San Miguel
  - Los desarrollos deben contar la documentación del detalle de puertos (protocolo, número y flujo) necesarios para su habilitación en el Firewall de las estaciones de trabajo, servidores y red.
- **Resiliencia y Continuidad:**

  - Documentación de los componentes de la arquitectura del software de gestión que se deben realizar resguardo, como también el espacio de almacenamiento estimado requerido.
  - Los desarrollos deben ser compatibles con el software de resguardo empleado por la Municipalidad de San Miguel (Veeam Backup)
  - Documentación de la tolerancia a cortes de conexión, indisponibilidad de los componentes del software desarrollado. Indicando los pasos de recuperación, tiempos y efectos producidos por la interrupción
  - Recomendación de arquitectura redundante o de alta disponibilidad que se debe considerer

- **Acuerdo de confidencialidad:**

    - El oferente debe firmar un acuerdo de confidencialidad para proteger la información confidencial que la Municipalidad de San Miguel comparte con el oferente durante la prestación de servicio.

- **Excepciones:**

    - *De existir alguna excepción a los requerimientos mencionados por limitación técnica debe ser analizado por la Dirección de Seguridad Informática y autorizado por el Comité de Seguridad de la Información de la Municipalidad de San Miguel.*

ÍNDICE