ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICIÓN DE UNA PLATAFORMA TECNOLÓGICA DE BUS DE INTEGRACIÓN EMPRESARIAL (ESB) DE SALUD Y REPOSITORIO DE SERVICIOS (SRR), QUE HABILITE LA INTEROPERABILIDAD A NIVEL DE DATOS Y APLICACIONES Y LA IMPLEMENTACIÓN DE SOLUCIONES DE INTEGRACIÓN ENTRE LAS ENTIDADES DE LA RED PÚBLICA INTEGRADA DE SALUD (RPIS) Y EL OPERADOR LOGÍSTICO EN EL MARCO DEL DECRETO EJECUTIVO 1033 PARA LA ADQUISICIÓN DE FÁRMACOS Y BIENES ESTRATÉGICOS EN SALUD

1. OBJETIVO GENERAL

Adquirir una solución informática de hardware y software para el despliegue de la plataforma de interoperabilidad que permita el intercambio de información derivados de las prescripciones de medicamentos, así como su validación, dispensación y administración, entre el operador logístico y la Red Pública Integral de Salud - RPIS, de forma segura y confiable, mediante un Bus de Servicios Empresariales (ESB).

1.1 OBJETIVOS ESPECÍFICOS

1. Intercambiar información mediante la definición de una arquitectura de interoperabilidad para el Ministerio de Salud que cumpla con la normativa técnica de Interoperabilidad Gubernamental.

2. Levantar las necesidades técnicas del diseño de la arquitectura de interoperabilidad y la implementación del Bus de Servicios Empresariales, haciendo énfasis: Interoperabilidad Operativa, Interoperabilidad Semántica e Interoperabilidad Tecnológica para el cumplimiento del decreto No. 1033.

3. Implementar una solución de hardware y software de interoperabilidad dentro del MSP para el intercambio de datos entre el operador logístico y la RPIS, de acuerdo a los lineamientos establecidos en conjunto con la RPIS.

4. Realizar el acompañamiento en la integración de los subsistemas de la RPIS (ISSFA, ISSPOL, IESS, MSP) y Operador Logístico, involucrados en el proceso de suministro de medicamentos del Decreto 1033.

5. Contar con los recursos de procesamiento, almacenamiento, memoria RAM suficientes, para el funcionamiento del Bus de Interoperabilidad de Salud,

6. Capacitar al personal técnico del MSP en la instalación, configuración, implementación, administración y el desarrollo de nuevos componentes de la solución de interoperabilidad.

7. Contar con un partner certificado para el soporte técnico especializado y mantenimiento de la solución durante el tiempo de ejecución del contrato.

2. ALCANCE

Alineados con la iniciativa de la Agenda Digital en Salud y como parte del proyecto de articulación de las compras públicas del sector, se necesita adquirir el **Bus de Servicios Empresariales (ESB) de Salud y los repositorios de servicios** que le permita a la RPIS compartir información de manera segura y confiable a través de una plataforma robusta, con la capacidad de escalar de acuerdo con otras necesidades futuras como la Historia Clínica Electrónica Nacional. Adicionalmente, y como parte integral de la arquitectura de interoperabilidad en salud, se necesita adquirir el componente que permitirá gestionar el Índice Nacional de Pacientes (**Master Patient Index**, por sus siglas en inglés), que garantizará la calidad en procesos de identificación unívoca de las personas en entornos de interoperabilidad. Toda la **infraestructura** requerida para la operación del intercambio de datos entre las entidades de la red pública y el operador logístico deberá ser disponibilizadas para este proyecto, para lo cual se requiere adquirir los equipos de cómputo (servidores de aplicación, de la capa de servicios, de bases de datos y back end, sistemas de balanceo, solución de hardware de respaldos) para los ambientes de Desarrollo, pruebas y producción. Todos los servicios asociados a la instalación y puesta en funcionamiento de la infraestructura así como los **servicios profesionales** requeridos para la implementación de los casos de uso detallados en los requerimientos funcionales de este documento, son requeridos para lograr el objetivo de la interoperabilidad de los actores involucrados en el proceso de compras públicas del sector salud, su distribución, almacenamiento y entrega de fármacos y bienes estratégicos

3. DESCRIPCIÓN DEL BIEN O SERVICIO

3.1 SERVICIOS DE IMPLEMENTACIÓN

- El MSP dispondrá de un equipo de trabajo definido en la estructura de Gobierno del proyecto, dicho equipo de trabajo realizará las actividades de seguimiento y supervisión según se acuerde con el proveedor.

- El equipo de trabajo del MSP realizará las siguientes acciones:

  - Vigilar el cumplimiento de cronogramas, entregables, ANS y calidad de las actividades y entregables definidos en la oferta presentada por el proveedor.
  - Revisar y aprobar los entregables del proveedor definidos en la propuesta.
  - Velar por el cumplimiento de los compromisos por parte del MSP que sean definidos durante el proyecto.

- El proveedor deberá cumplir con las medidas, normas y/o lineamientos existentes en el MSP en cuanto a calidad, seguridad, mejores prácticas, arquitectura, marco regulatorio y las demás especificadas en este documento.

- Es potestad del MSP componer el equipo anteriormente mencionado por personal interno o externos que sean contratados para tales fines si así lo requiriera.

- El proveedor deberá integrar un equipo de trabajo con mínimo los roles definidos en el capítulo 6.7 de este documento. Las personas que desempeñen estos roles deben hablar español y poder desplazarse a Ecuador durante el tiempo o las veces que el plan de implementación entregado por el proveedor lo defina.

- El proveedor dentro de su modelo de gestión deberá incluir informes periódicos de avance y seguimiento en un formato acordado con el MSP.

- El seguimiento del proyecto se deberá realizar en conjunto entre las partes, con los roles definidos en el plan del proyecto. En estos seguimientos se evaluará el cumplimiento de cronograma, actividades, calidad en los entregables, ANS definidos, problemas y riesgos que deban ser gestionados y resueltos, para dar aval o rechazar parcial o totalmente el entregable en cuestión.

- De estos seguimientos se deberán generar actas de control y definición de compromisos como soporte de gestión del proyecto. El proveedor deberá proporcionar la información requerida por las personas designadas por el MSP para el seguimiento y supervisión del proyecto.

- En caso de requerirse se podrán citar reuniones de seguimiento extraordinarias por parte del MSP o por parte del Proveedor para seguimientos, aclaraciones o manejo de situaciones o novedades en el desarrollo del proyecto.

- Toda la documentación de gestión del proyecto deberá almacenarse en el repositorio y con las estructuras definidas en el plan del proyecto.

- La implementación de la solución propuesta deberá estar dimensionada, a nivel de servicios de consultoría, hardware, licencias y software, para todas las funcionalidades descritas en este documento, teniendo presente que debe contarse al menos con entornos de desarrollo, calidad y producción.

- El proveedor será el responsable de gestionar el análisis, diseño y definición de los modelos y posterior implementación del ecosistema tecnológico incluyendo la puesta en producción, estabilización y tiempo de garantías correspondientes.

- La solución propuesta deberá ser capaz de cumplir con los requisitos definidos en el en el capítulo 6; para ello el proveedor deberá contemplar en su propuesta los mecanismos, productos, subproductos, licencias y tecnologías necesarios para implementar dichos requisitos. Además, la solución deberá contemplar el uso de herramientas que permitan gestionar el gobierno y la seguridad del dato y la definición clara de métricas de cumplimiento de estándares de datos que englobe métodos, protocolos, terminologías y especificaciones para la colección, intercambio, transporte, almacenamiento y recuperación de información asociada con datos clínicos, asistenciales y empresariales.

3.1.1 METODOLOGÍA DE IMPLEMENTACIÓN

La metodología de implementación que utilice el proveedor deberá adaptarse a las siguientes premisas:

- El proveedor deberá plantear la metodología de gestión de proyectos basado en su experiencia de implementación de este tipo de proyectos y en las buenas prácticas del mercado.
- Se requiere que la metodología permita Al MSP validar el avance de la solución periódicamente y adaptar sus requerimientos como consecuencia de las revisiones realizadas
- Todas las fases del proyecto deberán incluir los entregables descritos en el capítulo 6.8 del presente documento.
- El proveedor deberá incluir los siguientes frentes de trabajo:
- Gestión de proyectos (PMO) que permita la integración de todos los actores e interesados en el proyecto, considerando la gestión de riesgos e interesados.
- Gestión de Procesos que permita definir el AsIs y ToBe del modelo operativo de compras, distribución, almacenamiento y dispensación de medicamentos y bienes estratégicos por parte del Operador Logístico integrado con la RPIS.

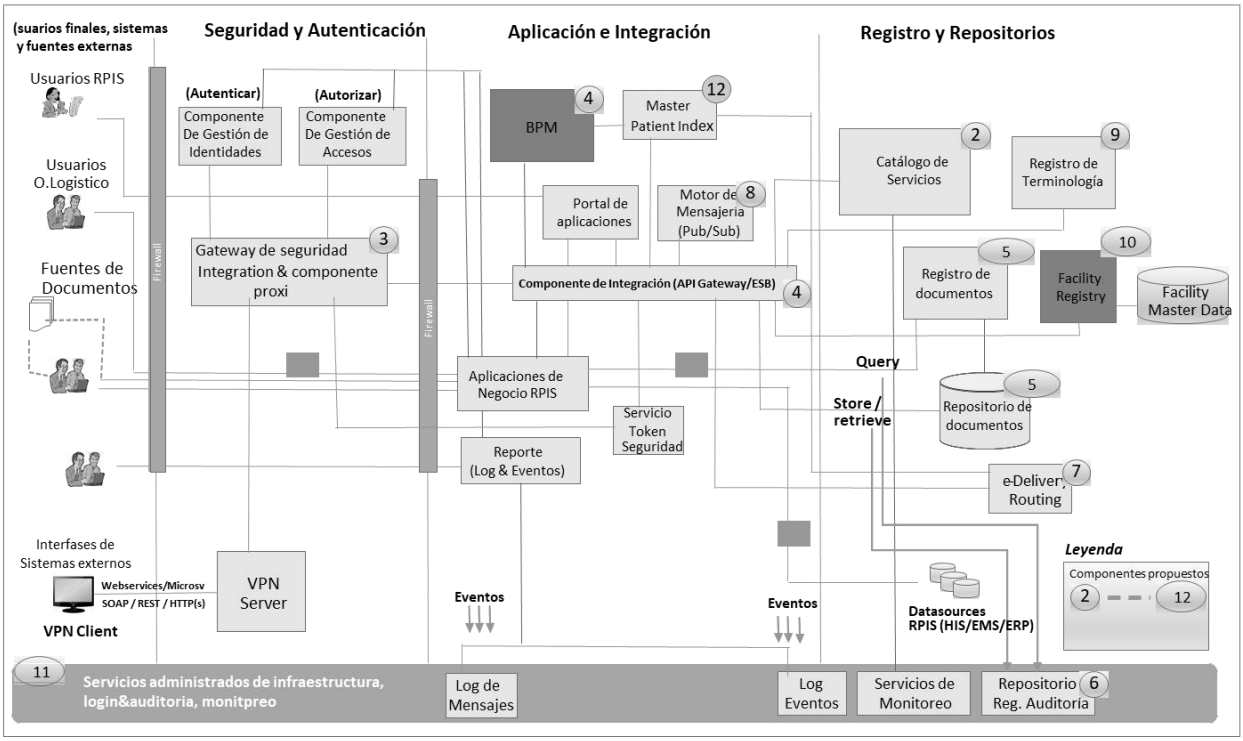
- El proveedor deberá incluir en su propuesta como fases mínimas las siguientes:
  - **Fase de Análisis:** En esta fase deberá realizar el análisis exhaustivo del estado actual, identificación y documentación de requerimientos, marco normativo, arquitectura y operación de sistemas y procesos en la organización.
  - **Fase de Implementación:** En esta fase se deberá realizar el Diseño, Desarrollo, Parametrización e Instalación de la(s) solución(es) propuestas por el proveedor, incluyendo pruebas funcionales, integrales, de carga y estrés y seguridad con todos los componentes que se definan en el plan del proyecto. Una vez se realice la instalación y puesta en marcha el proveedor deberá realizar las actividades correspondientes para la estabilización de la solución, incluyendo actividades de:
  - **Fase de Soporte:** En esta fase se deberán ejecutar los servicios correspondientes a soporte, mantenimientos (correctivo, preventivo, adaptativo y evolutivo) y la administración de la(s) solución(es) propuestas por el proveedor
  - **Fase de Entrega del Servicio**: En esta fase el proveedor deberá realizar la transferencia al MSP o a(los) tercero(s) que el MSP defina para dar continuidad a la plataforma implementada donde se incluya la transferencia de conocimiento, capacitaciones, transferencia de equipos, licencias o software en caso de que aplique, facilitando la comunicación, documentación e información correspondientes.

    Este plan de entrega no deberá impactar la prestación del servicio mientras se realiza. En el caso en que el proveedor no cumpla los requisitos de transferencia del servicio, el proveedor deberá seguir asumiendo la administración, soporte y operación de los sistemas en producción sin coste alguno para el MSP.

3.2 REQUERIMIENTOS TÉCNICOS Y FUNCIONALES

Los requisitos del sistema de integración de la RPIS con el operador logístico están organizados en torno a la arquitectura conceptual de integración representada en el siguiente gráfico:

Arquitectura de Integración



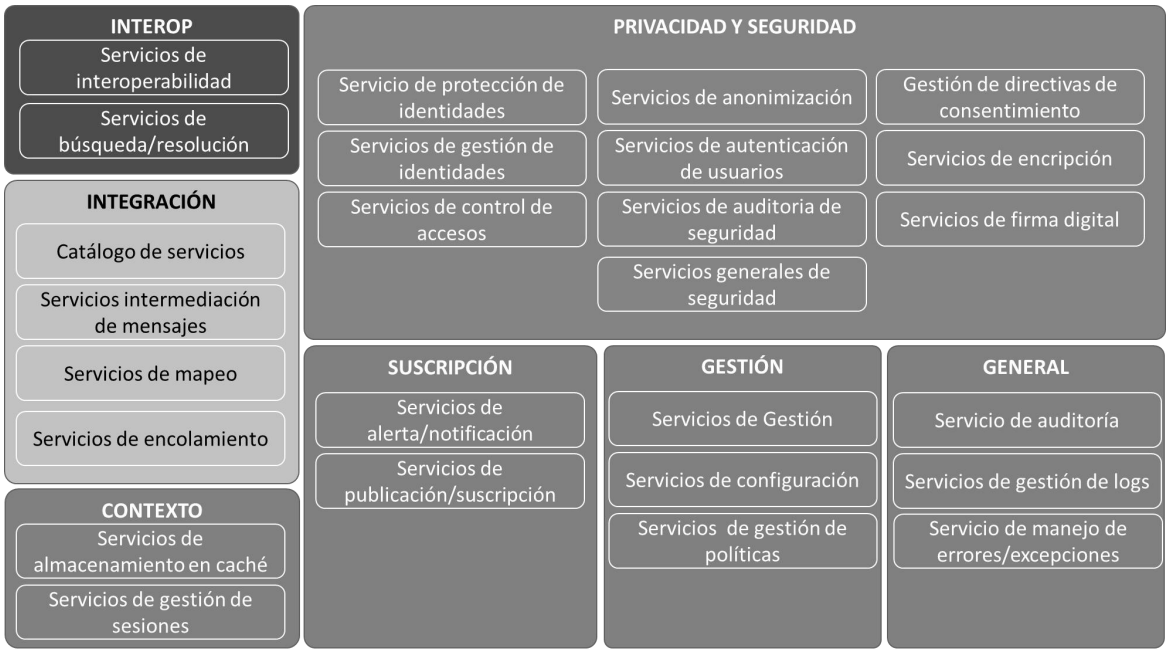
Si bien la arquitectura es conceptual, proporciona una base de comprensión de las capacidades deseadas organizadas por una descripción conceptual de los componentes de la solución, que describimos a continuación:

Número y nombre del componente	**Breve descripción y referencia cruzada a la sección que proporciona detalles específicos de implementación**
(2) Registro y repositorio de servicios empresariales (catálogo de servicios)	Este componente proporciona capacidades que respaldan la gestión del ciclo de vida del servicio (SOA) para varias fases, como modelar, ensamblar, implementar y administrar. Proporciona visibilidad y gobernanza del servicio de diseño y tiempo de ejecución y servidores como un registro y repositorio empresarial de servicios.
(3) Componente de puerta de enlace de seguridad, integración y proxy inverso	Este componente sirve como puerta de enlace de servicios web y proporciona servicios de seguridad e integración en el perímetro de la organización. Proporciona gestión centralizada de políticas y niveles de servicio para el cumplimiento de las políticas de la organización. Este componente interactúa con los componentes de gestión de acceso e identidad para proporcionar capacidades de autenticación, autorización y auditoría para el tráfico de servicios web.
(4) Componente de integración de servicios (ESB) (4) Gestión de procesos comerciales	Estos componentes abordan las responsabilidades principales de los aspectos de integración y orquestación de servicios. El componente de integración de servicios proporciona funcionalidades como la transformación de mensajes, el enriquecimiento de mensajes, la conmutación de protocolos y la invocación del punto final del servicio. La metodología y tecnología Business Process Management proporciona capacidades de orquestación de servicios.
(5) Depósito y registro de	Estos dos componentes proporcionan las capacidades para el

documentos	almacenamiento persistente de documentos, así como la capacidad de indexación para una búsqueda rápida (registro y depósito de documentos XDS).
(6) Repositorio de registros de auditoría	Este componente proporciona capacidades para proporcionar un repositorio de Audit Trail e interfaces con el repositorio según el perfil IHE ATNA y las especificaciones de transacción ITI. Este componente se utiliza para almacenar registros de eventos de auditoría.
(7) enrutamiento de entrega electrónica	Este componente proporciona capacidades para habilitar un repositorio y las interfaces de servicio correspondientes para permitir la configuración de la entrega a los proveedores de resultados de laboratorio, informes clínicos y otros contenidos para su distribución. Permite la configuración de opciones de entrega según el tipo y la naturaleza del contenido, como pacientes hospitalizados o ambulatorios, ubicaciones de servicios, función del proveedor y aspectos similares.
(8) Motor de mensajería	El componente del motor de mensajería proporciona capacidades de publicación / suscripción.
(9) Registro de terminología	Este componente proporciona las capacidades, las interfaces de usuario y de servicio para establecer un aspecto de Gestión de vocabulario.
(10) Registro de instalaciones	Este componente proporciona las capacidades para gestionar las identidades de las ubicaciones de prestación de servicios.
(11) Capa de gestión de servicios de TI	Esta capa proporciona varios componentes para agregar e informar de eventos y registros de mensajes de todo el sistema.
(12) Master Patient Index	Módulo para la gestión de la identificación única de pacientes por medio de un EMPI, Enterprise Managment Patient Index. El MPI provee un registro central de los pacientes y sus características demográficas, gestionar entradas duplicadas, localiza registros, usa mensajería de los perfiles PIX/PDQ de HIE y algoritmos determinísticos para la búsqueda de registros similares y búsquedas fonéticas.

3.2.1 PLATAFORMA DE INTEGRACIÓN

El componente de integración a contratar por el MSP debe cumplir las siguientes características mínimas, cómo muestra la siguiente gráfica y que se describen con detalle en el cuadro de requerimientos:



Se entiende que los sistemas proponentes varían y pueden proporcionar las capacidades deseadas a través de una organización diferente de componentes de la solución. Teniendo esto en cuenta, las especificaciones técnicas mínimas de los productos y servicios a adquirir se presentan a continuación. El código de autoevaluación de cada requisito debe ser uno de los siguientes y debe ir acompañado de una descripción para aclarar aún más la respuesta:

- 0: la solución no cumple el requisito.
- 1 - La solución cumple parcialmente con el requisito (califique).
- 2 - La solución se desarrollará para cumplir completamente con el requisito o se puede hacer para cumplir completamente el requisito con una personalización o una solución alternativa (describa una solución alternativa).
- 3 - La solución cumple plenamente con los requisitos.

ID	Descripción del requisito
Registro de servicios (Service Registry – SR) La arquitectura conceptual presentada en el punto anterior describe el registro de servicios (SR) como el componente que alberga metadatos de servicios para consumidores, proveedores, definiciones de servicios y políticas de servicios. Esta subsección está destinada a recopilar detalles específicos de los proponentes sobre el componente de su solución que cumple con los requisitos para un registro de servicios.	
SVR-001	La solución debe permitir la administración de servicios y suscripciones de consumidores, para gestionar análisis de impacto, versionado, acuerdos de nivel de servicio (SLA), utilizando el registro de servicios de acuerdo con los procesos de gobierno, ciclos de vida y mejores prácticas de SOA.
SVR-002	La solución debe proporcionar un diseño de SR (interfaz de usuario) y metadatos que facilite la administración, el control de versiones, la navegación, las políticas de administración de registros para los servicios, la aplicación de políticas y el análisis de dependencia en diferentes artefactos de servicio como esquemas de servicio, políticas de servicio.

SVR-003	La solución debe publicar los servicios existentes y los nuevos, los artefactos de soporte y las suscripciones de servicios al consumidor en el registro de servicios para que puedan ser consumidos y se facilite su búsqueda a nivel interno y externo
SVR-004	La solución debe crear y gestionar múltiples clasificaciones / taxonomías (por ejemplo, por usuario, por rol, por dominio clínico, por lista alfabética) y categorizar los servicios / consumidores en consecuencia en el SR para facilitar su búsqueda y la integración del servicio con otras componentes
SVR-005	La solución debe permitir cambios compatibles con versiones anteriores en un servicio al tiempo que conserva el nombre del servicio original y el end-point del proveedor (esto implica que no se requieren cambios en el lado del consumidor)
SVR-006	La solución debe configurar el SR, la generación de informes y la gestión de políticas para utilizar los servicios de gestión de acceso y gestión de identidades del MSP (Microsoft Active Directory) para la autorización de actividades relacionadas con la arquitectura orientada a servicios
SVR-007	La solución debe proporcionar integración entre el SR y la componente de supervisión / monitoreo del servicio. Los ejemplos de dicha integración incluyen: Los parámetros de supervisión del servicio (requisitos no funcionales, niveles de servicio) capturados en el SR que deben reflejarse / propagarse en el monitoreo del servicio en los estados correctos del ciclo de vida.
SVR-008	La solución debe administrar múltiples versiones de servicio y artefactos de acuerdo con las pautas de control de versiones.
SVR-009	La solución debe proporcionar vistas web seguras basadas en roles y paneles de control del SR. Las vistas y los datos mostrados deben adherirse a los perfiles de servicio definidos por el MSP.
SVR-010	La solución debe utilizar la gestión de acceso e identidad empresarial del MSP, así como cualquier control de acceso adicional disponible dentro del producto, para controlar el acceso y la gestión del SR, la gestión y supervisión de políticas.
SVR-011	La solución debe implementar el servicio y los ciclos de vida de los artefactos de soporte para respaldar los procesos / flujos de trabajo de gobierno de SOA, incluida: ● La aprobación y el registro de nuevos servicios y de la versión actualizada del servicio, ● La desactivación o el retiro del servicio ● Activación / desactivación del “end-point” del servicio ● Actualización y aprobación de la versión de la política ● Desaprobación de políticas ● Asociación de políticas / conjuntos de políticas con los servicios y la aprobación ● La aprobación y el registro de nuevas suscripciones de consumidores a los servicios ● La aprobación del servicio / suscripción y la promoción al siguiente entorno (proceso de promoción configurable para desencadenar la promoción de artefactos de servicio en el entorno destino, en función de la transición del ciclo de vida) ● El registro y la aprobación de nuevos esquemas estándar (aprobaciones y especificaciones de esquema) ● Creación y aprobación de nuevas políticas
SVR-012	La solución debe proporcionar integración entre la supervisión /monitoreo del servicio y la administración de políticas.

SVR-013	La solución debe proporcionar integración entre los puntos de mediación y supervisión /monitoreo del servicio.
SVR-014	La solución debe proporcionar integración entre el SR y la administración de políticas.
SVR-015	La solución debe proporcionar búsquedas configuradas de artefactos de servicio por metadatos (por ejemplo, todos los medicamentos prescritos, todas las órdenes pendientes, órdenes con dispensación parcial, así como los SLA.) para respaldar las actividades del usuario final y las necesidades de integración del sistema.
SVR-016	La solución debe proporcionar una interfaz de usuario para respaldar los flujos de trabajo del ciclo de vida del servicio (por ejemplo, el proceso de registro y aprobación) restringido a roles autorizados.
SVR-017	La solución debe proporcionar notificación sobre eventos del ciclo de vida (por ejemplo, nueva versión planificada, nuevo servicio identificado.) a los clientes / sistemas suscritos
SVR-018	La solución debe admitir la capacidad de analizar el impacto de los cambios en los artefactos del servicio y notificar a los clientes afectados por los cambios.
SVR-019	La solución debe admitir la ejecución de varias versiones de servicio simultáneas.
SVR-020	La solución debe proporcionar herramientas de gobierno SOA (p. Ej., SR, gestión de políticas, supervisión e informes), vistas e integración de procesos.
SVR-021	La solución debe indicar discrepancias entre los servicios capturados por la solución de monitoreo y los servicios registrados para alertar sobre intentos de activación en servicios inesperados, no registrados, inactivos o no aprobados. El SR puede simplemente poner sus metadatos a disposición de una solución de monitoreo o también puede actuar como la solución de tiempo de ejecución que alerta sobre la discrepancia.
SVR-022	La solución debe ser capaz de importar / exportar servicios o atributos registrados en XML u otros formatos "abiertos" / editables (por ejemplo, WSDL, XSD, AML o JSON)
SVR-023	La solución debe proporcionar integración de SR con herramientas de desarrollo (por ejemplo, un desarrollador de sistema de punto de venta/dispensación que accede al registro para identificar una descripción de servicio)
Gestión de seguridad, privacidad y servicios La arquitectura conceptual presentada, describe una capa de gestión de servicios, que se puede implementar en una DMZ, responsable en gran medida de la aplicación de políticas en torno a la autenticación, autorización y auditoría. Esta subsección busca que los proponentes describan los componentes de su solución que cumplen esos requisitos. Proporcione detalles sobre el componente o los componentes específicos de la solución que cumplen con los requisitos de administración de servicios y los protocolos de comunicación entrantes y salientes que son compatibles.	
SEC-001	La solución debe incluir un componente de capa de seguridad / gestión de servicios que se pueda implementar en un área de red / DMZ de acceso público y que pueda actuar como un proxy para los servicios de integración o interfaz que no son de acceso público.
SEC-002	La solución debe poder asociar un identificador único a cualquier mensaje en el punto de recepción (es decir, en el proxy de gestión de servicios) y asociarlo a cualquier otro mensaje que resulte del mensaje original que recibe el sistema, incluidos los mensajes de respuesta a través de la integración para la correlación de mensajes. / fines de registro.

SEC-003	La solución debe poder garantizar la seguridad de los mensajes entrantes o salientes utilizando la autenticación de cliente o servidor TLS a través de múltiples protocolos, incluidos MLLP, TCP, HTTPS, SOAP, FTP, SMTP, Syslog y poder comportarse como TLS punto de terminación para conexiones entrantes.
SEC-004	La solución debe poder registrar mensajes completos, sin cambios (con validación de integridad) al aceptar el mensaje en el sistema de integración, mediante una firma digital XML que se genere en el contenido de un mensaje SOAP.
SEC-005	La solución debe tener capacidades de firewalls XML que permitan asegurar el intercambio de mensajes de carga útil XML. Con el fin de evitar inyección de código malicioso o datos con formatos de entrada no válidos.
SEC-006	La solución debe ser compatible con el protocolo ICAP ((Internet Content Adaptation Protocol) usado para transportar mensajes HTTP entre el proxy y los dispositivos que proporcionan soporte antimalware, de tal manera que se puedan filtrar cualquier mensaje SOAP malicioso tan pronto como llegue a la DMZ de la red donde se implementa la plataforma para reforzar la seguridad de los servicios web detrás de un firewall IP existente.
SEC-007	Contar con mecanismos de definición, implementación y seguimiento de políticas de seguridad mediante un módulo de gestión.
SEC-008	El componente de soluciones debe admitir WS-Addressing para el enrutamiento de mensajes y la identificación coherente de los puntos finales – “end points” de los sistemas de consumo.
SEC-009	La solución debe validar firmas digitales a través de mecanismos que cumplan con las normativas de Firma electrónica en el Ecuador (Acuerdo Ministerial 0084 del 13 de noviembre del 2020) o vigentes.
SEC-010	La solución debe admitir la integración con la gestión de acceso e identidad del MSP para la autenticación y autorización de solicitudes de servicio.
SEC-011	La solución debe utilizar la gestión de acceso e identidad empresarial del MSP para controlar el acceso basado en roles y la gestión de la solución.
SEC-012	La solución debe ser capaz de admitir la autenticación y autorización del sistema externo, utilizando certificados digitales para validar que un sistema tiene la autorización necesaria para realizar la solicitud.
SEC-013	La solución debe seguir el patrón de seguridad específico del cliente para transacciones de Protocolo de capa inferior mínima (MLLP)
SEC-014	Debe permitir la definición de los atributos a validar por el esquema SAML
SEC-015	La solución debe admitir grupos de directorios anidados (grupos dentro de grupos) para fines de autorización.
SEC-016	La solución debe permitir diferentes autenticaciones, autorizaciones y registros de servicios dependiendo de si el servicio (por ejemplo, proveedor MPI) es llamado por un sistema interno (MSP-RPIS) o un sistema externo
SEC-017	La solución debe admitir el uso de control de acceso basado en roles para asegurar todas las funciones administrativas de del MSP - RPIS
SEC-018	Los registros de la solución deben ser seguros, tener su acceso controlado por reglas de autorización y tener acceso a la auditoría de ellos. Se debe garantizar la disponibilidad, integridad y confidencialidad de los registros.
SEC-019	La solución debe poder conservar / capturar la dirección IP y el nombre distinguido de la conexión entrante para el procesamiento descendente (por ejemplo, insertar en el encabezado HTTP descendente, registro, datos transitorios)
SEC-020	La solución debe implementar controles para evitar que se oculten los cambios

	realizados en la plataforma del MSP. Los controles deberían estar alineados a lo planteado y adicional responder a un análisis producto de un modelado de amenazas
SEC-021	La solución debe diseñarse para defenderse de ataques comunes, incluidos, denegación de servicio, secuestro de sesión, manipulación de URL y desbordamiento de búfer, utilizando mecanismos de protección de infraestructura estándar disponibles en el MSP (SEC-043). Incluir salvaguardas para los riesgos identificados mediante un modelado de amenazas, puede ser con método STRIDE o cualquier otro. Adicional considerar lo referente a SOA aplicables desde MITRE CWE TOP 25 y OWASP TOP 10 2017
SEC-022	El diseño de la solución debe utilizar controles de acceso a la red adecuados (como firewalls) para controlar el tráfico de la red, y los campos de datos del usuario deben usar la validación de datos para evitar la entrada de datos no conocidos y los ataques de manipulación de URL o de inyección en las peticiones.
SEC-023	La solución debe garantizar que todos los eventos relacionados con la privacidad y la seguridad se registren para respaldar la investigación en profundidad de los incidentes de privacidad y seguridad en la solución a nivel de software, componentes de red, bases de datos, sistemas operativos, sistemas de archivos, repositorios (en todos los componentes que incluya la solución).
SEC-024	La solución debe tratar los datos del Registro de pacientes como privados y seguros.
SEC-025	La solución debe tratar todos los datos del Registro de proveedores (PR) / Operador logístico como información personal, excepto los datos de ubicación y organización
SEC-026	La solución debe garantizar que ninguna información personal o de salud se recopile, use, divulgue o retenga de manera inapropiada durante el procesamiento de cualquier transacción a través de diversos medios, como la autenticación de usuario y la administración de acceso de identidad, registro / monitoreo y otras salvaguardas y controles de privacidad facilitados por la solución
SEC-027	La solución debe cumplir con la legislación de privacidad relevante según el marco normativo legal vigente
SEC-028	La solución debe garantizar que todos los datos personales y de salud que se utilizan, acceden, divulgan, transmiten, almacenan o intercambian por oa través de la solución sean accesibles solo por personas autorizadas o sistemas de confianza.
SEC-029	El almacenamiento en caché de todos los datos en la solución debe implementar controles de privacidad respetando confidencialidad, integridad y disponibilidad. Estos controles deben, como mínimo, restringir el acceso a información personal y de salud en el caché, así como garantizar que los datos del caché se almacenen, retengan y utilicen estrictamente para propósitos apropiados y consistentes y luego se purgan. en consecuencia
SEC-030	La solución debe garantizar la privacidad y seguridad de los datos personales y de salud en reposo, en uso y en tránsito.
SEC-031	La solución debe garantizar que las funciones de seguridad sensibles estén segregadas de otras operaciones y funciones de administración del sistema.
SEC-032	Los criterios de selección de búsqueda deben admitir cualquiera de los campos de metadatos asociados con mensajes como fecha / hora, tema, cola, componente, identificador de transacción y otros valores específicos del contexto del servicio.

SEC-033	Para proteger la privacidad de los pacientes, la solución debe garantizar que los informes de estadísticas de uso no muestren ninguna información personal o de salud
SEC-034	La solución debe cumplir con los requisitos de seguridad de ATNA (Audit Trail and Node Authentication), incluida la implementación de la autenticación mutua TLS, las versiones mínimas de TLS, los conjuntos de cifrado referenciados y el soporte de pistas de auditoría siguiendo los protocolos especificados por ATNA, el formato y el contenido del registro de auditoría.
SEC-035	La solución debe actuar en el rol de nodo seguro Nota: El actor de nodo seguro asegura que todas las transacciones que involucran el sistema físico que representa el nodo seguro se realizan de forma segura y solo con otros nodos de confianza en la red. La función de nodo seguro casi siempre se agrupa con otros actores para permitir un registro seguro, ya que el nodo seguro garantiza que todas las transacciones de documentos de registro y consultas se realicen de forma segura con solo sistemas confiables en la red)
SEC-036	La solución debe admitir la transacción Authenticate Node, que es el proceso de autenticación mutua del cliente y del servicio mediante certificados X.509.
SEC-037	La solución debe poder utilizar el protocolo Transport Layer Security (TLS) para cifrar los datos que se intercambian a través de una red insegura.
SEC-038	La solución debe poder proporcionar controles de acceso razonables (es decir, autenticación y autorización del usuario)
SEC-039	La solución debe ser responsable de proporcionar registros de auditoría de seguridad para rastrear eventos de seguridad.
SEC-040	La solución debe poder generar eventos de auditoría y transmitir esos eventos de auditoría a un Repositorio de registros de auditoría. Los eventos de auditoría son necesarios cuando la aplicación importa, exporta o consulta información médica o sensible protegida.
SEC-41	La arquitectura propuesta deberá contemplar en su capa de seguridad, como mínimo: ● Protocolos de IAM: LDAP, Active Directory, OpenSSO, OpenID, OAuth2, SAML2, SCIM, soporte de autenticación multi-option y multi-factor ● Datos en tránsito: TLS 1.2, EDH (intercambio), RSA 2048 (firmas), AES 256 (cifrado), entidad certificadora válida (certificados tipo extended) ● Datos en reposo: Diffie Hellman, RSA 2048 bits, AES 256, SHA2 de 256.
SEC-42	La solución debe tener la capacidad de procesar autorizaciones de APIs a través del protocolo OAuth 2.0.
SEC-43	Adicional a los requerimientos anteriores, la solución deberá estar alineada al 100% al Estándar de seguridad de la información para adquisición, desarrollo y mantenimiento de sistemas de información, elaborado por la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública (DNTIC-MSP) con el siguiente detalle: **Autenticación** a. Todas las peticiones a los sistemas deben pasar por un formulario de autenticación, y éste no debe ser evitado. b. No deben tener URLs de acceso directo, sin pasar por una autenticación. c. Todas las páginas que contengan información cargada dinámicamente catalogada como sensible, deben cumplir con el requisito de autenticación. d. Las credenciales de autenticación (o cualquier información

sensible), se las deben pasar únicamente a través de HTTP POST y nunca con GET.

e. Las páginas para la que se descarte el mecanismo de autenticación debe ser revisada para asegurarse de que no tiene brechas de seguridad.
f. Las credenciales de autenticación no deben ser enviadas en un archivo plano, sino debe ser cifradas.
g. No deben existir “puertas traseras” en el código en producción que permitan evitar la autentificación.

Autorización

a. Los sistemas de información deben tener mecanismos de autorización (control de acceso, gestión de roles y módulo de administración).
b. Los sistemas de información deben tener claramente definidos los tipos de usuario y sus privilegios.
c. Los mecanismos de autorización deben asignar los mínimos privilegios necesarios.
d. Los mecanismos de autorización no deben poder evitarse.
e. Todas las operaciones que se realizan en un sistema deben pasar por un proceso de autorización.
f. No deben existir “puertas traseras” en el código en producción que permitan escalar privilegios.

Gestión de Cookies

a. Las cookies no deben contener información sensible y de presentarse el caso, estas deben ser cifradas obligatoriamente.
b. No se debe poder realizar operaciones no autorizadas manipulando cookies.
c. Las cookies preferentemente deben ser cifradas.
d. Todas las transiciones de estados en el código de la aplicación, deben verificar el uso seguro de cookies.
e. La aplicación debe poder establecer una validación de los datos de la sesión.
f. Las cookies deben contener la mínima información privada posible.
g. Todas las cookies que usa la aplicación debe estar definidas claramente, identificando sus nombres y para qué son necesarias.
h. Todas las cookies deben tener tiempos de caducidad.

Validación de Entrada de Datos

a. Los sistemas de información deben tener mecanismos de validación de datos.
b. Las entradas que pueden ser modificadas como cabeceras HTTP, Input fields, hidden fields, drop down lists por parte de usuarios deben tener mecanismos de validación de datos.
c. Las aplicaciones deben comprobar las longitudes de los datos de todas las entradas.
d. Debe existir la validación de todos los campos, cookies, http headers/bodies y form fields.
e. Los datos de entrada deben ser formateados y deben contener solo los caracteres establecidos.
f. Los datos de entrada de ben ser validados en el servidor de aplicaciones.
g. No deben existir “puertas traseras” en el modelo de validación.

h. Toda entrada externa, sea cual sea, será examinada y validada.

Gestión de Errores / Fuga de Información

a. Todas las llamadas a métodos/funciones que devuelven un valor deben tener un control de errores y además comprobar el valor devuelto.
b. La aplicación debe gestionar adecuadamente las excepciones y los errores.
c. La aplicación no debe devolver al usuario los errores del sistema y debe manejar un log con los mismos.
d. La aplicación debe fallar de un modo seguro.
e. Los reportes con información sensible deben manejarse con autenticación de usuarios.
f. Los recursos del sistema deben ser liberados en caso de error.

Log / Auditoría

a. La aplicación no debe registrar información sensible en el log en caso de error.
b. La aplicación debe tener definido y controlado la longitud máxima de una entrada de log, de manera que vaya rotando y no sobrescribiendo.
c. La aplicación no debe registrar datos sensibles en el log como cookies, método HTTP “GET”, credenciales de autenticación.
d. La aplicación debe auditar las operaciones lanzadas desde el cliente, sobre todo la manipulación de datos: Create, Update, Delete (operaciones CUD).
e. La aplicación debe registrar en el log las operaciones de autenticaciones (fallidas o exitosas).
f. El servidor donde se aloja la aplicación debe registrar en un log de errores, los errores de la aplicación.
g. El modo de depuración (debug) no debe registrar en el log datos sensibles.
h. La aplicación debe registrar en los logs al menos la siguiente información del usuario: IP de origen, navegador, sistema operativo.

Cifrado de Datos

a. Los datos sensibles no deben ser trasmitidos en texto claro, interna o externamente.
b. La aplicación debe tener implementados métodos criptográficos.
c. Las claves deberán ser almacenadas de manera codificada, cifrada (encriptada) en la base de datos y/o en archivos de parámetros.
d. La aplicación si tiene un portal web debe funcionar en HTTPS.

Entorno de Código Seguro

a. La estructura de ficheros no debe estar directamente accesible para los usuarios.
b. La aplicación debe tener una gestión de memoria (reservar/liberar).
c. Si la aplicación usa SQL dinámico debe determinarse si es vulnerable a inyecciones de código.
d. Si la aplicación tiene funciones “main()” ejecutables deben establecerse su nivel de vulnerabilidad y depurarse “puertas traseras”.
e. La aplicación no debe tener código comentado (aunque sea para pruebas) que pueda contener información sensible.
f. Todas las bifurcaciones de código deben tener una cláusula

default (if, else, switch default, etc).

g. La aplicación no debe tener “development environment kits” en los directorios en explotación.
h. Las llamadas al sistema operativo, así como aperturas de ficheros deben contemplar un esquema de gestión en caso de error.
i. Si la aplicación usa APIs de terceros, se debe verificar que no trasmitan datos sensibles a través de la misma y que hayan sido reportadas como vulnerables.

Gestión de Sesiones (Login / Logout)

a. La aplicación debe comprobar cómo y cuándo se crean las sesiones de usuario, ya sean autenticadas o no.
b. El ID de sesión debe tener la complejidad necesaria para considerarse robusta.
c. Las sesiones deben ser almacenadas en la base de datos.
d. La aplicación debe tener un mecanismo de seguimiento de las sesiones (track sessions).
e. La aplicación debe tener mecanismos para detectar un ID de sesión inválido.
f. La aplicación debe tener mecanismos de invalidación de sesiones.
g. La aplicación debe gestionar las sesiones multithreaded/multiuser en caso de existirlas.
h. Debe estar establecido un parámetro de timeout de inactividad de la sesión HTTP.
i. La función de logout debe contemplar mecanismos robustos.

Gestión de usuarios y contraseñas

a. El módulo de administración del sistema debe permitir la gestión de usuarios y contraseñas. La depuración de usuarios debe realizarse regularmente.
b. La aplicación debe tener mecanismos de recuperación de clave robustos.
c. La aplicación debe tener mecanismos de caducidad de contraseñas.
d. La aplicación debe tener mecanismos de inactivación de usuarios.
e. Los usuarios y las contraseñas deben ser almacenados en la base de datos.
f. Las contraseñas deben ser almacenadas de manera cifrada.

Pruebas de seguridad

a. El código fuente debe ser analizado mediante herramientas de pruebas estáticas de seguridad de aplicaciones (SAST) durante todo el ciclo de desarrollo del software.
b. La interfaz web debe ser analizada mediante dos herramientas de pruebas dinámicas de seguridad de aplicaciones (DAST) basadas en el estándar OWASP.
c. Las vulnerabilidades ALTAS y CRÍTICAS resultado de los análisis SAST y DAST deben ser mitigadas previo al paso a producción.
d. Todas las vulnerabilidades deben ser documentadas como parte de la información técnica de la aplicación.

Procesamiento de mensajes / Control de flujo y organización de servicios La arquitectura conceptual presentada representa un bus de servicio empresarial centrado en la atención médica que existe como una capa arquitectónica distinta de la gestión de servicios. Esta capa es responsable del procesamiento y la orquestación de mensajes, no es de acceso público y está concebida para acceder a través de un servicio proxy en la capa de gestión de servicios. Se espera que esta capa cumpla con los requisitos para patrones comunes de interfaz de atención médica. Los proponentes deben responder a las preguntas de esta sección con el fin de proporcionar aclaraciones y detalles adicionales.	
ESB-001	La solución admite adaptadores de conectividad entrantes y salientes, y sus contrapartes seguras, con una gama de protocolos que incluyen, TCP, MLLP, HTTP, SOAP 1.2, REST, FTP, SFTP, SMTP, UDP, SQL, JDBC, ODBC, MQ. JMS, APIs REST FHIR, basadas en perfiles de IHE (de acuerdo a lo especificado en la fase de diseño y guía de implementación)
ESB-002	La solución debe admitir el modelado de procesos con capacidades BPEL o similar
ESB-003	La solución debe tener soporte listo para usar para patrones de integración de atención médica comunes con la capacidad de crear nuevas definiciones de patrones y usarlas para poner en marcha nuevos servicios de integración utilizando patrones existentes rápidamente.
ESB-004	La solución debe incluir aceleradores de interoperabilidad de atención médica que favorezcan el intercambio de mensajes con perfiles IHE 5y formatos de mensajes, incluidos XDS, XCA, PAM, PIX / PDQ, ATNA, XUA, HL7 V2.3.1, HL7 V2.5, HL7 V3, FHIR, CDA, CCD , DICOM, ebXML, ADT, ORU, ORM, y los específicos para los procesos de prescripción, validación, dispensación y administración de medicamentos y bienes estratégicos: ● RXO ● RXR ● RXC ● RXE ● RXD
ESB-005	La solución debe soportar la mediación y la definición del flujo de procesos para la validación, transformación, registro y manejo de excepciones.
ESB-006	La solución debe admitir el mapeo y la transformación entre los formatos de mensajes estándar de Healthcare y los formatos EDI o XML personalizados.
ESB-007	La solución debe tener características de orquestación que permitan la abstracción y el uso de múltiples líneas de servicios comerciales de backend para un único servicio comercial de frontend expuesto al consumidor.
ESB-008	La solución debe tener capacidades de mediación y orquestación que incluyan operadores lógicos, iteración y controles de proceso que incluyan la capacidad de generar procesos asíncronos, ejecutar procesos paralelos, mantener el orden en un flujo de mensajería (es decir, FIFO) con la opción de sincronizar respuestas de procesos paralelos en el orden en que fueron engendrados originalmente.
ESB-009	La solución debe tener la capacidad de capturar y retener datos y metadatos completos de mensajes de solicitud / respuesta, incluidos los atributos de encabezado SOAP o HTTP entrantes originales para los mensajes del servicio web, haciéndolos disponibles para su uso durante el procesamiento de intercambio de mensajes.
ESB-010	La solución debe incluir un sistema de colas robusto y escalable con colas de punto a punto o basadas en temas.
ESB-011	La solución debe poder analizar archivos por lotes en formatos de archivo HL7 y tener soporte para procesamiento XML: Transformaciones XSLT, Funciones XQuery y uso de XPath

ESB-012	La solución debe tener un marco de manejo de excepciones para una administración consistente de excepciones atrapadas o no atrapadas de la lógica de procesamiento empresarial.
ESB-013	La solución debe contar con un sistema de monitoreo empresarial para el registro de eventos a nivel del sistema, eventos de procesamiento comercial y excepciones en el contexto de los metadatos del servicio, incluido el consumidor del servicio, el proveedor, el tipo de operación y mensaje, el SLA y la información de la política.
ESB-014	El componente de gestión de eventos debe ser capaz de invocar los servicios correspondientes cuando el evento ocurra
ESB-015	La solución debe tener herramientas que permitan editar y reproducir o eliminar mensajes fallidos.
ESB-016	La solución debe estar respaldada con instrumentación y monitoreo para que el personal de integración pueda rastrear el estado de los servicios, los procesos en ejecución y el uso de recursos.
ESB-017	La solución debe poder capturar mensajes completos en un área de registro segura para que el personal de operaciones acceda a ellos y los analice. Los mensajes se pueden ver como formato de texto (sin procesar) o HEX, con opciones para filtrar la visualización de mensajes con los formatos estándar de Healthcare (por ejemplo, HL7, XML, DICOM, ebXML) para facilitar la visualización.
ESB-018	El ESB debe soportar mecanismos de autenticación o integración con sistemas de gestión de identidades contemplando protocolos tales como: LDAP, Active Directory, OpenSSO, OpenID, OAuth2, SAML2, SCIM, soporte de autenticación multi-option y multi-factor
ESB-019	La solución debe admitir la lógica de codificación en lenguajes de programación o scripts no propietarios.
ESB-020	La solución debe incluir control de versiones y gestión del ciclo de vida para la lógica empresarial y los artefactos de soporte.
ESB-021	La solución debe incluir herramientas que respalden el desarrollo basado en pruebas y las pruebas unitarias automatizadas mediante las cuales los scripts de prueba y las simulaciones pueden automatizarse para ejecutar los flujos de integración. Las pruebas deberán contemplar aspectos de seguridad, carga y estrés de operaciones y validación de entradas/salidas.
ESB-022	Transformaciones de mensajes, Convertir mensajes canónicos a mensajes propios de aplicaciones consumidores y aplicaciones legadas según corresponda
ESB-023	El ESB debe tener una consola de administración que permita la definición, gestión y monitoreo de SLA de los servicios a desplegar en el mismo
ESB-024	El ESB debe tener un componente encargado de procesar eventos programados en el sistema.
ESB-025	El ESB debe tener un componente de LOG configurable que permita a los servicios desplegados en el mismo, utilizar la funcionalidad de escribir en el LOG del ESB.
ESB-026	El ESB debe tener un componente de auditoria, que permita a los servicios del BUS registrar información auditable, de acuerdo con las necesidades del negocio
ESB-027	Integridad: El ESB debe garantizar mecanismos que permitan mantener la integridad de la información, expuesta a través de servicios de modificación de los datos.

ESB-028	Confidencialidad: EL ESB debe garantizar la protección frente a accesos no autorizados a información confidencial.
ESB-029	Disponibilidad y No repudio: El ESB debe tener herramientas que permitan evidenciar el registro del envío de mensajes por parte de los consumidores de los servicios y de la recepción por parte de los servicios proveedores. Y se deberá garantizar la disponibilidad del ESB, deberá atender todas las peticiones que le sean asignadas sin contener algún límite lógico.
ESB-030	Auditoría: El ESB debe tener un componente que permita registrar el rastro de auditoria para los mensajes que ingresen (resquest) y los mensajes que salgan (response) de cada uno de los servicios del BUS a través de componentes no invasivos, en los cuales se pueda determinar qué información es relevante para trazar.
Supervisión/Monitoreo: La arquitectura conceptual describe la supervisión y el monitoreo como una solución de nivel empresarial que captura registros y excepciones de la infraestructura de la solución y los componentes de procesamiento empresarial en todas las capas arquitectónicas. El sistema es capaz de calificar los registros contra los metadatos del servicio y los puntos finales (end points) específicos cuando sea apropiado y filtrar los datos para su presentación por función de las partes que interoperan (RPIS – Operador logístico). Se presume que una solución de monitoreo de nivel empresarial como esta puede estar separada del monitoreo del procesamiento de mensajes centrales en ausencia de la solución completa. Por lo tanto, los proponentes deben usar esta sección para calificar la funcionalidad que está disponible para cumplir con los requerimientos una solución de monitoreo a nivel empresarial.	
MON-001	La solución de supervisión debe poder capturar el estado del sistema de todos los componentes de la solución.
MON-002	La solución de monitorización debe admitir protocolos de registro estándar como SNMP, Syslog, conectores JMX TCP genéricos
MON-003	La solución de monitoreo debe poder capturar eventos como el inicio y el cierre del proceso, los pasos del proceso comercial y las excepciones.
MON-004	La solución de monitoreo debe poder monitorear la cola, la base de datos y los componentes del sistema de archivos para el desempeño, la capacidad y los umbrales.
MON-005	La solución de monitoreo debe poder capturar y alertar sobre eventos de seguridad como intentos fallidos de inicio de sesión, validaciones fallidas de certificados o certificados que están a punto de caducar.
MON-006	La solución de monitoreo debe poder configurarse para alertar solo una vez o en una iteración configurada a una situación repetida (por ejemplo, la cola en el umbral solo alerta una vez cada 30 minutos).
MON-007	La herramienta de supervisión debe poder alertar sobre patrones de tráfico anormales (por ejemplo, no hay mensajes desde el punto final dentro del intervalo de tiempo definido).
MON-008	La herramienta de monitoreo debe tener alertas o situaciones preconfiguradas para los componentes centrales de las soluciones.
MON-009	La solución de monitoreo debe integrarse con metadatos y políticas de servicio o definiciones de SLA de manera que pueda informar sobre eventos comerciales en el contexto del consumidor de servicio, proveedor y contrato de servicio.
MON-010	Visualizar recursos de las aplicaciones y flujos implementados, componentes y mensajes que se intercambian, estado del servidor en cuanto a consumo de recursos físicos donde se ha despejado, concurrencias, estados de ACK.

MON-011	La solución de monitoreo debe permitir la tenencia múltiple para el acceso a los datos, por lo que los roles comunes a varias organizaciones son calificados por la organización desde la que se accede a los datos y dos usuarios de dos organizaciones no pueden ver los datos del otro incluso cuando están en el mismo rol. .
MON-012	La solución de monitoreo permite personalizar las alertas para la función del usuario con texto preconfigurado o contenido dinámico (por ejemplo, la alerta incluye una identificación de documento de un mensaje).
MON-013	La solución de supervisión debe admitir la supervisión de la carga de trabajo.
MON-014	La solución de monitoreo permite generar informes, específicos para el rol del usuario, para una colección de servicios, para un servicio específico o para consumidores de servicios específicos.
MON-015	La solución de monitoreo debe poder informar sobre estadísticas técnicas o enfocadas en la información clínica para el volumen y el rendimiento relacionados con tipos de mensajes específicos (el proceso de prescripción, validación, dispensación y administración de medicamentos y bientes estratégicos).
MON-016	La solución de monitoreo se integra al sistema de administración de acceso de identidad del MSP y tiene controles de acceso que restringen el acceso a funciones y vistas por rol.
Registro XDS El componente de registro XDS de la arquitectura conceptual presentada representa tanto el repositorio como las interfaces de servicio basadas en los perfiles de integración IHE para el intercambio de documentos entre empresas (XDS) y el acceso entre comunidades (XCA). A través de los repositorios y las interfaces de servicio, MSP tiene la intención de permitir el intercambio de documentos federados entre los sistemas de salud afiliados. Los proponentes deben responder a los elementos de esta subsección para aclarar aún más los componentes de la solución propuesta que cumplen con esta visión.	
XDS-001	La solución incluye un repositorio y registro de documentos compatible con XDS capaz de almacenar resúmenes médicos de CDA's, CCD, datos de laboratorio, informes y documentos, ampliados con interfaces de servicio XDS y XCA.
XDS-002	La solución de registro XDS debe instalarse y configurarse, lo que incluye, la configuración del registro de auditoría, la configuración del dominio de afinidad (asignación de autoridades, códigos, reglas de validación), la configuración del registro XDS, la habilitación de puertos HL7, incluidas las fuentes de identidad del paciente, la configuración de conexiones de base de datos seguridad, incluida la integración con MSP Identity and Access Management, la configuración del punto final del agente de notificación.
XDS-004	La solución de XDS Registry debe cumplir con el actor IHE XDS-Ib Document Registry para la interoperabilidad con las fuentes de documentos y los consumidores, incluidas las transacciones principales de IHE Register Document Set – b [ITI-42] (respondedor), Registry Stored Query [ITI-18] (respondedor), información sobre la identidad del paciente [ITI-8] o información sobre la identidad del paciente HL7V3 [ITI-44] (respuesta), registro de eventos de auditoría [ITI-20] (emisor).
XDS-005	La solución XDS Registry debe configurarse para admitir metadatos de documentos para documentos clínicos (CDA), de resumen medicos (CCD) y otros documentos clínicos, incluidos los atributos de metadatos XDS / XDS-Ib estándar y cualquier extensión (metadatos personalizados) requeridos por MSP.
XDS-006	La solución de registro XDS debe configurarse para validar los metadatos del documento al registrarlo (consulte [ITI-42]).
XDS-007	La solución XDS Registry debe asociar un documento actualizado con la versión

	anterior del documento.
XDS-008	La solución de XDS Registry debe asociar el apéndice de un documento con el documento principal. (Debe permitir la persistencia de asociaciones de appendices)
XDS-009	La solución de registro XDS debe proporcionar funciones administrativas a través de una interfaz gráfica de usuario para administrar los privilegios administrativos, configurar el registro XDS, inspeccionar el estado de tiempo de ejecución del registro XDS, monitorear las conexiones a los puntos finales configurados, inspeccionar los registros de eventos y auditoría.
XDS-010	La solución de XDS Registry debe poder restringir el acceso a los repositorios de documentos por función.
XDS-011	La solución de registro XDS debe admitir transacciones IHE opcionales, incluidas Actualizar conjunto de documentos [ITI-57] (respondedor), Eliminar conjunto de documentos [ITI-62] (respondedor), Notificar cambio de enlace XAD-PID [ITI-64] (respondedor) o HL7v3 equivalente, consulta almacenada de varios pacientes [ITI-51] (respondedor).
XDS-012	La solución de XDS Registry debe cumplir con el actor IHE DSUB Document Metadata Publisher y respaldar transacciones, incluidas Document Metadata Publish [ITI-54] (emisor), Document Metadata Subscribe [ITI-52] (respondedor) y Document Metadata Notify [ITI-53] (emisor).
XDS-013	La solución XDS Registry debe brindar soporte para aplicar actualizaciones globales a los metadatos de los documentos, incluidos metadatos de terminología (es decir, como resultado de cambios en el mapeo de vocabulario), cambios demográficos de proveedores o pacientes u otros metadatos de documentos.
XDS-014	La solución de XDS Registry debe integrarse a la solución de monitoreo empresarial.
XDS-015	La solución deberá contemplar repositorios compatibles con estándares OpenEHR, ISO13606, RIM, SMART on FHIR® o similares.
XDS-016	El almacenamiento de datos en el repositorio único se realizará teniendo como referencia los catálogos maestros y terminologías definidas en Gestión de Catálogos Maestros y Terminologías del presente documento.
Seguimiento de auditoría El componente Audit Trail de la arquitectura conceptual del MSP representa tanto un repositorio de Audit Trail como interfaces de servicio basadas en el perfil IHE ATNA y las especificaciones de transacciones ITI para registros de eventos de auditoría. El objetivo de la arquitectura conceptual es lograr un repositorio central basado en estándares para divulgaciones clínicas a través de la integración. Esta subsección permitirá a los proponentes aclarar cómo su componente de solución puede cumplir esa función.	
AUD-001	La solución debe incluir un componente de seguimiento de auditoría compatible con IHE ATNA para registrar la divulgación de datos clínicos.
AUD-002	La solución Audit Trail debe tener una interfaz de usuario para ver registros de eventos de auditoría que permita filtrar por fecha y hora de inicio y finalización y otros metadatos comunes a los registros de eventos de auditoría definidos por ATNA.
AUD-003	La solución Audit Trail debe suprimir el acceso a la pista de auditoría clínica por función o rol
AUD-004	La solución Audit Trail debe poder recibir mensajes de auditoría de Syslog a través de UDP, TCP, HTTP o los equivalentes de TLS seguros para TCP y HTTP.
AUD-005	La solución Audit Trail debe admitir la transacción Record Audit Event [ITI-20]

	(receptor).
AUD-006	La solución Audit Trail debe admitir los formatos de mensajes de auditoría especificados por IHE y tener la flexibilidad de admitir formatos personalizados definidos por el esquema XML.
AUD-007	La solución Audit Trail debe proporcionar interfaces que permitan consultar el repositorio de pistas de auditoría desde otras aplicaciones para consultas de eventos de auditoría agregadas que respalden las investigaciones de privacidad.
Enrutamiento de entrega electrónica (e-Delivery Routing) La arquitectura conceptual presentada representa un repositorio de enrutamiento de entrega electrónica y un componente de interfaz de servicio. El repositorio permite la configuración de la entrega dirigida para proveedores nombrados sobre prescripciones, validaciones, dispensaciones, administraciones u otro contenido para su distribución. Una solución de entrega dirigida se diferencia de una solución de publicación / suscripción en que la institución remitente o autor de una solución de entrega dirigida requiere un reconocimiento de garantía de entrega para el destinatario designado. Un repositorio de enrutamiento de entrega electrónica permite la configuración de opciones de entrega basadas en el contenido y las necesidades de considerar el tipo de contenido, pacientes hospitalizados o ambulatorios, ubicación del servicio, la participación del proveedor de atención en el encuentro, la relación del proveedor con el paciente y las ubicaciones de servicios del proveedor y la función del proveedor en esas ubicaciones. Las preferencias o reglas del proveedor determinan si se puede resolver el enrutamiento de entrega y se puede devolver un reconocimiento positivo al sistema de envío. La arquitectura conceptual describe el enrutamiento de entrega electrónica que proporciona el contexto de entrega para el contenido que se origina en sistemas de la RPIS internos o externos a a ella, a través de una interfaz de servicio expuesta por el repositorio para la capa de orquestación / ESB de middleware.	
DLV-001	La solución e-Delivery debe integrarse con (servicio de validación de profesionales de la salud provisto por el Ministerio de Educación de Ecuador) para resolver las identidades de los proveedores de la RPIS
DLV-002	La solución e-Delivery debe integrarse con las soluciones Facility Registry para resolver las ubicaciones de los servicios de los prestadores de la RPIS y el operador logístico.
DLV-003	La solución e-Delivery incluye un repositorio de reglas de enrutamiento que permite especificar dónde deben entregarse los informes según el contenido del mensaje y las ubicaciones donde el prestador brinda el servicio.
DLV-004	La solución e-Delivery incluye una interfaz de servicio que identifica si un proveedor/prestador dado tiene reglas de enrutamiento definidas y puede responder con información sobre la modalidad de entrega de contenido al proveedor dado.
DLV-005	La solución e-Delivery debe poder transformar los mensajes en tiempo real en formatos de archivo por lotes estándar de Healthcare.
DLV-006	La solución e-Delivery debe admitir múltiples modalidades para la entrega de mensajes o informes, como SFTP, mensajería directa y servicios web SOAP Y REST.
DLV-007	La solución e-Delivery debe integrarse con la solución Pub / Sub para la identificación de sistemas de consumidores y métodos de entrega.
DLV-008	La solución e-Delivery debe poder garantizar que los informes o mensajes se entregarán al destinatario identificado cuando haya acusado recibo del mensaje o informe para su entrega.
DLV-009	La solución e-Delivery debe tener una interfaz de usuario para la gestión del sistema con acceso a funciones que se puedan restringir por rol.
DLV-010	La solución e-Delivery debe integrarse al sistema de gestión de acceso e

	identidad del MSP.
Pub / Sub La arquitectura conceptual presentada describe un sistema Pub / Sub que permite desvincular al editor o generador de contenido del consumidor suscrito al contenido. Esto implica un sistema de intermediación en el que el sistema de publicación envía su contenido al intermediario y el intermediario asume la responsabilidad de administrar a los consumidores suscritos y garantizar que esos consumidores reciban el contenido publicado en un estado desconectado del editor. Esto difiere de la entrega electrónica en que el remitente no especifica el destinatario ni requiere un reconocimiento de garantía de entrega para un destinatario previsto.	
PSB-001	La solución Pub / Sub debe admitir reglas de transformación y / o enmascaramiento basadas en el consumidor suscrito o el tipo de consumidor suscrito
PSB-002	La solución Pub / Sub debe admitir mensajería de publicación / suscripción negociada, donde pueda recibir notificaciones de los editores, realizar la comparación de suscripciones y, posteriormente, enviar notificaciones a los consumidores suscritos coincidentes.
PSB-003	La solución debe poder generar un informe para todas las suscripciones activas, incluidos campos como quién se suscribió, a qué tema.
PSB-004	La solución Pub / Sub debe garantizar que las notificaciones se envíen a los consumidores en la misma secuencia en que se recibieron del editor.
PSB-005	La solución Pub / Sub debe integrarse con el sistema de gestión de identidades del MSP para el acceso basado en roles de usuarios suscriptores (es decir, consumidores suscritos a través de una interfaz de usuario).
PSB-006	La solución Pub / Sub debe configurarse fácilmente para adaptarse a nuevos tipos de temas, suscripciones y notificaciones, sin afectar a los editores y suscriptores existentes.
PSB-007	La solución Pub / Sub debe admitir notificaciones de estilo push y pull
PSB-008	La solución Pub / Sub debe garantizar la entrega de notificaciones a los puntos finales de los consumidores.
PSB-009	La solución Pub / Sub debe tener la capacidad de enviar notificaciones a través de una variedad de canales de entrega, por ejemplo, correo electrónico, SMS, mensajería directa, servicio web (WS-BaseNotification), recurso de punto de extracción.
PSB-010	La solución Pub / Sub debe brindar a los administradores la capacidad de administrar todos los aspectos de la solución Pub / Sub, incluida la administración de mensajes no entregados y / o la administración de colas.
PSB-011	La solución Pub / Sub debe proporcionar informes a los usuarios comerciales y del sistema / operaciones sobre transacciones fallidas / reintentos para las notificaciones por suscripción por período de tiempo.
PSB-012	La solución Pub / Sub debe admitir el filtrado basado en contenido para suscripciones.
PSB-013	La solución Pub / Sub debe validar las solicitudes de suscripción (p. Ej., Validar suscriptor, consumidor, tema, filtros y puntos finales de entrega)
PSB-014	El servicio de solución Pub / Sub debe permitir la agrupación / procesamiento por lotes / segmentación de notificaciones en función de una variedad de parámetros, como la cantidad máxima de elementos, el período de tiempo, el tamaño de la notificación del lote.
PSB-015	La solución Pub / Sub debe admitir notificaciones en formatos de archivo por lotes especificados por HL7.

PSB-016	La solución Pub / Sub debe proporcionar informes a los usuarios comerciales y del sistema / operaciones sobre suscripciones activas por consumidor o por tema - Historial de suscripciones por consumidor o por tema - Actividad de suscripción (actualizaciones, pausas / reanudaciones) por tema por período de tiempo (semanal, mensual): las suscripciones vencerán el próximo período de tiempo (la próxima semana, mes.)
PSB-017	La solución debe proporcionar informes a los usuarios comerciales y del sistema / operaciones sobre el informe de auditoría - quién / cuándo / qué se hizo por Suscripción / tema - Informe general del sistema - número de temas, sus correspondientes suscripciones y volúmenes El monitoreo de la solución debe proporcionar información real - vista de tiempo de las mismas métricas
PSB-018	La solución debe proporcionar informes a los usuarios comerciales y del sistema / operaciones sobre el volumen de transacciones de notificación por suscripción / tema / consumidor por prioridad de mensaje por período de tiempo
PSB-019	La solución debe proporcionar informes a los usuarios comerciales y del sistema / operaciones sobre la longitud / tamaño de la cola / tema por período de tiempo (cuántos mensajes hay en las colas / temas) en comparación con la longitud / tamaño máximo de la cola con tendencias
PSB-020	La solución debe proporcionar informes a los usuarios comerciales y del sistema / operaciones sobre el informe de SLA: tiempos de procesamiento / entrega de notificaciones, tamaños de mensajes, volúmenes en comparación con SLA
Registro de terminologías La arquitectura conceptual presentada cita un componente de Registro de terminología que está previsto para proporcionar una interfaz de servicio para la orquestación, así como interfaces de usuario para la gestión de vocabulario.	
TRM-001	La solución incluye un repositorio de terminología y debe proporcionar un almacenamiento centralizado de los sistemas de códigos utilizados en Ecuador, incluidas colecciones de términos relacionados con la salud como el Cuadro Nacional de Medicamentos Básico CNMB, SNOMED CT® (Nomenclatura sistemática de la medicina - Términos clínicos), ICD-10. (Clasificación internacional de Enfermedades 10ma edición), LOINC® (Nombres y códigos de identificadores de observación lógica), Tablas de codificación HL7 o ISO, DICOM, el catálogo de medicamentos para Ecuador CNMB
TRM-002	La solución debe incluir una interfaz de servicio de validación terminológica y debe determinar automáticamente que los términos y los datos codificados (tanto clínicos como no clínicos) existen en una colección específica de términos.
TRM-003	La solución debe proporcionar acceso basado en roles configurable y seguro a todos los activos terminológicos (aplicaciones y servicios)
TRM-005	Las herramientas de mantenimiento de terminología deben permitir a los administradores de terminología importar conjuntos de valores desarrollados en otras herramientas al repositorio de terminología
TRM-006	El repositorio de terminología debe conservar un historial auditable y un registro de los cambios en todos los activos terminológicos Las versiones publicadas de los activos terminológicos deben tener un período de validez con fechas de vigencia.
TRM-007	El repositorio de terminología debe tener una interfaz de servicio que permita a sistemas específicos solicitar y recuperar conjuntos de valores para ese sistema.

TRM-006	El repositorio de terminología debe permitir la inactivación de un sistema de códigos y permitir la adición de sistemas de códigos por parte del MSP/RPIS cuando se requiera
TRM-007	La herramienta de mapeo terminológico debe conservar un historial auditable de los cambios en las asociaciones para respaldar la auditoría, los informes y las métricas basadas en roles.
TRM-008	La solución debe proporcionar una interfaz de sistema para la notificación de cambios, configurable en niveles de granularidad que incluyen sistema de código, conjunto de valores / conjunto de referencias (por ejemplo, medicamentos, códigos de país), códigos de terminología, metadatos de código y asignaciones.
TRM-008	La solución debe proporcionar una validación de la terminología sensible al contexto (por ejemplo, un término solo es válido en una determinada posición dentro de un mensaje HL7; los términos deben validarse con el conjunto de valores correcto según el contexto dentro del mensaje).
TRM-009	El repositorio de terminología y las herramientas de mantenimiento de terminología deben proporcionar un medio para relacionar una versión de un conjunto de valores con la versión adecuada del sistema de códigos o estándar subyacente.
TRM-010	La solución debe ajustarse a los requisitos de licenciamiento del país para el uso de contenido terminológico según las Organizaciones de desarrollo de estándares (SDO) aplicables. Esto se aplica a los estándares de terminología como SNOMED CT, LOINC, ICD 10, HL7, ISO.
TRM-011	La solución debe proporcionar a los administradores de terminología la capacidad de importar solicitudes de cambio (RFC) al repositorio de terminología tanto de forma manual como automatizada, validando el término solicitado con las terminologías existentes.
TRM-012	La herramienta de mapeo terminológico debe proporcionar una visualización integrada de mapeos anteriores (en muchas instalaciones / sitios, por ejemplo, mapeo para la publicación de CNMB); Visualización simultánea mientras se realizan funciones de mapeo
TRM-013	La solución debe proporcionar la capacidad de exportar un informe que muestre cambios entre versiones de conjuntos de valores.
TRM-014	La solución debe proporcionar una interfaz gráfica de usuario, servicios web y un mecanismo de importación / exportación basado en archivos.
TRM-015	El repositorio de terminología y las herramientas de mantenimiento de terminología deben respaldar el desarrollo, el mantenimiento continuo y la publicación de conjuntos de valores que contienen una combinación de códigos definidos por el MSP (códigos provisionales o extensiones) y códigos universales.
TRM-016	La solución debe proporcionar la capacidad a los suscriptores de agregar / modificar el servicio de suscripción para contenido terminológico como LOINC y otros estándares de contenido terminológico aplicables en cualquier momento.
TRM-017	Las herramientas de mantenimiento de terminología deben brindar la capacidad de importar y exportar terminología en una variedad de formatos predefinidos (por ejemplo, archivo plano, hoja de cálculo, XML, servicios web)
TRM-018	El repositorio de terminología debe admitir descripciones múltiples en campos separados por código y admitir la codificación de acentos de idiomas (por ejemplo, ASCII, UTF-8, ISO-8859)
TRM-019	Toda la funcionalidad proporcionada por las herramientas de mapeo y mantenimiento de terminología que involucran la interacción del usuario final debe estar disponible a través de la interfaz gráfica de usuario (GUI) basada en la web.

TRM-020	La solución debe proporcionar notificaciones sobre los eventos del ciclo de vida de la terminología (nuevo, actualizado, obsoleto) a los clientes / sistemas suscritos
TRM-021	La solución debe proporcionar informes exportables que incluyan: valores de código que cambiaron por período de tiempo, número de valores de código por mapa de terminología, valores de código cambiados por función, valores de código cambiados por usuario
TRM-022	La herramienta debe proveer capacidades de Mapeo de Terminología con capacidad de exportar las asignaciones en varios formatos predefinidos y personalizables (incluidos XML y CSV) para importarlos a sistemas y para revisión humana.
TRM-023	La solución debería proporcionar al MSP la capacidad de agregar nuevos informes terminológicos en el futuro.
TRM-024	La solución debería normalizar el formato de las cadenas dentro del contenido de la terminología (por ejemplo, mayúsculas y espacios adicionales)
TRM-025	La solución debe admitir múltiples formatos de carga útil en notificaciones de terminología (es decir, CSV, XML y HTML)
TRM-026	El proveedor debe migrar versiones actuales y heredadas de terminologías y reglas de mapeo mantenidas en los sistemas actuales de MSP al registro de terminología (CNMB), así como también incluir catálogos de especialidades (ACESS), catálogos de DPA (INEN), catálogo de UNIDADES DE SALUD (MSP)
Registro de instalaciones La arquitectura conceptual presentada describe un registro de instalaciones como un componente separado para administrar las identidades de los lugares de prestación de servicios y farmacias comunitarias en asociación con sus organizaciones matrices. Dicho componente permite que una capa de orquestación valide identidades de instalaciones conocidas o busque y utilice atributos de datos maestros de instalaciones en otros servicios comerciales orquestados.	
FCY-001	La solución incluye un registro de instalaciones para rastrear e identificar entidades proveedoras de servicios de atención (por ejemplo, hospitales, clínicas, puestos de salud, consultorios médicos, farmacias) dentro o fuera del MSP o RPIS.
FCY-002	El registro de la instalación debe tener interfaces de servicio (p. Ej., Servicio SOAP / RESTful) que permitan la búsqueda, validación, adición, actualización o desactivación de las identidades y atributos de la instalación.
FCY-003	El registro de la instalación debe mantener un historial de cambios en el registro con metadatos que rastreen qué cambios se realizaron, quién, cuándo y desde dónde.
FCY-004	El registro de la instalación debe tener una interfaz de usuario para el acceso administrativo y las tareas de mantenimiento.
FCY-005	El registro de la instalación debe integrarse a la solución de gestión de acceso de identidad del MSP y poder restringir el acceso a las funciones por función.
FCY-006	El registro de instalaciones debe asociar las instalaciones con su organización coordinadora. La organización “paraguas o maestra” tiene un identificador único y atributos administrativos y demográficos, Una organización debe poder tener una o más instalaciones asociadas.
FCY-007	Las instalaciones en el registro de instalaciones deben especificar uno o más servicios que se brindan en esa instalación.
FCY-008	Las instalaciones en el registro de instalaciones deben tener atributos que incluyan el tipo de instalación, las horas de operación, la información de contacto.
FCY-009	La interfaz del servicio de registro de instalaciones debe permitir encontrar una

	instalación por nombre, dirección, tipo o identificación.
FCY-010	El registro de la instalación debe poder asociar a los proveedores como miembros de la instalación y como proveedores de los servicios de la instalación.
Organización y requisitos generales de la solución	
GEN-001	Debe tener una hoja de ruta de producto establecida que cubra de 3 a 5 años y múltiples ciclos de lanzamiento de versiones por año.
GEN-002	La hoja de ruta histórica debería mostrar una tendencia hacia la respuesta a las tecnologías emergentes en la atención médica.

<table>
<tr><td>GEN-003</td><td>Debe tener capacidad para implementar la solución e integrar sitios de atención médica de la RPIS, considerando como mínimo:
MSP: 1939 Centros de Salud y 135 Hospitales.
F.F.A.A: 78 Centros de Salud y 1 Centro de Especialidades.
Policía Nacional: 42 Centros de Salud y 2 Hospitales.
IESS: 659 Seguro Campesino, 48 Centros de Salud y 53 Hospitales.
Con alrededor de 3000 usuarios (como base), considerando al menos 20 sistemas de información dentro de los cuales son en de uso común en las entidades, los siguientes: PRAS (MSP), AS/400 (IESS), Innovativa (ISSFA), IntegraSalud, Hosvital (ISSPOL)</td></tr>
<tr><td>GEN-004</td><td>Debe tener capacidad para gestionar un volumen de transacciones mínimo o superior al que se especifica en la siguiente tabla:

<table>
<tr><th>INSTITUCIONES</th><th>PROMEDIO MENSUAL (2018-2019)</th><th>CANTIDAD PROMEDIO RECETAS FISICAS DIARIO (2018-2019)</th><th>CANTIDAD DE RECETAS ELECTRONICAS (Considerando 1 y 2 ítems por receta)</th><th>CANTIDAD DE PETICIONES BASE DIARIAS BUS ESTIMADAS</th></tr>
<tr><td>FFAA</td><td>5.336</td><td>178</td><td>356</td><td>711</td></tr>
<tr><td>IESS</td><td>3.179.739</td><td>105.991</td><td>143.883</td><td>287.767</td></tr>
<tr><td>ISSPOL</td><td>21.336</td><td>711</td><td>975</td><td>1.950</td></tr>
<tr><td>MSP</td><td>7.147.659</td><td>238.255</td><td>443.828</td><td>887.657</td></tr>
<tr><td>Total general</td><td>10.354.070</td><td>345.136</td><td>589.042</td><td>1.178.085</td></tr>
</table>

1) La estimación se la realizó utilizando los datos proporcionados por las entidades de la RPIS, para el volumen de recetas producidas en promedio entre 2018-2019 dentro de 2353 establecimientos de salud. Resaltando que no se cuenta con datos estadísticos para 584 establecimiento de salud, los cuales representan un 24,82% del total. Por lo que es importante considerar para la volumetría de recetas diarias este número, que corresponde principalmente a entidades que no reportaron datos o no tienen receta electrónica.
2) La estimación de ítems por receta es un valor aproximado, ya que, en función de la entidad y tipo de establecimiento, puede haber mínimo 1 ítem por receta, y no puede tener un valor máximo (n ítems). Para los cálculos se utilizó un promedio de 2 ítems por receta para centros y 1 ítem por receta para hospitales.
3) La cantidad de peticiones básicas (de la receta) como mínimo pueden ser dos, se incluye una consulta de la receta (validada) para ejecutar el proceso de dispensación, así como un registro por parte de quien ejecuta la dispensación (en este caso el Operador Logístico). Se deben considerar de manera adicional las peticiones relacionadas a autenticación y autorización (Ejemplo: generación de un Token).
4) Se debe considerar que el peso aproximado de una receta electrónica con 10 medicamentos es de 1.6-2.5KB. Por lo que se debe tener presente el dimensionamiento de almacenamiento necesario para albergar los registros</td></tr>
</table>

	durante 10 años.
GEN-005	Los servicios deben contemplar la autenticación con TOKEN cómo mecanismo adicional de autenticación.
GEN-006	Se debe contemplar la capacidad de cifrar información del paciente en caso de ser necesario, esto en los servicios que involucren el envío de información sensible del mismo. Mediante el uso de cifrado y anonimización.
GEN-007	Se debe garantizar el no repudio de las invocaciones de los servicios tanto desde sistemas externos, como a sistemas fuera del MSP
GEN-008	El fabricante ofrece cobertura local y es capaz de implementar y proveer soporte post venta en Ecuador, a través de dos o más canales o proveedores de sus servicios.
GEN-009	Preferible pertenecer a una comunidad de usuarios con evidencia de actividad e interacción regular.
GEN-010	El proponente debe acreditar experiencia en implementaciones similares que incluyan la integración de instituciones médicas públicas/privadas /hospitales universitarios y preferiblemente que las integraciones involucren procesos de logística de prescripción/dispensación de medicamentos.
GEN-11	El sistema deberá permitir realizar notificaciones vía correo electrónico, SMS, WhatsApp y portal de usuarios Sanitas a los profesionales y los usuarios.
GEN-12	Deberá permitir la auditabilidad y la trazabilidad para medir de forma fiable y ágil el uso que hacen los usuarios de las funcionalidades principales
GEN-13	Como herramienta de usuario final deberá estar en español, pero podrá ser configurable para ser multi idioma.
GEN-14	Las componentes funcionales descritas deberán estar operativas y disponibles como mínimo el 99.9% del tiempo, que traduce en una indisponibilidad máxima de 1 minuto 26 segundos diarios o 10 minutos y 4 segundos semanales o 43 minutos y 33 segundos mensuales (sin tener en cuenta paradas programadas aprobadas por el MSP).
GEN-15	El proveedor deberá definir un modelo de gobierno para la capa de interoperabilidad de acuerdo con las políticas, roles, miembros, actividades considerando estándares, lineamientos, procedimientos
GEN-16	El proveedor deberá entregar un inventario de los servicios, API'S y microservicios implementados para la solución
GEN-17	La solución deberá permitir interoperar e integrar la información de forma síncrona y asíncrona de los catálogos maestros y sistemas de información internos y externos
GEN-18	La solución deberá permitir interoperar e integrar diversas fuentes de información con los estándares XML, JSON, HL7, FHIR

GEN-19	La solución deberá proporcionar medidas que aseguren el funcionamiento y la calidad de las integraciones con base en auditorías técnicas y monitoreos
GEN-20	La solución propuesta deberá tener capacidad de gestión de OIDs (Identificadores de objetos) para los artefactos de interoperabilidad y/o integración.
GEN-21	Los procesos de interoperabilidad e integración deben utilizar certificados digitales en ambientes productivos y no productivos
GEN-22	El proveedor seguirá las guías de implementación HL7, con base en IHE, HL7 v2.x y CDA y FHIR para la información clínica.
GEN-23	La capa de interoperabilidad deberá garantizar la escalabilidad vertical y horizontal para recursos de hardware.
GEN-24	Las integraciones y servicios deberán soportar múltiples codificaciones de caracteres, por defecto la plataforma debe estar configurada en UTF-8
GEN-25	La plataforma deberá contar con un sistema de monitoreo para la capa de interoperabilidad que sea capaz de identificar el sistema consumidor, origen, usuario, tramas de entrada y salida, consolidar la información mensual de la cantidad de transacciones y tiempos de respuesta mínimos, máximos y promedios y consultar el detalle de las transacciones a demanda por medio de un visor.
GEN-26	El proveedor implementará la consulta y recepción de información por integración desde y hacia el repositorio.
Arquitectura, resiliencia y disponibilidad	
ARC-001	Debe poder implementarse en las versiones actuales de VMWare.debe implementarse en versión existente VMWARE de la Infraestructura tecnológica del MSP.
ARC-002	La solución debe estar disponible 7x24x365 99,982% del tiempo - alta disponibilidad
ARC-003	La solución deberá incluir las componentes de infraestructura requerido para respaldos, tales como librería de cintas LTO y servidor para instalación del orquestador con sus respectivos catálogos, manuales hojas técnicas de los servicios o software asociado al servicio
ARC-004	El estado del sistema y los datos de la aplicación deben poder recuperarse al último estado consistente dentro de las 2 horas posteriores a la falla del sistema si la severidad de la falla es alta, 4 horas si la severidad es media y 6 horas si la severidad es baja, tal como se especifica en la tabla de SLA´s de la componente de requerimientos técnicos de este documento.
ARC-005	La solución debe ser recuperable, en un escenario de recuperación ante desastres, en menos de 24 horas.
ARC-006	Debe tener capacidad de procesar mensajes de hasta 1 GB a nivel lógico
ARC-007	Debe escalar para soportar una instalación un crecimiento en instalaciones de atención en un 2% anual y de farmacias comunitarias de un 2% anual estimado, puede variar dependiendo de la cantidad de farmacias que se integren al operador logístico.
ARC-008	La plataforma debe estar en capacidad de soportar la solicitud de al menos 2.000.000 prescripciones al mes (es decir cerca de 25 solicitudes por segundo en promedio), y debe dar respuesta en menos de 3 segundos a cada solicitud.
ARC-010	La plataforma deberá soportar un crecimiento sostenido de un 30% en la invocación del servicio durante los próximos 5 años de vida útil de los equipos.
ARC-011	La plataforma debe estar en capacidad de ejecutar al menos 2.000.000 consultas al mes del servicio de Consulta de prescripciones (25 consultas por

	segundo aproximadamente), con un tiempo de respuesta menor a 3 segundos por cada invocación
ARC-012	La plataforma debe estar en capacidad de soportar al menos 2.000.000 invocaciones mensuales de los servicios de dispensación de medicamentos, con un tiempo de respuesta menos a 3 segundos.
ARC-013	Debe proporcionar funcionalidad donde no se pierdan mensajes
ARC-014	Debe poder poner en cola las transacciones pendientes durante al menos 24 horas sin afectar el rendimiento del sistema
ARC-015	Debería tener 0 pérdida de mensajes en todos los componentes de la solución.
ARC-016	Los nodos, componentes y servicios del sistema deben tener un alto nivel de independencia entre sí, por lo que las fallas y los cambios dentro del entorno se gestionan de tal manera que el sistema pueda continuar las operaciones.
Documentación, ayuda y soporte	
SUP-001	La solución debe poder proporcionar documentación, ejemplos, tutoriales y archivos de ayuda disponibles en formatos de uso común para todas las funciones del producto.
SUP-002	La solución debe poder proporcionar ayuda sensible al contexto
SUP-003	La solución debe ser compatible con servicios de resolución de problemas remotos e in situ, incluido el soporte telefónico y web 24x7 utilizando analistas de soporte capacitados.
SUP-004	El acceso de soporte de la solución a los sistemas del cliente debe regirse por las pautas y controles de acceso adecuados, teniendo en cuenta la privacidad y la confidencialidad de la información médica personal.
SUP-005	Debe tener un proceso documentado para escalar a más analistas de soporte de experiencia y / o recursos de desarrollo.
SUP-006	Debe proporcionar un soporte in situ de calidad en caso de una crisis.
SUP-007	La documentación debe estar disponible en línea y debe poder imprimirse.
SUP-008	Debe proporcionar actualizaciones a la documentación con cambios de sistemas provisionales.
SUP-009	Debe proporcionar un conjunto completo de documentación para cada versión de software.
SUP-010	Debe proporcionar documentación detallada del sistema para todas las funciones y métodos, incluida la sintaxis de todos los campos.
SUP-011	Debe proporcionar documentación de usuario detallada para todas las funciones y procedimientos de la aplicación, incluida la sintaxis de codificación y las definiciones de campo.
SUP-012	Debe proporcionar instrucciones paso a paso para realizar actividades de rutina.
SUP-013	Debe proporcionar servicios educativos básicos y avanzados para arquitectos, desarrolladores y otros analistas u operadores de sistemas.
SUP-014	Debe tener educación continua para nuevas funciones / cambios (por ejemplo, seminarios web, en el sitio

3.2.2 Identificación Única del Paciente (EMPI)

Este componente dentro de la arquitectura de referencia presentada es la encargada de proveer un identificador único e irrepetible del paciente, que asegure su identificación en el sistema. Este identificador único se debe asociar con los identificadores asociados al paciente en los sistemas de información de las entidades de la RPIS, donde ha tenido eventos de prescripción. Este proceso de identificación debe estar apoyado en el MPI, que se convierte en la única fuente de la verdad para la identificación de los pacientes y su información

demográfica. Los requerimientos técnicos de esta componente de la solución se describen a continuación:

ID	Descripción del requisito
MPI-001	Se debe proveer un enterprise master patient index que garantice la calidad de la información del paciente y por medio de probabilidad avanzada y lógica determinista asegurar una coincidencia de documentos, y crear, de forma automática y eficaz, historias de salud completas a partir de los múltiples sistemas de información
MPI-001	Debe permitir la implementación del perfil PIX (Patient Identifier Cross-Referencing) el cual define los actores y transacciones (mensajes HL7) necesarios para mantener un registro maestro de identificadores de pacientes y proporcionar esta información a otras aplicaciones
MPI-002	El perfil PIX (Patient Identity Cross-referencing) soporta la referencia múltiple de identificadores de pacientes que pertenecen a diferentes dominios de identificación.
MPI-003	Es soportado dentro de los dos tipos de mensajería con el mismo propósito: HL7 V2 messaging (PIX/PDQ) y HL7 V3 messaging (PIX/PDQ V3).
MPI-004	Debe proveer herramientas de análisis que disminuyan la posibilidad de crear pacientes duplicados, mediante el uso de gestores que limpien los datos que ingresan desde los sistemas fuente y permita descubrir problemas potenciales generados por datos errados en el MPI
MPI-005	Herramientas de carga de datos de pacientes de forma masiva o por lotes
MPI-006	Visor de registros que permitan validad la identidad y los datos demográficos de los pacientes en todos los registros
MPI-007	Herramientas para la Fusión de pacientes duplicados
MPI-008	Herramientas que garantizan la integridad de registros mediante diagnósticos preventivos de problemas de calidad o de integridad de datos
MPI-009	Debe proveer APIs para la conectividad basada en estándares como HL7 FHIR, HL7 v2.x, IHE (PIX, PDQ, PDQm, XCPD) y Web services, que faciliten la integración del MPI con las aplicaciones de las entidades de la RPIS
MPI-010	Debe contar con un motor de reglas que permita crear e implementar lógica de negocio requerida definida por el dominio de afinidad
MPI-011	Debe proveer mecanismos de auditoria que permita gestionar el acceso a datos y funcionalidades, permitiendo auditor además todas las actualizaciones de registros.

3.2.3 REQUERIMIENTOS FUNCIONALES

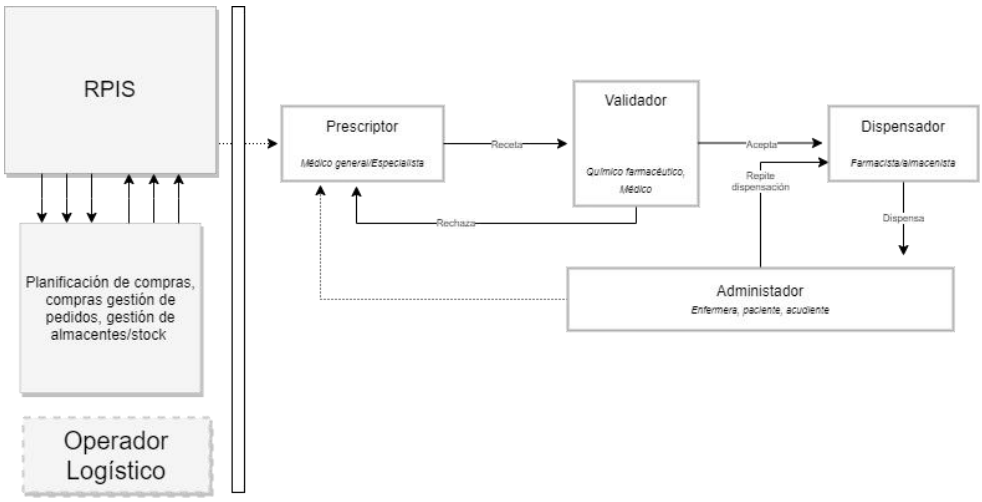
CONSIDERACIONES PARA LA IMPLEMENTACIÓN DE REQUERIMIENTOS FUNCIONALES Y DE INTEGRACIÓN

a) **Subdominios dentro del dominio de farmacia:** Dentro del alcance del proyecto se incluyen sólo los flujos del subdominio de farmacia comunitaria, del dominio de farmacia; esto es:

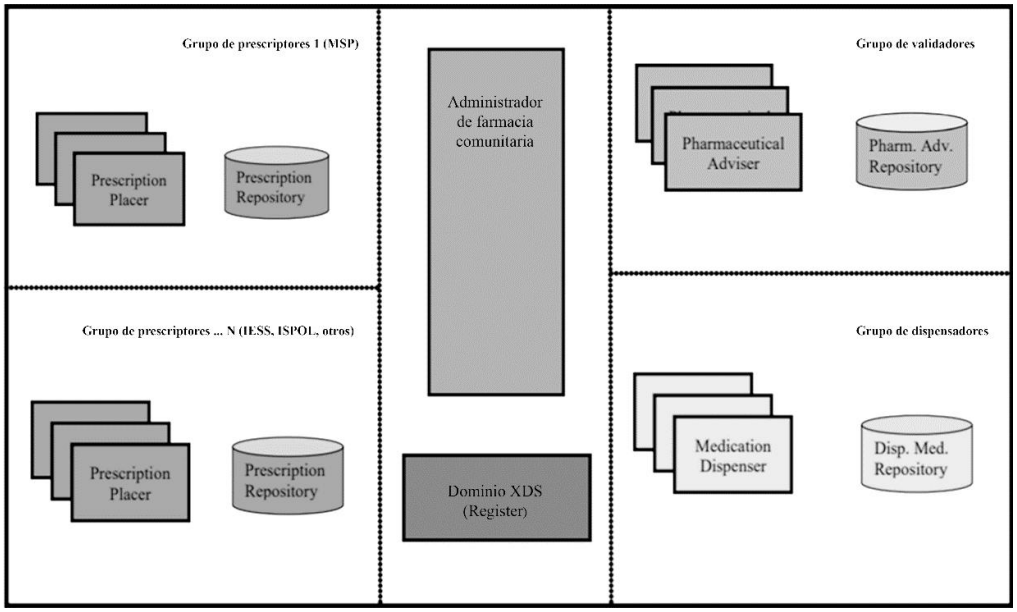
Subdominio de farmacia comunitaria:

- El paciente no está hospitalizado

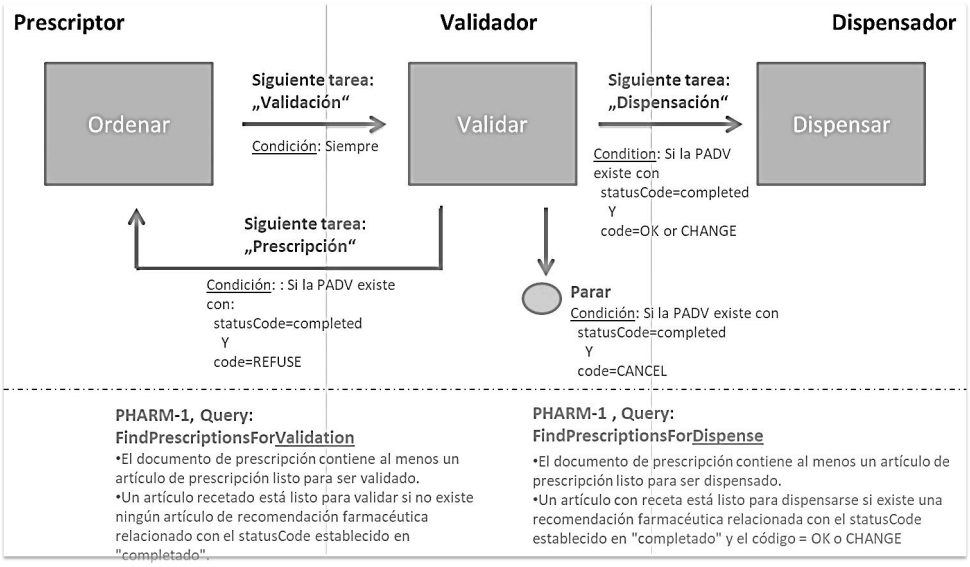
- El prescriptor es un profesional de la salud como: un médico de cabecera o médico familiar o un médico especialista, que prescribe desde un servicio o establecimiento ambulatorio o en un entorno de práctica privada
- El dispensador, en la mayoría de los casos, es un farmacéutico comunitario
- El administrador del medicamento, en la mayoría de los casos es el paciente, cuidador (enfermera, asistente o alguien de la familia). No se hace seguimiento a la adherencia/administración de la prescripción. El flujo general de la información en este subdominio se presenta a continuación:



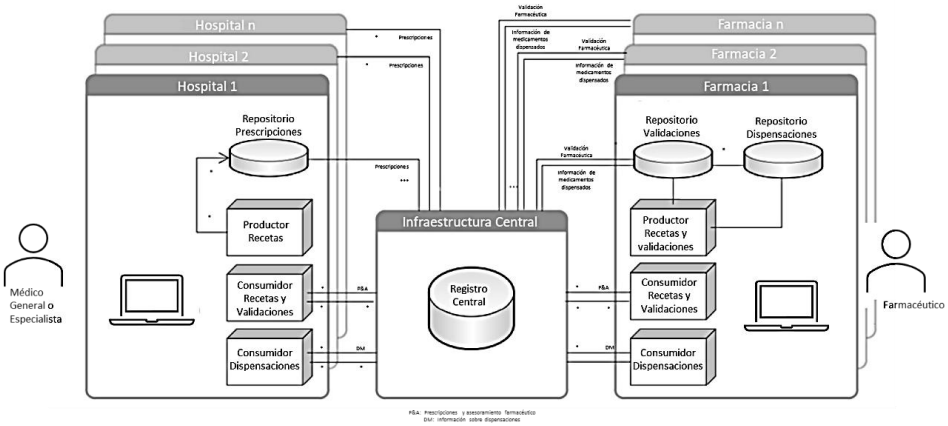
b) **Un solo dominio de afinidad para la RPIS:** Todas las entidades participantes actuarán dentro de un mismo dominio de afinidad, pues dado que el modelo de intercambio fue diseñado para un sistema de ámbito nacional, se requiere la gobernanza de este dominio, con el fin de establecer y asegurar reglas o políticas compartidas que la RPIS se debe cumplir.



c) El flujo de procesos de la farmacia comunitaria se puede diferenciar principalmente en dos escenarios de flujo de trabajo básicos, uno que incluye un paso de validación por parte de un asesor farmacéutico y otro que lo excluye: La solución deberá estar en capacidad de operar en ambos escenarios de flujo de trabajo:

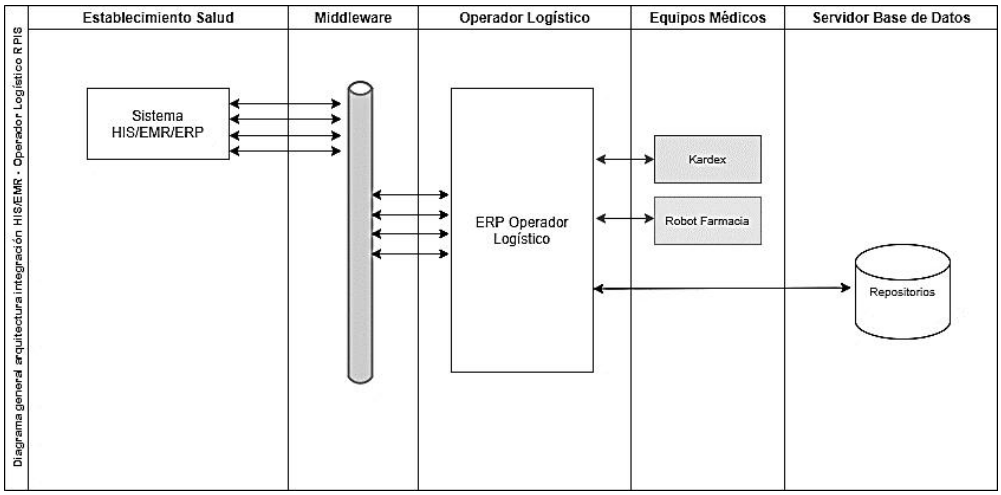


d) **Un modelo federado de registros y repositorios de prescripciones electrónicas en el subdominio de farmacias comunitarias** que garanticen a las entidades administrar y brindar la custodia de los registros médicos de sus afiliados y al mismo tiempo tener una vista completa de las prescripciones, validaciones, dispensación y administración de medicamentos cuando y donde sea necesario.



En este modelo de despliegue descentralizado, las prescripciones y los datos de dispensación se almacenan en la base de datos del sistema que los genera y / o registra. Estas bases de datos cubren el proceso empresarial del departamento, organización o grupo de organizaciones que utilizan el sistema. Cada organización sanitaria (dentro del dominio de afinidad) es responsable de la gestión de sus propias recetas y datos de dispensación.

Esto significa que los médicos y farmacéuticos necesitarán tener una forma de acceder a los datos en otros sistemas y necesitan poner sus datos a disposición de esos otros sistemas. Para ello, es necesario que exista una infraestructura que conecte los sistemas, ya sea a escala regional, nacional o internacional. Esta infraestructura puede contener un componente central (ESB) que actúa como índice y / o intermediario. Este componente almacena referencias a datos, siendo informado por los sistemas descentralizados sobre la existencia de datos a medida que son producidos.



e) Sistemas de prescripción electrónica: Los sistemas de prescripción electrónica son soluciones de software que permiten la creación de recetas digitales y las indicaciones para su administración. Cada entidad de la RPIS implementa estos sistemas de acuerdo con sus propias necesidades y prioridades, por lo tanto, el proceso de prescripción electrónica no está incluido dentro de este alcance, no obstante, el oferente debe considerar que las siguientes funcionalidades básicas de la prescripción electrónica están disponibles en los sistemas de información de las entidades:

- Buscar la medicación por principios activos o marca comercial: los profesionales deben poder buscar e indicar la medicación por su composición, las marcas comerciales pueden ser útiles para llegar a la composición genérica.
- Soportar la toma de decisiones para prevenir errores o potenciales eventos adversos como son: interacciones medicamentosas, alergias conocidas, efectos adversos pasados, contraindicaciones por patologías del paciente o resultados de laboratorios, rangos de dosis, ajustes por peso o función renal. De manera similar, algunos de estos sistemas de prescripción implementan controles para asegurar el cumplimiento de guías de práctica clínica, expresando la preferencia de algunos tratamientos sobre otros.

- Mantener una lista actualizada de medicación: los sistemas de prescripción deben contar con una lista de prescripciones activas del paciente, y con herramientas que permitan su actualización periódica. En este punto**, se requiere** que los sistemas de prescripción electrónica se puedan vincular a uno o más repositorios electrónicos de recetas e invocar los siguientes servicios de los repositorios para integrar garantizar la interoperabilidad de la receta electrónica entre las entidades de la red pública y el operador logístico:

- Consultar recetas en un repositorio de recetas: Permite conocer las prescripciones del paciente, conformando la lista de medicación activa del paciente.
- Agregar una receta en un repositorio de recetas: Desde los sistemas de prescripción de las entidades, se insertan nuevas recetas invocando este servicio del repositorio.
- Cancelar una receta en un repositorio de recetas: Permite al sistema de prescripción cancelar una receta existente, esto previene su dispensación a partir de ese momento.

- Este proceso no invalida los sistemas existentes de receta electrónica, estos seguirán funcionando en paralelo y se combinarán para ejecutar algunos pasos del proceso actual y de los relacionados con la interoperabilidad. Los sistemas existentes deberán incorporar estándares de la receta interoperable sin dejar de cumplir su función actual (ver detalle de requerimientos funcionales).

f) **Entrega de medicamentos a domicilio**: Se ha definido en Ecuador un grupo de pacientes especiales que, por su condición de vulnerabilidad, edad, riesgo, cronicidad, los medicamentos prescritos son dispensados directamente en su lugar de residencia. Se considera entonces dentro del operador logístico el servicio de "Delivery" que es gestionado a través del su sistema de información el permitirá administrar y operar la logística de la entrega de medicamentos a este tipo de pacientes.

g) **Dispensación Dirigida o Abierta**: Dependiendo de las políticas definidas por las Entidades de la Red, una prescripción puede estar dirigida a una farmacia específica (en este caso solo la farmacia a la que se envía puede dispensar la orden) o puede ser abierta, en cuyo caso el paciente podrá reclamar los medicamentos en la en la farmacia autorizada por su financiador, de su preferencia.

h) **Actores/ mensajes/recursos**: Se espera que el proponente incluya dentro de los servicios de consultoría funcional y técnica, al menos la implementación del siguiente conjunto de transacciones que permiten el intercambio de información relativa a prescripciones, dispensaciones de medicamentos y bienes estratégicos que intervienen en el circuito de prescripción para pacientes ambulatorios.

Nota: La implementación **preferiblemente** deberá estar basada en FHIR R4. A continuación, describiremos los elementos mínimos obligatorios que deberán intercambiarse mediante perfiles de recursos y extensiones FHIR: tipos de datos, vocabularios controlados y formatos XML y JSON, utilización de recursos usando tecnología REST y mensajes o documentos clínicos empleando arquitecturas basadas en servicios (servicios web Representational State Transfer (RESTful).

En caso de que el proveedor no cuente con el conocimiento técnico para la implementación a través de FHIR, puede presentar su propuesta de servicios usando el protocolo HL7 v2.7 o posterior con XML como formato canónico.

Actores

ACTOR	DESCRIPCIÓN
SISTEMA PRESCRIPTOR (PRES)	Sistema de información donde un profesional de la salud realiza las prescripciones al paciente. Este sistema está integrado normalmente con el sistema de Historia Clínica del Hospital y deberá integrarse con el repositorio de la farmacia comunitaria, donde además de notificar nuevas prescripciones, podrá modificar, cancelar, consultar, consultar las prescripciones activas del paciente, las dispensaciones, las anotaciones o consejos farmacéuticos generados durante el proceso de validación en las farmacias dispensadoras
SISTEMA DE GESTION DE FARMACIA (FARM)	Sistema de información del operador logístico, que opera en las farmacias comunitarias encargado de codificar las prescripciones (cuando estas vienen con códigos diferentes al del Catálogo Nacional de Medicamentos Básicos, o como principios activos o como ingredientes de una fórmula magistral). Adicionalmente hace el "picking" o preparación del pedido: Recepción del pedido confirmado, selección y recogida de los elementos necesarios para completar la orden de prescripción, actividades de embalaje de los artículos (cuando se requiere) y la programación del envío. Así mismo gestiona el stock de la farmacia. Cuando aplica, este sistema se encarga de validar o revisar las prescripciones activas del paciente y generar anotaciones o consejos al médico prescriptor alertando sobre posibles problemas relacionados con la medicación (interacciones entre principios activos, dosis máximas permitidas por período, dosis de toxicidad, concentración y los relacionados con la seguridad del paciente). Este último paso no es obligatorio en todas las farmacias, pero es deseable.
SISTEMA DE DISPENSACIÓN (DISP)	Una vez preparados y validados los medicamentos a dispensar, es el encargado de notificar la dispensación al repositorio y dejar la prescripción en estado de dispensación total o parcial, cuando no hay capacidad en el stock para surtir toda la orden.
CATÁLOGOS	**Medicamentos comerciales y genéricos/bienes estratégicos:** Cuadro Nacional de Medicamentos Básicos del Ecuador, 10ª revisión (2019).

	Profesionales de la Salud: utiliza ACCESS (Agencia de Aseguramiento de la Calidad de los Servicios de Salud y Medicina Prepagada) expuesto como el recurso FHIR Practitioner. **Establecimientos de Salud**: utiliza el Registro de la Red Pública Integral de Salud (RIPS, amparados en el Convenio Marco Interinstitucional) expuesta como el recurso FHIR Location y Organization, según corresponda. **Farmacias**: utiliza Registro Nacional de Farmacias, expuesto como como los recursos FHIR Location y Organization, según corresponda.
REPOSITORIO (REPO)	Sistema que registra todo el historial de las prescripciones, dispensaciones y cualquier evento relacionado con los tratamientos farmacoterapéuticos

Operaciones FHIR (Bus como mediador: (Servidor/Enrutador)

Operación	Acción	Comportamiento de los sistemas
GET Endpoint	Describe los detalles técnicos de una ubicación a la que se puede conectar para la entrega / recuperación de información.	**PRES, DISP,FARM:** Cliente **REPO:** Declara **BUS:** Servidor
GET MedicationRequest	Una orden o solicitud para el suministro del medicamento y las instrucciones para la administración del medicamento a un paciente. El recurso se llama "MedicationRequest" en lugar de "MedicationPrescription" o "MedicationOrder" para generalizar el uso en entornos de pacientes hospitalizados y ambulatorios, incluidos los planes de atención, y para armonizar con los patrones de flujo de trabajo.	**DISP:** Cliente **REPO**: Servidor **BUS:** Rutea
POST MedicationRequest	Registra la receta. Crea una orden de medicamento (la receta electrónica solo tendrá un medicamento por receta para evitar la posibilidad de dispensaciones parciales)	**PRES:** Cliente **REPO:** Servidor **BUS:** Rutea
PUT MedicationRequest	Cancelar receta	**PRES:** Cliente **REPO:** Servidor **BUS:** Rutea

POST MedicationDispense	Registra dispensación de la receta	DISP: Cliente REPO: Servidor BUS: Rutea
PUT MedicationDispense	Cancela el registro de dispensación de una receta	**DISP:** Cliente **REPO:** Servidor **BUS:** Rutea

o Mensajes HL7

Mensaje	Evento	Origen /Destino
OMP^O09	Crear, cancelar o modificar una prescripción	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
ORP^O10	ACK (Creación/Modificación/cancelación de prescripción)	
RDE^O11	Prescripción validada/codificada/con sustitución (si es permitida) o rechazada	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
RRE^O12	ACK Validación	
RDS^O13	Notificación de dispensación	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
RRD^O14	ACK Dispensación	
RAS^O17	Cancelación de dispensación	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
RRA^O18	ACK Cancelación de dispensación	
QBP^Q31	Consulta lista de tratamientos activos	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
QBP^Z01	Consultar una prescripción	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
ORP^010	ACK consulta de prescripción	
QBP^Q31	Consultar dispensaciones	**PRES:** Cliente (Sender) **REPO:** Servidor **BUS:** Rutea
RSP^K31	ACK consulta dispensaciones	

- **Gestión de catálogos:** Este perfil detalla la mensajería para todos los mensajes que tengan que ver con información relativa al mantenimiento de catálogos en los sistemas de información de la RPIS:

ACTOR	DESCRIPCIÓN
SISTEMA GESTOR DE CATÁLOGO	Sistema de información que gestiona de forma absoluta la estructura y composición de cada registro en un catálogo
SISTEMA USUARIO DE CATÁLOGO	Sistema que desea conocer la estructura y el contenido de un catálogo

- **Mensajes (Algunos ejemplos)**

Mensaje	Evento	Origen /Destino
MFN^Z05	Actualización de datos de ubicación de un centro asistencial	**GESTOR LOCALIZCIONES - USUARIO**
MFN^Z15	Actualización de datos de un material	GESTOR MATERIALES-USUARIO
MFK^XXX	Imposible procesar una actualización de catálogo	**USUARIO-GESTOR DE CATÁLOGO**

Master Patiente Index:

- Actores

ACTOR	DESCRIPCIÓN
Patient identity source	Genera la notificación de los eventos de la actualización de información de identificación de un Paciente al Patient Identifier Cross-reference Manager
Patient identity consumer	Determina la identificación de un paciente en diferentes dominios usando los servicios del Patient Identifier Cross-Reference Manager.
Patient identity consumer	Gestiona la identificación cruzada de paciente en diferentes dominios, basado en la información que recibe de los Patient identity Source. Gestiona las consultas

- Transacciones

Transacción	DESCRIPCIÓN

ITI – 8	Patient Identity Feed: La transacción ITI-8 IHE, que es utilizada por los actores PIX Manager y PIX Source IHE para crear, actualizar y eliminar registros de pacientes, se puede auditar utilizando un nodo ATNAAudit
ITI – 9	PIX Query: se acciona cuando uno de los dominios en el sistema PIX/PDQ solicita una lista de identificadores del paciente que se asocian a un identificador específico del paciente. Esta solicitud es procesada por el índice maestro, que responde con una lista de identificadores de paciente asociados si existen.
ITI – 10	PIX Update Notification: se produce cuando los datos clave de un registro de paciente son actualizados por un dominio en el índice maestro, que luego difunde la actualización para que estén disponibles para todos los dominios interesados.

Dado el contexto anterior, el oferente debe estar en capacidad de desarrollar las siguientes integraciones a través del ESB, encargado de recibir, procesar y enrutar los mensajes que interactúen con los componentes del sistema utilizando protocolos y estándares de interoperabilidad y los específicos en el ámbito de la prescripción y dispensación de medicamentos y bienes estratégicos. A su vez, este puede transformar, validar, integrar y realizar acciones de enrutamiento sobre mensajes que provienen de las aplicaciones que interactúan con él.

Dentro del bus de interoperabilidad se deberán definir diferentes puertos de origen y de destino sobre los cuales se publican los servicios para el intercambio de información utilizando las recomendaciones, perfiles y estándares internacionales de interoperabilidad en salud.

1	Insertar/Modificar Prescripción (Sistema Asistencial -> Repositorio)	Una prescripción, junto con las recetas necesarias para cumplir esa prescripción, se inserta en el repositorio. Así mismo, se puede modificar una prescripción previamente insertada. La prescripción puede o no estar direccionada a una farmacia o punto de dispensación específico.	PRES	REPO
2	Anular Prescripción (Sistema Asistencial -> Repositorio)	Desde el sistema asistencial se podrá anular en cualquier momento una prescripción, así como las recetas que dependen de esa prescripción.	PRES	REPO
3	Consulta de administración; tratamientos y recetas. (Sistema Asistencial -> Repositorio)	Desde el sistema asistencial se podrá realizar en cualquier momento una consulta de administración correspondiente a recetas o tratamientos.	PRES	REPO

4	Resolución de validación; (Validación -> Sistema Asistencial)	Desde el sistema de validación de prescripciones se aprobará o denegará la prescripción (a través de mensajes con consejos farmacéuticos al prescriptor)	FARM	PRES
5	Propuesta de anulación de una prescripción (Validación -> Sistema Asistencial)	En cualquier momento de la vida de la prescripción el validador podrá generar propuestas de anulación de la prescripción y las recetas correspondientes	FARM	PRES
6	Modificación de tratamientos; (Validación -> Sistema Asistencial)	En cualquier momento de la vida de la prescripción desde Validación Farmacéutica se podrá solicitar modificar una prescripción y las recetas correspondientes	FARM	PRES
7	Consulta de lista de prescripciones existentes y no dispensadas para un paciente (Dispensación -> Repositorio)	Desde la Farmacia Hospitalaria se podrá solicitar en cualquier momento una lista de prescripciones existentes para un paciente	DISP	REPO
8	Información de la dispensación realizada para una prescripción identificada por Nº de prescripción. (Dispensación -> REP)	La Farmacia podrá solicitar información de la dispensación al Repositorio cuando lo estime oportuno.	DISP	REPO
9	Cancelar una receta; (Sistema asistencial -> Repositorio)	A través de este servicio se podrá cancelar una receta sin borrarla (ponerla en estado “cancelado”) previniendo su dispensación; esta funcionalidad se requiere cuando un profesional médico modifica los tratamientos y define la cancelación de una receta y la creación de nuevas.	PRES	REPO
10	Respuesta de cancelación de una receta, (Farmacia/Dispensación Prescripción	La farmacia transmite una respuesta indicando si la cancelación fue exitosa, de acuerdo con lo solicitado	DISP	REPO
	Notificación de cancelación de dispensación; Farmacia/Dispensación Prescripción	Una farmacia notifica al médico que prescribe que se ha revertido una dispensación procesada previamente (p. Ej., El paciente no recogió el medicamento).	DISP	PRES
11	Buscar receta por número identificador de la receta (Farmacia/Dispensación/Prescripción -> Repositorio)	Recibe como parámetro el número identificador de la receta y retorna su contenido.	DISP/FARM	REPO

12	Buscar recetas por número de identificación de pacientes (Farmacia/Dispensación/Prescripción -> Repositorio)	Recibe como parámetro la identificación del paciente y retorna, de acuerdo a los parámetros de entrada, las prescripciones activas, las prescripciones pendientes de dispensar, las dispensadas parcial, las dispensadas completas, las recetas canceladas, las recetas vencidas, las recetas con validaciones.	DISP/FARM	REPO
13	Actualizar Dispensación (Farmacia/Dispensación -> Repositorio)	Este servicio se utiliza cuando se registra una dispensación total o parcial de una receta y actualizar su estado, de tal manera que se evite la posibilidad de dispensar más de una vez la misma receta, considerando que el repositorio se convierte en la única fuente del estado actual de la receta.	DISP	REPO
14	Gestión de estados de la receta (Sistema Asistencial, Farmacia/Dispensación -> Repositorio	El sistema debe manejar de manera automática los diferentes estados por los que pasa una receta, dependiendo del actor o estación donde ésta se encuentre y la acción que ellos ejecuten sobre ella: ● Borrador: No es válida para dispensar. Es el estado inicial de la receta que puede ser consultada y validada su estructura ● Solicitada: Estado de la receta cuando el profesional confirma su emisión en el sistema de prescripción y queda apta para ser dispensada. ● Dispensada Total: Cuando todos los productos que contiene la receta fueron dispensados totalmente. Una receta en este estado ya no estará más disponible para dispensaciones futuras. ● Vencida: Cuando la fecha de validez de la receta se cumple, la receta debe pasar a este estado y no debe poderse dispensar. ● Cancelada: Cuando fue cancelada por un profesional y no puede generarse en consecuencia, ninguna dispensación.	FARM/DISP/PRES	REPO

Detalle de requerimientos funcionales

No.	Descripción del requerimiento
RF-001	El proveedor debe integrar las aplicaciones de usuario (prescripción, validación, dispensación) con el Directorio Activo actual o el que se implemente en la RPIS para la autenticación y autorización del usuario.
RF-002	El proveedor integrará todas las aplicaciones de usuario con el Gestor de Identidades de la RPIS para la solicitud y asignación de permisos.
RF-003	La autorización de accesos a los sistemas finales se aprovisionará desde la Gestión de identidades de la RPIS
RF-004	Se requiere que proveedor implemente una solución Single Sign On (SSO), de forma que el usuario no deba volver a Autenticarse si ya lo ha hecho en los sistemas sus sistemas asistenciales o logísticos (HIS, dispensación del operador logístico, por ejemplo).
RF-005	Todas las aplicaciones de usuario deberán generar traza (logs) de las acciones llevadas a cabo dentro de la(s) misma(s).
RF-006	Las plataformas y soluciones a implementar deberán generar como mínimo un log de auditoría donde se registre todas las actividades asociadas a los usuarios del sistema, acceso a información sensible y eventos de seguridad de interés. Este log deberá estar protegido contra eliminación o modificaciones y deberá ajustarse a la estructura definida por el área de Seguridad de la información del MSP.
RF-007	De manera general el proveedor deberá desarrollar componentes funcionales que permitan al usuario: ● La consulta del identificador único del paciente dentro del Sistema de Interoperabilidad de Prescripción / Dispensación. ● Localización de prescripciones, dispensación y validaciones a través del identificador del paciente o el número unívoco de la receta electrónica ● Adicionar registros: servicio que se utiliza para adicionar prescripciones, dispensaciones, validaciones y eventos relacionados con la prescripción y la dispensación ● Consumir servicios: muestra prescripciones, dispensaciones, validaciones al solicitante que envía los parámetros específicos para su despliegue
RF-008	La componente de MPI debe mantener un registro central de todos los pacientes y sus características demográficas y asignar un identificador único para cada paciente
RF-009	La solución de MPI deberá detectar errores de asignación de identificador junto con herramientas para resolución de dichos errores: Debe proveer funcionalidades que permitan eliminar las entradas duplicadas de registro de pacientes derivados de errores de entrada de datos durante el registro, falta de información demográfica o cambios en su demografía.
RF-010	El MPI deberá proporcionar servicio de localización de registros, permitiendo a los prescriptores, validadores y dispensadores del dominio de afinidad consultar las prescripciones, dispensaciones y otros eventos relacionados con las recetas de los pacientes
RF-005	El MPI usará mensajería de los perfiles PIX/PDQ de IHE para los procesos de actualización, consulta y modificación de los datos del MPI
RF-006	El MPI usará algoritmos determinísticos y probabilísticos para la búsqueda de registros similares

RF-007	El MPI permitirá comparaciones utilizando librerías fonéticas en español sobre las cadenas de texto. El algoritmo fonético atenderá los problemas típicos debidos a errores de ortografía o nombres étnicos.
RF-008	Las búsquedas en el Master Patient Index pueden ser realizadas usando datos demográficos o la identificación del paciente. Una lista de pacientes encontrados de acuerdo con los criterios de entrada es desplegada y el paciente puede ser seleccionado para procesos posteriores.
RF-009	Permite insertar un nuevo paciente: Los datos son enviados al repositorio central de índice de Pacientes, donde son validados. Un identificador nuevo para el dominio de afinidad XDS (Cross-Enterprise Document Sharing) es automáticamente creado, si éste no existe. En caso de que el paciente coincida con otro existente en el maestro, éste es vinculado o insertado automáticamente a una lista de potenciales duplicados, que pueden ser gestionados en procesos posteriores
RF-010	Actualizar datos del paciente: Los datos demográficos de un paciente pueden ser modificados y enviados al Master Patient Index en cualquier momento
RF-011	El sistema permitirá, para los casos en que se descubra que un paciente tiene más de un número de identificación, la combinación de los documentos de prescripción de dichos números de identificación con el elegido.
RF-012	El Índice Maestro de Pacientes se mantendrá de manera centralizada permitiendo el acceso de hospitales y clínicas individuales a la última versión global del índice.
RF-013	El MPI se implementará como un "servidor de identificación de pacientes" que permitirá que otras aplicaciones (suministradas por las entidades de la RPIS) interactúen con el MPI para obtener la identificación del paciente o sus datos demográficos. Esta interacción se realizará a través de una interfaz definida y documentada, preferiblemente implementada a través de un esquema de mensajería estándar como HL-7 y ebXML.
RF-014	El usuario se autentica en el sistema de la entidad y se aplican las políticas de autenticación y autorización previstas. Los servicios que proveen la funcionalidad requerida serán consumidos por las aplicaciones de las entidades de la RPIS.
RF-015	La solución propuesta, a nivel de seguridad de las aplicaciones de usuario, debe preservar las restricciones de los sistemas origen: los sistemas origen enviarán toda la información que se defina y el nivel de seguridad sobre la misma. Los requisitos de seguridad a implantar serán los establecidos para sistemas de nivel alto en el marco legal vigente, así como las Políticas, Normas, Estándares y lineamientos de Seguridad del MPS y las leyes de protección de datos de Ecuador, entre otros que apliquen en el país.
RF-016	La solución, en todos sus componentes (repositorios, aplicaciones) deberá cumplir con las dimensiones: Disponibilidad, Autenticidad, Integridad, Confidencialidad y Trazabilidad en el procesamiento, almacenamiento y transporte de la información.
RF-017	La solución propuesta deberá permitir la explotación de datos anonimizada y no anonimizada. El MSP será quien decida las situaciones en que se anonimice la información con base en los protocolos de seguridad de la información de la RPIS
RF-018	En cualquier caso, en todos los desarrollos e integraciones el proveedor deberá atender lo establecido por la normativa y arquitectura de seguridad vigente en la RPIS y las mejores prácticas internacionales de seguridad para desarrollo de aplicaciones (por ejemplo, OWASP, OSSTMM).

RF-019	Los sistemas propuestos incorporarán una herramienta de gestión de las auditorías de accesos y control de cambios, tanto los realizados a través de los aplicativos como los realizados directamente a las bases de datos, sobre la información almacenada.
RF-020	El sistema de la RPIS asume la función de identificación, autenticación y validación de los permisos de acceso de sus profesionales, certificando electrónicamente estos procesos hacia la plataforma de interoperabilidad.
RF-021	El sistema debe permitir interactuar con los sistemas de información de la RPIS y con el sistema del operador logístico, permitiendo la trazabilidad del registro, control y seguimiento de las solicitudes de entrega de medicamentos y bienes estratégicos ambulatorios realizadas en la red pública y en el operador de medicamentos. La integración de la información se debe realizar mediante mensajería estándar entre las entidades participantes preferiblemente HL7 FHIR
RF-022	Recibir órdenes de medicamentos y/o bienes estratégicos enviadas por los sistemas de prescripción de la RPIS y disponibilizarlo para procesos posteriores. Registrar los eventos de dispensación de medicamentos y bienes estratégicos dispuesto por el operador logístico
RF-023	Permitir la trazabilidad en los cambios de estados de las prescripciones y registros de dispensación de medicamentos y bienes estratégicos, asegurando la persistencia de la información.
RF-024	Permitir realizar proceso de auditoría que cumpla con la recomendación del perfil ATNA de IHE
RF-025	Debe soportar al menos los siguientes mensajes: Prescripción: ● Crear nueva receta ● Detener receta ● Mantener/prorrogar una prescripción ● Revocar el permiso de dispensación ● Modificar una prescripción ● Eliminar o cancelar una prescripción Dispensación ● Surtir receta ● Transferencia de receta (cuando una prescripción está dirigida y la farmacia no cuenta con stock para surtirla) ● Cancelar dispensación ● Registrar dispensación parcial (cuando aplique) Funciones comunes ● Solicitud de retractación ● Agregar notas (prescripción, validación, dispensación) ● Remover notas ● Consultar notas Consultas (pacientes) ● Obtener dispensaciones para una receta de medicamentos ● Obtener detalles de dispensación de un solo medicamento ● Obtener detalles de la medicación del paciente ● Obtener resumen de medicamentos para el paciente ● Obtener consulta genérica de perfil de medicación ● Obtener contraindicaciones de medicamentos para pacientes ● Obtener el historial de dispensación de medicamentos del paciente ● Obtener recetas para pacientes, nunca dispensadas ● Obtener recetas para pacientes con las dispensaciones restantes ● Obtener el resumen del pedido de medicamentos recetados para el paciente ● Obtenga listado de medicamentos recetados sin dispensación ● Obtener listado de prescripciones vencidas

	● Obtener listado de prescripciones canceladas ● Obtener historial de eventos de prescripción de medicamentos Consultar medicamentos (por diferentes criterios Alergias/intolerancias • Agregar/actualizar alergia, intolerancia • Consultar alergias e intolerancias de los pacientes • Historial de cambios en alergias/intolerancias
RF-026	● Crear orden de dispositivo o bien estratégico ● Dispensar orden de dispositivo o bien estratégico ● Buscar dispensaciones ● Buscar histórico de dispensaciones por paciente
RF-027	El sistema debe generar un identificador univoco de receta electrónica, el cual será usado para acceder a su contenido en los diferentes procesos del ciclo de prescripción-dispensación. La estructura del identificador será creada mediante el uso de reglas establecidas en el estándar ISO 9834 (OID). Esta estructura deberá incluir información de la red que genera la receta (MPS, IESS, ISPOL, ISFA), la identificación del grupo (cuando se prescriben varias recetas en un mismo evento de salud) y la identificación del medicamento, el cual será diferente para cada medicamento indicado. El sistema deberá generar un código de barras o código QR con el cual el paciente puede reclamar los medicamentos en la farmacia indicada o en la preferida, según aplique. La farmacia tendrá la capacidad de leer el código generado o ingresarlo manualmente (el código QR/Barras se generará con su identificación legible por el humano) y recuperar la receta a dispensar.
RF-027	La prescripción electrónica deberá contener los datos mínimos del paciente, de acuerdo con la identificación unívoca de personas (Ver requerimientos del EMPI)
RF-028	Los medicamentos prescritos deberán estar codificados en su representación genérica, según el Cuadro Nacional de medicamentos básicos, especificando para cada uno de ellos la concentración, forma farmacéutica, principios activos, la presentación y la cantidad. Puede contener opcionalmente la marca comercial si dentro del proceso de implementación, se considera pertinente. Adicionalmente debe indicarse la frecuencia, la vía de administración, la dosis por frecuencia, el tiempo y las indicaciones. La información debe ser legible por un humano: paciente, cuidador o profesional que lo administra
RF-029	El sistema puede permitir, pero no exigir, que se complete el motivo de la prescripción. Donde esté poblado, debe representarse como un valor codificado CIE 10 o SNOMED CT. Cuando el motivo de la prescripción (indicación clínica) se incluye como un valor codificado, el sistema DEBE incluir también el motivo de la prescripción como un campo de texto (legible por humanos)
RF-030	La receta electrónica debe contener datos de validez como son la fecha de inicio del tratamiento, el vencimiento de la receta (una receta vencida no podrá ser modificada, cancelada ni dispensada).
RF-031	Datos del prescriptor, la entidad de salud desde donde se genera (según el catálogo de entidades de salud provistos por el ACCESS), la fecha y la hora de la generación de la prescripción.
RF-032	Cuando la prescripción debe ser dispensada en una farmacia específica, la prescripción electrónica debe proveer el código de la farmacia de acuerdo con el catálogo de farmacias provisto por el Registro Nacional de Farmacias.

RF-033	El sistema también DEBE admitir e incluir (si aplica) en la receta Electrónica en número de referencia de autorización por parte del financiador (hasta 25 caracteres alfanuméricos). Nota: todos los financiadores utilizan el mismo concepto de número de autorización y el número de autorización realiza la misma función en todas las financiadoras. Los sistemas y las bases de datos pueden utilizar el mismo campo / atributo, pero debe presentarse de acuerdo con lo definido por cada entidad.
RF-034	Todas las recetas electrónicas deben tener una firma digital, a través de mecanismos que cumplan con las normativas de Firma electrónica en el Ecuador (Acuerdo Ministerial 0084 del 13 de noviembre del 2020) o la normativa legal vigente. La firma está asociada al profesional que hace la prescripción asegurando la autoría y la inmutabilidad del contenido.
RF-035	Cuando se dispensa la receta electrónica, se deben adicionar a ésta, los datos de la farmacia donde fue dispensada (de acuerdo al catálogo), la fecha y hora de la dispensación, producto dispensado, cantidad y si fue completa o parcial (en el caso de una receta electrónica por medicamento prescrito, la dispensación parcial no debería existir, sin embargo, puede ser una decisión del proyecto o una política de alguna entidad. El sistema debe soportar ambos escenarios)
RF-036	Se debe mantener actualizado el estado de una receta electrónica según la estación donde esta se encuentre: borrador, solicitada, dispensada, cancelada, modificada, vencida.
RF-037	A nivel de estándares usados en la receta electrónica se deben considerar al menos, los siguientes: ● Cuadro Nacional de Medicamentos Básicos (CNMB), que incluye principios activos, formas farmacéuticas, concentración, presentación, diagnósticos relacionados ● índice Nacional de Pacientes (EMPI), que gestiona la identificación y datos demográficos de los pacientes, de acuerdo con los especificado en este documento de requerimientos, (indispensable para la interoperabilidad que se prescriba, dispense y administre la medicación al paciente correcto). ● Estructura de documentos electrónicos con recursos HL7 FHIR o HL7 v2.x según capacidades del oferente ● Comunicación de información a través de API´s REST basada en perfiles IHE o SOAP basada en IHE, según capacidad del oferente
RF-038	Se deberán implementar mecanismos para asegurar que el acceso a las recetas solo ocurre cuando el paciente, responsable o familiar a cargo, está presente y lo autoriza. Todos los accesos a recetas digitales a través del Bus de Interoperabilidad del MSP serán registrados para su auditoría, sin guardar información del contenido de las recetas.
RF-039	Toda la información generada desde el proceso de prescripción (generación de una nueva receta, modificación, cancelación, repetición) debe generar un registro de auditoría con los detalles que permitan recuperar la receta y las novedades registradas durante su ciclo de vida.
RF-040	Al transmitir una receta electrónica, el software DEBE asegurarse de que la transmisión incluya: a) Un componente de metadatos y b) Un componente de prescripción. Nota: El componente de metadatos es el encabezado/ contenedor que permite la identificación e indexación del componente de prescripción. El componente de prescripción a menudo se denomina "carga útil".
RF-041	El componente de metadatos de toda receta electrónica SERÁ: a) Desencriptado cuando está en reposo y; b) Cifrado cuando está en tránsito;
RF-042	El componente de metadatos de cada receta electrónica DEBERÁ contener al menos: a) El número de receta único para esa receta (ID de receta única a nivel nacional) y; El ID de conformidad de cada sistema de información utilizado para generar, enviar,

	recibir, almacenar o procesar la receta electrónica y; la identificación UNIVOCA del paciente a quien se prescribe
RF-043	Independientemente de la inclusión de cualquier valor codificable, el sistema DEBERÁ incluir todos los campos de información presentados al prescriptor en el "Texto original". Nota: El farmacéutico clínico / supervisor ve las instrucciones como se muestran al prescriptor cuando el prescriptor escribió la prescripción. "Texto original" se define como el texto "exactamente como se presenta al prescriptor o dispensador".
RF-044	Después de la finalización, cuando se ha enviado una receta electrónica al Repositorio como una receta electrónica, el sistema DEBE proporcionar un mecanismo para que el prescriptor corrija una receta si lo requiere. Nota: una receta que se ha dispensado no se puede corregir ni cancelar. Las repeticiones pendientes aún se pueden cancelar, dependiendo de la funcionalidad requerida.
RF-045	El sistema DEBERÁ almacenar, de forma permanente e inalterable dentro del repositorio de medicamentos para quién se realizó la prescripción electrónica, generado los detalles de cualquier receta electrónica almacenada, de conformidad con y según lo requieran las regulaciones aplicables. Nota: Las regulaciones de Ecuador requieren que los detalles de la prescripción se conserven durante al menos siete años.
RF-046	El sistema DEBE mostrar la receta electrónica en un formato que cumpla con los requisitos de las Regulaciones Nacionales y la legislación relevante al prescriptor (RPIS) y devolver el ACK o indicación de acusado recibo de la receta electrónica desde el repositorio. Los datos del acuso de recibo deben registrarse permitiendo auditorías posteriores.
RF-047	Toda la transmisión de información de prescripción electrónica a través de redes públicas DEBERÁ cifrarse utilizando algoritmos criptográficos válidos en Ecuador.
RF-048	El sistema DEBE permitir al usuario emitir una cancelación de una receta electrónica después del acuse de recibo. Nota: Se entiende que la cancelación puede no surtir efecto si la receta electrónica ya ha sido dispensada o transferida a entregada al servicio de Delivery.
RF-049	Con la lectura del código QR/barras o la digitación del número de la prescripción, el dispensador podrá recuperar la receta para su dispensación: La prescripción electrónica original; la dispensación más reciente (si corresponde) y todas las anotaciones (si las hay).
RF-050	El sistema DEBE mostrar todos los elementos de datos como se muestra al prescriptor, independientemente de la presencia o no de campos de información codificados.
RF-051	El sistema DEBE indicar claramente al usuario si el prescriptor ha especificado que no se permite la sustitución de marca.
RF-052	El sistema permite la notificación de la dispensación en el repositorio, el cambio de estado de la receta y devolverá el ACK, cuyos datos deberán registrarse para auditorías posteriores.
RF-053	Después de la finalización, cuando se ha enviado un registro de dispensación al repositorio, el sistema DEBE proporcionar un mecanismo para que el dispensador corrija un registro de dispensación si el dispensador lo necesita.

RF-054	El sistema DEBE poder enviar un mensaje que refleje una anotación al repositorio como parte de la actividad de dispensación (proceso de validación, por ejemplo)
RF-055	El sistema DEBE comunicar una inversión de dispensación al repositorio. Nota: Puede haber casos en los que un dispensador deba revertir un evento de dispensación después de que se haya publicado un aviso de dispensación en el repositorio (por ejemplo, el paciente rechaza el suministro). En este caso, después del evento de dispensación, se requiere que el dispensador invierta el evento de dispensación y devuelva el registro de prescripción electrónica a un estado desbloqueado. El resultado es que la receta es válida para dispensar.
RF-56	Si el repositorio no está disponible o no responde, el sistema DEBERÁ poner en cola los mensajes y volver a intentarlo hasta que el repositorio acuse recibo.
RF-57	El sistema NO DEBE aceptar recetas electrónicas ni dispensar notificaciones de sistemas no conformes.
RF-58	El sistema NO DEBE proporcionar información de prescripción electrónica ni dispensar información a un sistema no conforme
RF-59	El sistema DEBE verificar la autenticidad del solicitante para todas las solicitudes de conexión a través de redes públicas que utilizan la infraestructura de clave pública (PKI). Nota: el sistema no aceptará conexiones de participantes desconocidos. Los requisitos de conformidad se actualizarán si cambian los métodos de autenticación aprobados.
RF-60	El sistema DEBE registrar cada transacción en un registro de auditoría. Los detalles del registro DEBERÁN incluir: Fecha y hora de creación (hora y zona horaria); Tipo de transacción; Estado de la transacción (por ejemplo, "Aceptada", "Rechazada"); Razón del rechazo (si se rechaza); Identificador del sistema de envío / solicitud; El identificador de recetas único a nivel nacional; Fecha y hora de reconocimiento (hora y zona horaria) si corresponde; y Todos los campos de información contenidos en los metadatos del mensaje. Nota: La gestión de eventos e información de seguridad (SIEM) debe utilizarse para identificar intentos de acceso no autorizado. Esto debería generar un incidente para la investigación cuando se identifica un número mínimo de intentos.
RF-61	El sistema, previa solicitud, generará un archivo o archivos que contengan la información capturada en los registros de auditoría en formato legible por humanos. Nota: este requisito permite la generación de un archivo o archivos que se pueden compartir o enviar a los organismos reguladores pertinentes a pedido. Los "formatos legibles por humanos" incluyen archivos de texto, archivos PDF, archivos de registro o cualquier otro formato que presente la información requerida de manera clara
RF-062	Cuando un sistema de dispensación recupera una receta electrónica, el sistema DEBE poder recopilar y proporcionar toda la información relevante, incluyendo: • Receta electrónica original; • Registro de dispensación más reciente; y • Todas las anotaciones

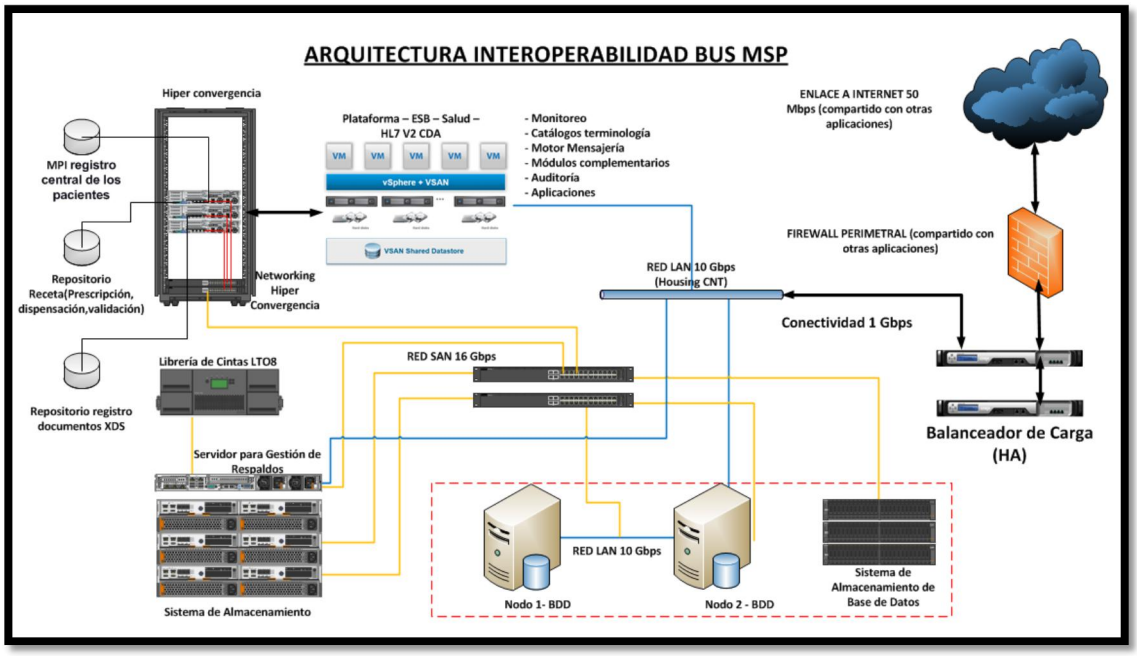
RF-063	Cuando un sistema de dispensación recupera una receta electrónica, el sistema DEBE bloquear esa receta electrónica mientras la transacción está en curso para evitar múltiples transacciones simultáneas.
RF-064	El sistema DEBE aceptar recetas electrónicas de sistemas de prescripción que proporcionen una identificación de conformidad válida de una organización con la que tengan un acuerdo contractual.
RF-065	El sistema DEBE proporcionar un acuse de recibo de una receta electrónica al sistema de prescripción.
RF-066	El sistema DEBE aceptar y procesar una solicitud de cancelación de una receta electrónica.
RF-067	El sistema DEBE proporcionar un acuse de recibo de una solicitud de cancelación de receta electrónica y el resultado de esa solicitud al sistema de prescripción.
RF-068	El sistema DEBE aceptar una notificación de dispensación contra una receta electrónica
RF-069	El sistema DEBE proporcionar un acuse de recibo de un Registro de dispensación al sistema de dispensación.
RF-070	El sistema DEBE aceptar una anotación realizada por un dispensador contra una receta electrónica como parte del evento de dispensación.
RF-071	El sistema DEBE proporcionar un acuse de recibo de una anotación al sistema de dispensación.
RF-072	El sistema DEBE aceptar y procesar una notificación de cancelación de suministro. Nota: Puede haber casos en los que se requiera que un distribuidor abandone un evento de suministro antes de que se publique un aviso de suministro en el repositorio (por ejemplo, el medicamento está agotado). En este caso, después de que cese el evento de dispensación, el registro de prescripción electrónica debe volver a un estado desbloqueado. El resultado es que la receta es válida para dispensar
RF-074	El sistema DEBE aceptar y procesar una notificación de reversión de suministro. Nota: Puede haber casos en los que un dispensador deba revertir un evento de suministro después de que se haya publicado un aviso de suministro en el repositorio (por ejemplo, el paciente rechaza el suministro). En este caso, después del evento de dispensación, se requiere que el dispensador invierta el evento de dispensación y devuelva el registro de prescripción electrónica a un estado desbloqueado. El resultado es que la receta es válida para dispensar.
RF-075	El sistema DEBE desbloquear una receta electrónica cuando el sistema de dispensación la libere (sin cambios). Nota: Cuando el sistema de dispensación libera una receta electrónica sin un aviso de dispensación (es decir, no dispensa), la receta se desbloqueará. Esta prescripción no se modificará con respecto a la originalmente extraída por el dispensador.
RF-076	El sistema DEBE facilitar el intercambio de recetas electrónicas entre las farmacias del operador logísticos conformes
RF-077	Cada sistema DEBE gestionar el proceso de seguridad de repositorio conectado para facilitar la recepción y entrega de recetas electrónicas

RF-078	El sistema DEBERÁ garantizar que los controles de privacidad del repositorio se mantengan durante el proceso de entrega al sistema de dispensación solicitante.
RF-079	Cuando un sistema solicita una receta electrónica al repositorio, el sistema DEBERÁ garantizar que el dispensador solicitante u otro usuario es un punto final registrado y conocido y el sistema puede afirmar la validez del usuario.
RF-080	El sistema y el operador del repositorio NO DEBEN cambiar ni manipular el contenido semántico (metadatos o carga útil cifrada) de ningún mensaje.
RF-081	El sistema DEBE cifrar todos los datos de prescripción electrónica en tránsito a través de la red pública entre todos los puntos finales autorizados y en reposo. Nota: Los puntos finales son cualquier organización que envía o recibe información hacia / desde el repositorio que ha sido autorizada para hacerlo. Tenga en cuenta que todos los datos "en tránsito a través de una red pública" deben estar cifrados. Esto incluye tanto los metadatos como la carga útil de prescripción electrónica.
RF-082	El sistema NO DEBE exponer la carga útil no cifrada al operador o usuario del sistema repositorio cuando esté en operaciones normales. Nota: en circunstancias normales, el sistema prohibirá el acceso a la carga útil no cifrada al personal o técnicos a través de una interfaz de usuario, conexión remota, exportación de datos o por cualquier otro medio. La imposibilidad técnica de acceder a datos no cifrados protege la privacidad del paciente. El sistema puede necesitar exponer cargas útiles no cifradas internamente para mantenimiento, búsqueda de fallas, investigaciones autorizadas o por orden legal.
RF-083	El sistema NO DEBE compartir la carga útil con otros sistemas internos o externos a menos que: Estos sistemas receptores están cubiertos por marcos regulatorios legales y / o; Bajo orden / dirección legal y / o; Existe un consentimiento explícito del paciente para el acceso de solo lectura a sus datos personales y de salud por razones de atención médica.
RF-084	El componente de metadatos de toda receta electrónica SERÁ: Sin cifrar cuando está en reposo y; Cifrado cuando está en tránsito; Nota: los metadatos están diseñados para estar disponibles para los sistemas de prescripción electrónica para ayudar a esos sistemas en la entrega de prescripciones electrónicas. Nota: este requisito no afecta otros requisitos relacionados con la presentación de recetas electrónicas. La inclusión de información en metadatos o de otro modo no implica que esta información deba o pueda ocultarse a los proveedores de atención médica
RF-085	El componente de prescripción (la carga útil) de la transmisión DEBE ser: a) Cifrado en reposo y b) Cifrado cuando está en tránsito; EXCEPTO cuando un sistema de dispensación conforme requiera que la carga útil se descifre en reposo con el fin de dispensar esa receta. Nota: La información de prescripción (la carga útil) solo está disponible para los sistemas de dispensación para actividades de dispensación.
RF-086	El contenido de las recetas digitales es información sensible del paciente, y su almacenamiento en un repositorio está regulado por la ley de protección de datos personales. Las recomendaciones de buenas prácticas para el almacenamiento seguro y privado de información en salud aplican a todo el tratamiento de la receta digital.

3.2.3. REQUERIMIENTOS TECNOLÓGICOS Y DE INFRAESTRUCTURA

El proveedor deberá proporcionar el equipamiento de infraestructura necesario para cumplir con todos los requerimientos de la solución. Para ello deberá realizar la instalación de equipos en el Data Center de CNT, garantizando el cumplimiento de las fechas en el cronograma. Si existieran demoras en la importación o adquisición de infraestructura, el proveedor deberá proporcionar todo el hardware de similares características temporal (de contingencia), que cubra las necesidades de los requerimientos y permita desplegar la solución de manera correcta, hasta la instalación del hardware definitivo. De darse esta situación, el proveedor deberá proporcionar el mecanismo de migración o cambio de hardware de manera transparente, respetando los SLAs (sin degradar o interrumpir el servicio más allá de lo permitido).

La solución residirá en el centro de datos del Ministerio de Salud Pública, ubicado en el Mega Centro de Datos de la Corporación Nacional de Telecomunicaciones CNT E.P cuya arquitectura de infraestructura, y para efectos netamente ilustrativos es la siguiente:



Es necesario que el proveedor realice un correcto dimensionamiento previo del hardware, ancho de banda, y se utilicen tecnologías modernas que favorezcan la interoperabilidad, que sean flexibles y permitan la rápida implementación de nuevas funcionalidades, correcciones o mejoras.

Requerimientos:

a) Sistema Hiper Convergente y sus respectivos Subsistemas

CARACTERÍSTICAS TÉCNICAS SISTEMA HIPERCONVERGENTE
ESPECIFICACIONES SOLICITADAS
En las especificaciones técnicas el Sistema HIPERCONVERGENTE hará referencia a los siguientes subcomponentes: Nodos HIPERCONVERGENTES Virtualización Cómputo Virtualización Almacenamiento Gestión Virtualización. Todos los equipos que forman parte de la solución deben ser nuevos de fábrica, no re-manufacturados, ni reparados en ninguna de sus partes. Su año de fabricación debe ser al menos 2021, esto incluye a cada uno de los componentes, el proveedor deberá sustentar con certificado emitido por el fabricante.
El sistema HIPERCONVERGENTE debe ser instalado por el fabricante en conjunto con el proveedor de acuerdo con las mejores prácticas de todos sus componentes. Se instalará en el Data Center del Ministerio de Salud Pública.
El soporte del Sistema HIPERCONVERGENTE debe ser entregado en forma unificada: hardware de los nodos, virtualización de cómputo, virtualización de almacenamiento y sistemas de gestión a través de un servicio de soporte integral y unificado. Adjuntar certificado emitido por el fabricante.
Producto certificado y catalogado por el fabricante como SISTEMA HIPERCONVERGENTE de virtualización donde los componentes de red, cómputo, almacenamiento y virtualización están constituidos como un solo producto.
Las actualizaciones de software, firmware, parches/fixes deben ser certificadas y entregadas por el fabricante en forma integrada y considerando todos los componentes de red, computo, almacenamiento y virtualización. El proveedor deberá obtener del fabricante parches/fixes cada seis meses, así como detalles de parches/fixes soportados y su procedimiento de aplicación. No podrán ser aplicadas actualizaciones y/o parches por separado que no hayan sido pre-validados por el fabricante.
Toda la infraestructura y sus componentes de red, cómputo, almacenamiento y virtualización deberá ser con esquema de alta redundancia N+1. Adjuntar el certificado respectivo.
El proveedor deberá garantizar a la institución que a través de la entrega de un certificado el fabricante ofrece y certifica un esquema de atención directa de llamadas y problemas que deberá ser provisto desde un centro de soporte unificado, desde donde deberán asistirse todos los problemas asociados a los componentes de red, computo, almacenamiento y virtualización, durante el tiempo que dure la garantía en la modalidad 7x24x 365 con un tiempo de respuesta en sitio máximo de 4 horas para solventar inconvenientes.
La infraestructura HIPERCONVERGENTE deberá incluir todo el licenciamiento e instalación del software Hipervisor que permita el cumplimiento de todo lo requerido. El proveedor deberá detallar la cantidad, versión de todo el licenciamiento necesario para cumplir con el objeto de la contratación.
El sistema debe contar con una aplicación de soporte que reporte el estado del equipo al fabricante en forma automática. El proveedor deberá detallar las características técnicas de aplicación de soporte propuesta.
NODOS HIPERCONVERGENTE
DESCRIPCIONES GENERALES
Los Nodos HIPERCONVERGENTES deben ser alojados en rack estándar de 19 pulgadas.
El Sistema HIPERCONVERGENTE debe tener una escalabilidad de hasta 64 Nodos.
Cada Nodo debe contar como mínimo con los siguientes puertos de red: Dos puertos 25GbE SFP28 1 puerto 1000Mb Ethernet – Gestión
Cada Nodo debe contar como mínimo con la siguiente capacidad de cómputo:

Un (1) procesador de: o Mínimo 26 núcleos por cada procesador. o Mínimo 2,1 GHz. o Mínimo 35.75MB de Cache o Conjunto de instrucciones de 64-bits. o Última tecnología liberada por el fabricante de los procesadores o Fecha de Lanzamiento: 2021 o Procesadores de segunda Generación
Cada nodo debe contar como mínimo con la siguiente capacidad de almacenamiento: Cache: mínimo 2 x 1600GB SSD Almacenamiento mínimo: 12 x 4TB 7.2K HDD
Cada nodo debe permitir incrementar memoria RAM, Discos de Caché, Discos de Almacenamiento y tarjetas de Red de acuerdo con la disponibilidad del hardware. El proveedor deberá detallar en su propuesta las características técnicas.
Mínimo 128 GB de memoria RAM DDR4 de 3200 MT/s de velocidad por nodo
La Solución Hiperconvergente debe entregar un pool garantizado de recursos de las siguientes características: Procesamiento mínimo: 90 GHz IOPS mínimo: 60000 de front end (70% lectura, 30 % escritura)
Deberá contar mínimo con: Software de administración. Software de monitoreo. Software de reportería
LICENCIAS/SUSCRIPCIONES DE PLATAFORMA DE VIRTUALIZACIÓN
DESCRIPCIONES GENERALES
Modelo/número de parte: (Especificar).
Marca: (Especificar).
Cantidad: (Especificar).
El SISTEMA HIPERCONVERGENTE debe incluir el licenciamiento/suscripción para la plataforma de virtualización considerando que se tiene 1 procesador por nodo. El proveedor deberá detallar las especificaciones de licenciamiento/suscripción propuestas. Todo licenciamiento debe ser establecido a nombre del Ministerio de Salud Pública del Ecuador.
Se debe instalar en los respectivos servidores la última versión liberada y soportada por el fabricante del SISTEMA HIPERCONVERGENTE, adjuntar certificado.
El Sistema HIPERCONVERGENTE debe incluir y venir pre-cargado de fábrica con el Hipervisor, de modo de minimizar los tiempos de puesta en marcha y debe ser 100% compatible con la actual plataforma de virtualización existente (VMWARE).
El fabricante del Sistema HIPERCONVERGENTE debe proveer el soporte integrado de la capa de virtualización de cómputo.
El Hipervisor debe disponer de funcionalidades de alta disponibilidad.
La solución deberá permitir entregar estadísticas completas sobre las máquinas virtuales, como consumos de CPU, RAM y Almacenamiento, así como los IOPs de lectura/escritura y latencias.
El licenciamiento/suscripción debe ser aplicable a un nuevo servidor del mismo fabricante del SUBSISTEMA DE CÓMPUTO, es decir no estar atado el hardware.
Debe contar con el mayor nivel de funcionalidades desarrolladas por el fabricante específicamente para la plataforma de virtualización, debe cumplir como mínimo: Migración en vivo de las máquinas virtuales de un nodo a otro. Migración en vivo de los datastore de un almacenamiento o LUN a otra. Configuración de alta disponibilidad Integración con agentes de respaldos para recuperación de máquinas virtuales. Soportar la capacidad de replicación a través de red LAN y WAN. Capacidad de recuperarse ante una falla de sistema operativo o aplicación. Permitir capturar la configuración de un nodo virtual para poder cargarlo a otro. El proveedor deberá incluir todo lo necesario para el funcionamiento de la solución como es cables, licencias, transceivers, entre otros. Garantía técnica, vigencia y soporte por cinco (5) años en la modalidad 7x24x365

(7días a la semana, 24 horas los 365 días del año) y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública 4 horas que aseguren la operatividad de la plataforma) acorde al SLA.
VIRTUALIZACIÓN DE ALMACENAMIENTO
DESCRIPCIONES GENERALES
El sistema Hiperconvergente debe incluir un software integrado de virtualización de almacenamiento. El proveedor deberá detallar las especificaciones de software integrado.
El fabricante del Sistema HIPERCONVERGENTE debe proveer el soporte integrado de la capa de virtualización de almacenamiento.
La capa de virtualización de almacenamiento debe correr en el mismo Kernel del Hipervisor a fin de optimizar el uso de los recursos y asegurar rendimiento.
El sistema de virtualización de almacenamiento debe proveer recursos de bloques a sistemas fuera del Sistema HIPERCONVERGENTE a través de protocolos estándares como iSCSI.
La administración de la virtualización de almacenamiento debe ser integrada a la administración de servidores virtuales y no ser una consola independiente.
El sistema de almacenamiento debe manejar como políticas características mínimas como: Desempeño Nivel de protección Calidad de Servicio Estas características deben tener la granularidad de máquina virtuales.
Garantía técnica, Vigencia y soporte por cinco (5) años en la modalidad 7x24x365 (7días a la semana, 24 horas los 365 días del año) y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública 4 horas que aseguren la operatividad de la plataforma) acorde al SLA.
SERVICIOS DE ALMACENAMIENTO
DESCRIPCIONES GENERALES
Debe soportar el Sistema HIPERCONVERGENTE ofertado los siguientes servicios de almacenamiento como mínimo: Replicación. Gestión de almacenamiento jerárquico en nube pública.
Estas aplicaciones de servicios de almacenamientos deben venir pre-cargadas de fábrica o ser instaladas a través de un portal integrado.
El fabricante del Sistema HIPERCONVERGENTE debe proveer el soporte integrado acorde al SLA de estas aplicaciones de servicios de almacenamiento, mientras dure la garantía técnica de la solución. El proveedor deberá incluir un certificado emitido por el fabricante para la verificación del cumplimiento de éste requerimiento.
El Sistema HIPERCONVERGENTE debe soportar la funcionalidad de replicación de máquinas virtuales a un sistema externo, basado en el mismo Hipervisor. El sistema externo podrá ser un Sistema HIPERCONVERGENTE o no, del mismo fabricante o de un tercero.
La replicación deberá permitir replicación con RPO = 0 (es decir replicación sincrónica).
SISTEMA DE GESTIÓN
DESCRIPCIONES GENERALES
Las funciones de administración de cómputo y almacenamiento virtualizado deben ser integradas en una sola consola.
Debe proveerse una consola integrada tipo GUI para realizar funciones de gestión. Al menos debe contar con todas las siguientes: Aprovisionamiento de nodos nuevos. Actualización de parches de software del sistema. Visualizar la utilización de los recursos. Visualizar el estado de salud del sistema.
Debe proveer capacidad de monitoreo remoto para diagnóstico y reparación.
ADMINISTRACIÓN DEL SISTEMA HIPERCONVERGENTE
REQUERIMIENTOS GENERALES
Debe proveer la funcionalidad de alarmas preventivas y automáticas en caso de falla de componentes del sistema a través de correo electrónico.

El sistema HIPERCONVERGENTE debe contar con un software de gestión que mínimo cumpla con las siguientes funcionalidades: Descubrir y mantener automáticamente el inventario de toda la infraestructura del sistema. Chequeo de las versiones de software instaladas en el sistema versus las versiones de software certificadas por el fabricante. Log HIPERCONVERGENTE del sistema. Monitoreo del estado de salud de la infraestructura.
La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de hiperconvergencia instalada en los nodos que componen la solución, manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información.
La solución debe permitir analizar en forma gráfica el impacto que tiene un evento con el comportamiento de la plataforma global y/o con el comportamiento de una máquina virtual a nivel de CPU, memoria, disco y red.
El servicio de administración debe ser gestionado desde una consola permitiendo al menos lo siguiente:
Gestionar todos los componentes de la solución Hiperconvergente. Gestionar todos los clústeres de recursos centralizadamente. Soporte para monitoreo de los hipervisores centralizadamente. Aprovisionar recursos. Asignar roles de usuario basado en perfiles por lo que la solución soportará la integración con Directorio Activo o con sistemas LDAP para la autenticación en el uso de la herramienta. Debe tener interfaz gráfica de administración basada en un entorno WEB de uso intuitivo amigable al usuario.
Debe permitir determinar en tiempo real el consumo de los recursos de CPU, Memoria RAM y almacenamiento por nodo, por máquina virtual, por clúster y en forma global.
La interface gráfica debe entregar mínimo estadísticas completas sobre las máquinas virtuales como consumos de vCPUs, Memoria RAM y discos así como: IOPS de lectura, IOPS de escritura y métricas de red.
La solución debe permitir el análisis de ancho de banda utilizado por una máquina virtual, un host físico, o un clúster.
La interfaz gráfica de administración debe tener la capacidad de configurar roles de usuario, al menos rol operador y rol administrador, por lo que la solución soportará la integración con Directorio Activo o con sistemas de LDAP para la autenticación en el uso de la herramienta.
La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, cómputo e Hipervisor) directamente desde la consola WEB y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni ocurrencia de indisponibilidad del servicio.
La solución debe soportar integración mediante el uso de REST API, SNMP, Web Services u otros similares que habilite la integración a otra soluciones de administración para facilitar la integración con ambientes de monitoreo actuales.
La solución debe estar en la capacidad de emitir alertas en caso de problemas detectados a nivel de hardware y software.
La solución debe permitir configurar umbrales para la emisión de alertas, así como su criticidad (al menos 3 categorías: crítica, warning y normal).
La solución debe poder brindar información out of the box en formatos CSV de al menos: Capacidad por clúster. Capacidad por nodo. Rendimiento por clúster. Rendimiento por nodo. Rendimiento por máquina virtual o por grupo de máquinas virtuales. Alertas presentadas.
Licenciamiento: El proveedor debe especificar el tipo de licenciamiento y los correspondientes costos que aplican para el software de gestión & administración de la Plataforma Hiperconvergente:

Por tipo. Por capacidad. Por funcionalidad. Por consumo. Por recursos.
Garantía técnica, Vigencia y soporte por cinco (5) años en la modalidad 7x24x365 (7días a la semana, 24 horas los 365 días del año) y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública 4 horas que aseguren la operatividad de la plataforma) acorde al SLA.
INSTALACIÓN - GARANTÍA
DESCRIPCIONES GENERALES
El sistema HIPERCONVERGENTE en su totalidad debe ser diseñado, armado, preconfigurado y probado por el fabricante. El proveedor deberá adjuntar certificado emitido por el fabricante.
El proveedor en conjunto con el fabricante desarrollará un Plan del Proyecto, con rutas críticas, eventos e hitos junto con personal técnico del Ministerio de Salud Pública. En este documento se reflejará los requerimientos técnicos del Ministerio de Salud Pública para todos los componentes del SISTEMA HIPERCONVERGENTE, de acuerdo con el diseño establecido. (Número de clúster de virtualización, configuración de pools de recursos, VLAN de producción.).
Adicionalmente el Proveedor deberá elaborar todos los documentos relacionados al diseño, planificación y entregables documentales del proyecto para incluir en la documentación final para el despliegue del sistema HIPERCONVERGENTE.
El Proveedor deberá realizar el despliegue y configuración del sistema HIPERCONVERGENTE, tomando como referencia las mejores prácticas para la configuración y administración especificadas por el fabricante.
Se deberá incluir todo el software y hardware requerido, cables, paquetes, drivers para el correcto funcionamiento del sistema HIPERCONVERGENTE.
El proveedor deberá incluir todos los catálogos de los equipos ofertados en formato digital.
El Proveedor deberá etiquetar y peinar todo el cableado de FO y Cobre solicitado en este apartado, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo a los lineamientos de la Corporación Nacional de Telecomunicaciones y la DNTIC. Todo el cableado de FO y Cobre que el Proveedor instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes de mínimo 5 años.
El proveedor deberá incluir todos los cables eléctricos que permitan la integración de la solución a la red eléctrica de manera redundante. Adicionalmente deberá incluir los rieles de montaje para rack estándar de centro de datos para todos los equipos que forman parte de su solución.
El equipamiento requerido deberá incluir fuentes de poder 100-240 VAC y ventiladores redundantes hot-swap. El tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC-320 C13/14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del MSP.
Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 24x7x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 24x7x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor. La garantía técnica de fabricante (incluido el periodo de extensión de garantía técnica) deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio incluido sin ningún costo adicional para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública.

El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de micro código (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.

El proveedor, como parte de adquisición del equipamiento, proporcionará un pool de 80 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica), sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la infraestructura de procesamiento y software relacionado, que se encuentra detallado en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):

Prioridad	Descripción	Tiempo Respuesta para iniciar trabajos de soporte especializado	Tipo Soporte
Alta	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.	Hasta 2 horas	Remoto y/o Teléfono
		De 3 – 4 horas	En sitio
Moderada	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.	5 – 6 horas	En sitio, Remoto o Telefónico
Baja	Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.	24 horas	En sitio, Remoto o Telefónico

Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.
Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.

El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas:

El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA						
Prioridad	**Descripción**	**Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente**	**Modalidad de comunicación**	**Tiempo máximo de diagnóstico del incidente o problema**	**Forma de Trabajo, para diagnóstico o solución**	**Tiempo de Cambio de Repuestos y solución a incidentes.**
Alta	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.	2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	4 horas posteriores al resultado del diagnóstico
Media	Herramienta continúa	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-	4 horas posteriores a la	Respuesta inicial Telefónica y/o	12 horas posteri

	en funcionamiento, causa molestias pero no se paralizará la producción en el corto plazo		mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	remoto. En sitio para diagnóstico y/o resolución de incidente	ores al resultado del diagnóstico
Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico

El proveedor deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de cada uno de los componentes de hardware y software que conforman la solución en forma detallada a manera de procedimiento técnico documentado. Este manual técnico debe permitir la re instalación de cualquier componente

de hardware y/o software que conforman la solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.
El proveedor deberá realizar la transferencia de conocimientos en el manejo y administración de toda la solución a adquirirse tanto del hardware como software/firmware del equipamiento y configuraciones realizadas; para un mínimo de 5 analistas que la DNTIC designe. La transferencia de conocimientos se deberá organizar en dos grupos de funcionarios y los horarios serán coordinados con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública, con una duración mínima de 40 horas por grupo. Se deberá incluir y documentar una capacitación en todas las funcionalidades o features del equipo ofertado. Al finalizar la transferencia se deberá entregar un certificado de culminación a cada participante.

b) Switchs LAN para Integración de Hiperconvergencia

DESCRIPCIONES GENERALES
Se deberá incluir mínimo 2 Switches LAN para la comunicación redundante de los nodos hiperconvergentes. Estos switches deben ser del mismo fabricante de la solución de Hiperconvergencia.
Cantidad: 2
Modelo: Especificar. Todos los equipos que forman parte de la solución deben ser nuevos de fábrica, no re-manufacturados, ni reparados en ninguna de sus partes. Su año de fabricación debe ser al menos 2021, esto incluye a cada uno de los componentes, el proveedor deberá sustentar con certificado emitido por el fabricante.
Marca: Especificar
Tamaño: 1 Unidad de Rack
Cada Switch del Centro de Datos, debe ser capaz de operar en capa 2 (L2) y capa 3 (L3).
Cada Switch mínimo tendrá puertos que puedan soportar de 10Gbps, 25Gbps 40Gbps o 100Gbps. según la necesidad.
Cada Switch deberá poseer mínimo 24 puertos capaces de operar a 10Gbps y 25Gbps según sea la necesidad.
Cada switch debe incluir un cable de un metro de 40Gbps para configuración de alta disponibilidad
Incluir los transceivers, conectores y cables (patch Cords) necesarios para conectar los nodos de hiperconvergencia de forma redundante a cada uno de los puertos de 25Gbps solicitados para los nodos hiperconvergentes.
Cada switch tendrá una capacidad de Switching mínimo de 1 Tbps y 2.16 Tbps en full dúplex.
Cada switch tendrá un tamaño del Buffer mínimo de 32 MB
Cada switch tendrá un Throughput mínimo de 954 Mpps
Puertos de consola: 1
Cada switch deberá soportar una latencia de máximo 800 ns (nano sec)
Alta disponibilidad: Se debe configurar los dos equipos en Alta Disponibilidad en funcionamiento Activo-Activo
Los ventiladores deben ser redundantes en esquema N+N retirables en caliente.
Todos los puertos de acceso Ethernet deberán funcionar a tasas completas (full rate).
Alimentación de 100 a 240V AC 60Hz. Deberán incluir fuentes de energía redundantes y los cables de alimentación eléctrica para los tomacorrientes con líneas a tierra. El tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC-320 C13/14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del MSP.
El sistema operativo de los switches deberá soportar la funcionalidad de actualización en caliente sin necesidad de apagar o reiniciar los switches.
Cada switch deberá soportar protocolos de capa 3 como OSPF, BGP y Vxlan en capa 2.
Cualquier integración que se requiera a nivel LAN con el core de comunicaciones del proveedor de Housing del MSP, se deberá realizar con patch cords de categoría 6A

<table>
<tr><td>Administrables y/o cables de FO de tipo LC-LC OM3.</td></tr>
<tr><td>Cada switch debe soportar características de networking para hacer cascada, agregación de enlaces, calidad de servicio (QoS) y seguridad.</td></tr>
<tr><td>Los switches del centro de datos deberán ser instalados y configurados en el Rack de la solución de Hiperconvergencia ofertado.</td></tr>
<tr><td>Se debe garantizar que los puertos de los equipos ofertados se encuentren licenciados para trabajar a 10Gbps/25Gbps y los puertos de uplink a 40Gbps y 100Gbps.</td></tr>
<tr><td>El proveedor deberá incluir los rieles de montaje para rack estándar de centro de datos para todos los equipos que forman parte de su solución.</td></tr>
<tr><td>Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas, deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 24x7x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 24x7x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor.

La garantía técnica de fabricante (incluido el periodo de extensión de garantía técnica) deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio incluido sin ningún costo adicional para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública.</td></tr>
<tr><td>El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de micro código (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.</td></tr>
<tr><td>El proveedor como parte de adquisición del equipamiento proporcionará un pool de 20 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica) sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la infraestructura de procesamiento y software relacionado, que se encuentra detallado en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):

<table>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo Respuesta para iniciar trabajos de soporte especializado</th><th>Tipo Soporte</th></tr>
<tr><td rowspan="2">Alta</td><td rowspan="2">Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.</td><td>Hasta 2 horas</td><td>Remoto y/o Teléfono</td></tr>
<tr><td>De 3 – 4 horas</td><td>En sitio</td></tr>
</table>
</td></tr>
</table>

Moderada	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.	5 – 6 horas	En sitio, Remoto o Telefónico
Baja	Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.	24 horas	En sitio, Remoto o Telefónico

Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.
Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.

El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas:

El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA

lad	**Descripción**	**Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente**	**Modalidad de comunicación**	**Tiempo máximo de diagnóstico del incidente o problema**	**Forma de Trabajo, para diagnóstico o solución**	**Tiem de Cambio de Repuestos y solución a incidentes.**
	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el	2 horas posterior a la comunicación inicial, o	Respuesta inicial Telefónica y/o remoto.	4 horas posteriores al resultado del

			Proveedor, para constancia y registro respectivo.	definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	En sitio para diagnóstico y/o resolución de incidente	diagnóstico
	Herramienta continúa en funcionamiento, causa molestias pero no se paralizará la producción en el corto plazo	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	12 horas posteriores al resultado del diagnóstico
	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico
El proveedor deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de cada uno de los componentes de hardware y software que conforman la solución en forma detallada a manera de procedimiento técnico documentado. Este manual técnico debe permitir la re instalación de cualquier componente de hardware y/o software que conforman la solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.						
El proveedor deberá realizar la transferencia de conocimientos en el manejo y administración de toda la solución a adquirirse tanto del hardware como software/firmware del equipamiento						

y configuraciones realizadas; para un mínimo de 5 analistas que la DNTIC designe. La transferencia de conocimientos se deberá organizar en dos grupos de funcionarios y los horarios serán coordinados con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública, con una duración mínima de 10 horas por grupo. Se deberá incluir y documentar una capacitación en todas las funcionalidades o features del equipo ofertado. Al finalizar la transferencia se deberá entregar un certificado de culminación a cada participante.

c) Software de Orquestación de Respaldos

SOFTWARE DE RESPALDO
DESCRIPCIONES GENERALES
Especificar marca de la solución de respaldos
Especificar versión. Debe ser la última versión de software disponible por el fabricante.
El Proveedor deberá incluir el licenciamiento de la solución de respaldos para todos los nodos físicos solicitados en la solución Hiperconvergente y las BDD (Oracle, My SQL y PostgreSQL) detalladas en este documento, sin limitación de la cantidad de máquinas o servidores virtuales que se encuentren desplegadas dentro.
Licenciamiento basado en procesador (sockets), de uso perpetuo, con servicio de mantenimiento y actualización del producto ofrecidos por el término mínimo estándar de 3 años y con un periodo de extensión de servicios de mantenimiento y actualización de 2 años adicionales. Todo licenciamiento deberá ser registrado a nombre del Ministerio de Salud Pública del Ecuador.
El proveedor deberá incluir la instalación y configuración de la solución ofertada dentro del equipo servidor requerido en este documento y conforme a las recomendaciones y buenas prácticas definidas por el fabricante del producto. Esta parametrización deberá incluir la configuración de los repositorios “stage” donde se realizarán los respaldos de las Máquinas Virtuales, así como de los repositorios para el respaldo de las bases de datos, repositorios NFS, las configuraciones de red, configuraciones del sistema operativo y demás pre requisitos definidos por el fabricante del sistema orquestador de respaldos y que permitan garantizar su rendimiento. El Proveedor deberá incluir la configuración de al menos 30 tareas de respaldo automatizadas para las máquinas virtuales que la DNTIC determine y que se encontrarán desplegadas dentro de la solución Hiperconvergente requerida en este documento. El Proveedor deberá ejecutar pruebas de generación y recuperación de los respaldos, con la finalidad de evidenciar el correcto funcionamiento de la solución y consistencia de los datos generados dentro del proceso de respaldo.
La solución propuesta deberá incluir los componentes y/o funcionalidades necesarias para la ejecución de respaldos de al menos 10 instancias de base de datos Oracle desplegadas en infraestructura Power con Sistema Operativo AIX 7.x., o Sistema Operativo Solaris/Oracle Linux en sus últimas versiones liberadas por el fabricante, operando sobre arquitectura SPARC; el que el MSP indique. La solución deberá permitir definir la programación de ejecución automatizada de tareas de respaldo de estas bases de datos conforme a las necesidades de la DNTIC. La solución deberá tener integración con Oracle RMAN y deberá permitir una recuperación rápida a nivel de transacción de bases de datos a un punto preciso del tiempo y/o una transacción específica. Deberá permitir como mínimo lo siguiente: Recuperación a nivel de transacciones a través del análisis del log de transacciones. Recuperación de bases de datos a un punto en el tiempo a través del replay del log de transacciones desde un backup de imagen en un solo paso. Gestionar logs archivados para evitar el llenado de backups y aprovechar al máximo la cantidad de almacenamiento usada para el backup. Publicar o exportar la base de datos, incluso como un backup RMAN Recuperación en otra infraestructura de base de datos
La solución deberá incluir funcionalidades de respaldo (backup) y replicación integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada.

La solución no deberá necesitar de la instalación de agentes para poder realizar sus tareas de respaldo, recuperación y replicación de máquinas virtuales.
La solución deberá poder realizar respaldos sin detener las máquinas virtuales, y sin generar degradación en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto.
La solución deberá ser capaz respaldar las configuraciones de las mismas, al margen de los datos propios de las máquinas.
La solución deberá ser compatible con las bases de datos Oracle 11g, 12c y 19c. PostgreSQL desde la versión 10.x hasta la versión estable liberada por el fabricante a fecha de elaboración de este informe y MySQL desde la versión 5.3 hasta la versión estable liberada por el fabricante a fecha de elaboración de este informe
La solución deberá ser capaz de respaldar las bases de datos Oracle 11g, 12c y 19c. PostgreSQL desde la versión 10.x hasta la versión estable liberada por el fabricante a fecha de elaboración de este informe y MySQL desde la versión 5.3 en adelante hasta la versión estable liberada por el fabricante a fecha de elaboración de este informe
La solución deberá ser capaz de respaldar de forma indistinta una máquina virtual completa o discos virtuales específicos de una máquina virtual.
Deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador.
Deberá ser una solución altamente eficaz y preparada para el futuro integrándose en forma extensiva, con las APIs de los fabricantes de infraestructura virtualizada, para la protección de datos.
La solución deberá poder realizar respaldos (backup) incrementales ultra rápidos aprovechando la tecnología de seguimiento de bloques de disco modificados (changed block tracking) reduciendo al mínimo el tiempo de respaldo (backup) y posibilitando un respaldo (backup) y una replicación más frecuente.
La solución deberá permitir la recuperación instantánea de las máquinas virtuales, así mismo deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilidad del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.
La solución propuesta deberá tener integración nativa con la librería robótica solicitada en este documento. Adicionalmente deberá permitir la programación automática de tareas de respaldo a cintas LTO.
La solución propuesta, luego de una recuperación rápida, deberá poder realizar una restauración total sin interrupciones del servicio. Se pretende que el trabajo realizado por los usuarios no deba verse afectado al migrar sus máquinas virtuales desde el respaldo (backup) hasta el almacenamiento de producción
La herramienta propuesta deberá proveer la capacidad de completar restauraciones completas del respaldo (backup) de cualquier máquina virtual dentro de una ventana de mantenimiento mínima. La estrategia deber consistir en replicar o realizar una copia en caliente del respaldo (backup) de la máquina virtual que se encuentra en un almacenamiento de-duplicado al almacenamiento en producción donde la máquina virtual se ejecuta.
No deberá requerir licencias independientes para las actividades de respaldo, recuperación y replicación.
Deberá soportar las últimas versiones disponibles de los hipervisores, al menos VMWare vSphere 6.5
El software debe presentar estadísticas de rendimiento, calendarización, trabajos, respaldos. Debe permitir enviar alertas vía correo y SNMP.
Todo el software que conforma la solución requerida en estas especificaciones técnicas, deberán disponer de una garantía técnica y soporte de fabricante vigente por 3 años en modalidad 8x5x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica y soporte de fabricante del software por 2 años adicionales, en modalidad 8x5x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor.
El Proveedor será responsable de aplicar/instalar las últimas actualizaciones estables liberadas por el fabricante del producto, en coordinación con la DNTIC del MSP y máximo un mes después de su lanzamiento oficial, mientras dure el periodo de garantía técnica y soporte

de fabricante (incluido el periodo de extensión de la garantía técnica y soporte). Todas las actividades descritas en este párrafo no implicarán costos adicionales para el MSP.

El proveedor, como parte de adquisición del equipamiento, proporcionará un pool de 40 horas de soporte técnico especializado canal mientras dure la garantía y soporte del software (incluido el periodo de extensión de garantía técnica) sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la solución de respaldos detallada en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):

Prioridad	Descripción	Tiempo Respuesta para iniciar trabajos de soporte especializado	Tipo Soporte
Alta	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.	Hasta 2 horas	Remoto y/o Teléfono
		De 3 – 4 horas	En sitio
Moderada	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.	5 – 6 horas	En sitio, Remoto o Telefónico
Baja	Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.	24 horas	En sitio, Remoto o Telefónico

Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.

Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.

El tiempo de respuesta ante fallas del software que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas:

El proveedor deberá dar atención en el análisis de daños/errores/problemas y resolución de incidentes que se presenten en el software requerido. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante del producto sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA						
Prioridad	**Descripción**	**Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente**	**Modalidad de comunicación**	**Tiempo máximo de diagnóstico del incidente o problema**	**Forma de Trabajo, para diagnóstico o solución**	**Tiempo de solución a incidentes.**
Alta	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.	2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 5x8x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	4 horas posteriores al resultado del diagnóstico
Media	Herramienta continúa en funcionamiento, causa molestias pero no se paralizará la producción en el corto plazo	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	12 horas posteriores al resultado del diagnóstico

				para la atención. Modalidad 5x8x365		
Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 5x8x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico
El proveedor deberá entregar un manual técnico de instalación y configuración de cada uno de los componentes de hardware y/o software que conforman la solución ofertada en forma detallada a manera de procedimiento técnico documentado. Este manual técnico debe permitir la re instalación de cualquier componente de hardware y/o software que conforman la solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.						
El proveedor deberá realizar la transferencia de conocimientos en el manejo y administración de toda la solución a adquirirse para un mínimo de 5 analistas que la DNTIC designe. La transferencia de conocimientos se deberá organizar en dos grupos de funcionarios y los horarios serán coordinados con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública, con una duración mínima de 20 horas por grupo. Se deberá incluir y documentar una capacitación en todas las funcionalidades o features de la solución ofertada. Al finalizar la transferencia se deberá entregar un certificado de culminación a cada participante.						

d) Solución de Hardware de Respaldos - Librería de cintas LTO y servidor para instalación de orquestador

HARDWARE PARA GESTIÓN DE RESPALDOS - LIBRERÍA DE CINTAS LTO Y SERVIDOR PARA INSTALACIÓN DE ORQUESTADOR	
El cumplimiento de todas y cada una de las especificaciones debe ser completamente respaldado con catálogos, manuales hojas técnicas de los servicios o software asociado al servicio, los cuales deben adjuntarse obligatoriamente a la oferta en formato digital.	
CARACTERÍSTICA TÉCNICA	**ESPECIFICACIÓN DEL SERVICIO**
Tipo de Equipo	Librería robótica de cintas
Cantidad requerida	Un equipo
Marca	Especificar
El fabricante, a través del proveedor adjudicado, deberá certificar que los equipos son NUEVOS DE FABRICA, no son re manufacturados no "REFURBISHED" y/o no "REBUILDERS".	Obligatorio

Modelo	Especificar. Debe ser de año de fabricación 2021.
Debe ser apto para montaje en chasis tipo rack, de tipo modular, debe incluirse cables de conexión de FO, cables de energía y rieles de montaje.	Obligatorio. El tamaño de los cables de interconexión de FO y energía eléctrica debe permitir la instalación e interconexión de los equipos requeridos por el MSP, dentro de un mismo rack de tamaño estándar de centro de datos.
Generación de fabricación.	La última generación de librería de cinta disponible por el fabricante de los equipos para el modelo ofertado.
Capacidad total de alojamiento de cartuchos	Igual o mayor a 24 cartuchos LTO.
Soporte de capacidad física por cartucho.	La librería de cintas debe tener la capacidad de utilización para lectura/escritura de como mínimo cartuchos de hasta 12 TB (Ultrium 8), 9 TB (Ultrium 7 tipo M) y 6 TB (Ultrium 7).
Velocidad de transferencia soportada por Drives	La librería de cintas debe soportar velocidades de transferencia de datos nativos de mínimo 360MB/s para drives de tipo LTO8 FH (Full High)
Cintas incluidas	El proveedor deberá incluir en su oferta, como mínimo 125 unidades de cinta (cartuchos) LTO8 de 12TB de capacidad (sin compresión) cada una y cuatro cintas de limpieza compatibles con los drives LTO8 a instalar. Las cintas (cartuchos) deberán incluir el respectivo código de barras como adhesivo de material resistente para colocar en cada una de las cintas y la numeración deberá ser definida por el MSP previo a la impresión a realizarse por parte del Proveedor. Las unidades de cinta LTO8 (cartuchos) deben incluir una garantía técnica otorgada por el proveedor, contra defectos de fabricación de mínimo 5 años.
Interfaz de red	La librería robótica de cintas deberá incluir como mínimo una (1) interface 100/1000 Mbps Ethernet (RJ45) para administración del equipo.
Integración Librería de Cintas - Servidor Requerido / Compatibilidad	El Proveedor deberá realizar las interconexiones y configuraciones necesarias para integrar la librería de cintas, con el equipo servidor requerido en este documento y en donde el proveedor del servicio de Centro de Datos Virtual IaaS realizará posteriormente, la instalación del software gestor de respaldos. La librería de cintas deberá ser integrada con el servidor requerido, mediante interfaces de Fibra Óptica, esto con la finalidad de garantizar mayor rendimiento en la transferencia de datos. La librería de cintas deberá ser compatible, para su integración y uso, con mínimo los siguientes sistemas gestores de respaldos: Veeam Backup and Replication 9.x o versión superior, Networker o Spectrum Protect en sus últimas versiones estables liberadas por el fabricante.
Instalación y configuración de la solución	El Proveedor deberá incluir la instalación de todo el equipamiento de hardware solicitado en este documento, en el Mega Centro de Datos de la CNT E.P., contratado por el MSP en calidad de “Housing”, y ubicado en la ciudad de Quito, Sector

	de La Armenia - Estación Terrena.
Documentación	El proveedor deberá entregar documentación técnica de la arquitectura desplegada, así como un manual técnico de instalación y parámetros de configuración que haya realizado/aplicado en cada uno de los componentes de hardware y software que conforman la solución requerida, en forma detallada, a manera de procedimiento documentado. Debe incluir en dicho documento, la configuración realizada en los componentes tales como tarjetas de comunicación de FO, switches SAN, equipos de networking de propiedad del MSP, librería de cintas, etc.
Compatibilidad	La librería de cintas debe ser compatible (a nivel de controladores de Sistema Operativo) con las últimas versiones liberadas por los fabricantes de sistemas operativos: Windows Server y Linux en sus distribuciones CentOS y Red Hat Enterprise.
Transferencia de Conocimientos	El proveedor deberá realizar la transferencia de conocimientos del funcionamiento y tareas de administración de toda la solución de librería y servidor requerida en este documento y las configuraciones realizadas, para un mínimo de 4 analistas que la Dirección Nacional de Tecnologías de la Información y Comunicaciones del MSP designe. La transferencia de conocimientos se deberá organizar en dos grupos con una duración mínima de 10 horas por grupo.
Fuente de alimentación	La librería de cintas deberá incluir como mínimo 2 fuentes de alimentación con la finalidad de garantizar redundancia en alimentación de energía
Número de Drivers LTO instalados	La librería de cintas deberá incluir como mínimo dos unidades (drives) de escritura/lectura LTO8 Fiber Channel FH (Full High) a velocidades de transferencia de datos nativos de mínimo 360MB/s, ambas con soporte para LTO8, LTO7 y LTO7 tipo M en escritura y lectura.
Crecimiento	La librería de cintas debe soportar la capacidad de crecimiento como mínimo en 2 drives (unidades) LTO8 FH o HH adicionales a los requeridos en este documento, que permitan la paralelización de tareas de respaldo. La librería de cintas deberá soportar dicho crecimiento mediante la agregación de unidades LTO adicionales en el mismo equipo ofertado o agregando expansiones al equipo ofertado.
Lector de código de barras de alta velocidad	Obligatorio, como parte del equipo.
Administración remota vía interface WEB	Si, obligatorio
Función multi ruta	Si, la librería de cintas debe permitir una arquitectura Multi-path lista para SAN con la finalidad de hacer posible la compartición de la librería. La librería debe incluir y garantizar capacidades de uso de una ruta alternativa de comunicación (redundante), cuando la ruta principal falla. En caso de que esta funcionalidad

	requiera licenciamiento adicional se deberá incluir como parte de la solución.
Compartición e Integración	La Librería de cintas debe tener la capacidad de compartirse con otras aplicaciones de respaldo existentes. La librería debe permitir su integración con mínimo los siguientes sistemas gestores de respaldos: Veeam Backup and Replication 9.x o versión superior, Networker o Spectrum Protect en sus últimas versiones estables liberadas por el fabricante, sea que dicho software esté instalado en equipamiento físico o en servidores virtualizados.
El equipo debe tener la capacidad de crear librerías lógicas	Si, obligatorio como mínimo 2 librerías lógicas.
Conectividad con el servidor requerido en este documento	Igual o mayor a 8 Gbps Fiber Channel. De requerirse, se deberá incluir los transceivers correspondientes para todas las tarjetas/puertos de fibra óptica de la solución ofertada que permitirán esta integración.
Panel de operador	El equipo debe incluir un panel de operador frontal que permita gestionar las configuraciones básicas del equipo.
Servidor de Gestión de Respaldos	
El Proveedor debe incluir un equipo servidor (Gestor de Respaldos) para la instalación de todo el software de gestión de respaldos que disponga el MSP y/o drivers de control de la librería, con al menos las siguientes características técnicas mínimas:	Obligatorio

Ítem	Características Técnicas del Equipo Servidor
Marca	Especificar
Modelo	Especificar
Compatibilidad con SO	El equipo servidor deberá ser compatible con sistemas operativos Windows Server en sus últimas versiones, VMware ESX en sus últimas versiones y Linux en sus últimas versiones para distribuciones Centos o Red Hat. El Proveedor debe incluir el licenciamiento de sistema operativo necesario que permita la instalación de la librería de cintas detallada en este documento y su detección a nivel de sistema operativo (drivers) como dispositivo; y adicionalmente para permitir la instalación de cualquiera de los siguientes sistemas gestores de respaldos: Veeam Backup and Replication versión 9.x o superior, Networker o Spectrum Protect en sus últimas versiones estables liberadas por el fabricante. El licenciamiento de Sistema Operativo entregado por parte del Proveedor deberá ser perpetuo e incluirá la correspondiente suscripción de soporte de fabricante que permita realizar descarga de parches de seguridad y “updates” como mínimo por un año. El licenciamiento deberá ser registrado a nombre del Ministerio de Salud Pública del Ecuador.
Partes y piezas	Todas las partes y piezas del servidor, deben ser homologadas por el fabricante de la marca del equipo.
Generación de fabricación	El equipo debe ser de la última generación disponible por el fabricante para el modelo ofertado. El fabricante, a través del proveedor adjudicado, deberá certificar que los equipos son nuevos de fábrica, no deben ser re manufacturados no

	"refurbished" y/o no "rebuilders".
Procesador	Debe incluir dos procesadores de última generación de mínimo: 2.2GHz, 10 Cores, 13.75M Cache. Debe ser procesador instalado de 64 Bits.
Conectividad FO	Debe incluir como mínimo dos tarjetas de FO de 16 Gbps de velocidad, FC Dual-port HBA cada una, con conectores tipo LC; para interconexión del servidor descrito, con los dos Switch SAN requeridos en este documento; esto con la finalidad de permitir su integración con los sistemas de almacenamiento solicitados en este documento. Las tarjetas de FO ofertadas deben incluir Transceivers (de ser aplicable).
Conectividad con Librería de cintas	Debe incluir mínimo dos tarjetas de FO de 8/16 Gbps de velocidad, FC Dual-port HBA cada una; para interconexión con librería de cintas. Las tarjetas de FO deben incluir Transceivers (de ser aplicable).
Memoria RAM Instalada	Igual o superior a 64 GB RDIMM
Almacenamiento Interno	Debe incluir mínimo 4 discos de 2.5” o 3.5" de mínimo 1.8TB de capacidad cada uno, 10K RPM, interface SAS 12Gb, Hot Swap, con la finalidad de configurar RAID 5.
RAID	Si debe incluir, la controladora RAID deberá soporta RAID 0, 1, 5, 6, 10, 50, 60. La controladora RAID deberá incluir una interfaz SAS a 12Gbps
Fuentes de Poder	Si, debe incluir fuentes de poder redundantes.
Conectividad LAN	Si, debe incluir como mínimo 2 interfaces 1/10 Gigabit Ethernet RJ45. Adicionalmente se deberá incluir los patch cords de integración LAN RJ45 de categoría 6A administrables para todos los puertos disponibles dentro de la solución de librería y servidor ofertados.
Tipo	Servidor de tipo “Rackeable” de máximo 2U. Se debe incluir rieles de montaje para Rack estándar.
Adicionales	Incluir cualquier tarjeta adicional que se requiera para la interconexión con la Librería de Cintas ofertada. (si aplicare)
Puertos USB y VGA	Debe incluir como mínimo 3 puertos USB 2.0 o de tecnología superior y 1 puerto VGA
Instalación y Configuración	El Proveedor debe incluir todas las tareas de instalación del equipo servidor y su software base (sistema operativo y drivers de librería de cintas) en el centro de datos del MSP ubicado en la ciudad de Quito, sector de la Armenia (Mega Centro de Datos - CNT E.P.). Debe incluir cables de poder y cables de FO LC-LC para integración del servidor requerido con la librería de cintas ofertada. El Proveedor deberá realizar, en coordinación con la Dirección Nacional de Tecnologías de la Información y Comunicaciones, las configuraciones requeridas en las unidades de almacenamiento y equipos de Networking de propiedad del Ministerio de Salud Pública del Ecuador que permitan integrar el servidor requerido, con las redes SAN y LAN existentes.
Garantía	Debe incluir cinco años de garantía de fabricante en partes y piezas contra defectos de fabricación, incluido sin costo para la institución, la mano de obra en sitio y cambio de partes o reposición del equipo en caso de aplicarse la garantía.
Nivel de servicio (SLA) para atención de incidentes en el equipamiento ofertado.	Se deberá manejar el mismo nivel de servicio (SLA) que está establecido para el equipo librería de cintas.

Servicios Adicionales / Garantía	
El Proveedor deberá disponer de una mesa de servicios para gestionar la atención de incidencias sobre el hardware adquirido.	Obligatorio, conforme al SLA establecido en este documento.
El Proveedor deberá entregar como mínimo 8 patch cords de fibra óptica multimodo conector LC/LC y 8 patch cords UTP 6A administrables. La longitud de los cables debe ser la adecuada para permitir una organización y peinado eficientes en cada rack, se debe garantizar el radio de curvatura indicado en las especificaciones técnicas de los cables. El Proveedor deberá etiquetar y peinar todo el cableado de FO y Cobre solicitado en este apartado, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo a los lineamientos de la Corporación Nacional de Telecomunicaciones y la DNTIC. Todo el cableado de FO y Cobre que el Proveedor instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes de mínimo 5 años	
Garantía técnica de los equipos y SLA	Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 8x5x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 8x5x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor.
El Proveedor será responsable de realizar las actualizaciones necesarias en el firmware/micro código de la librería de cintas y servidor a adquirir al menos una vez por año, durante la vigencia de la garantía técnica del fabricante (incluido el periodo de extensión de la garantía técnica). Las actividades de actualización del firmware/micro código de la librería de cintas y/o servidor deberán, de manera obligatoria, ser notificadas por el	Obligatorio

Proveedor cuando el fabricante libere versiones estables, y serán coordinadas con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del MSP para su aplicación en el equipamiento, todo esto sin costos adicionales para el MSP. Adicionalmente, y durante la vigencia de la garantía técnica del fabricante (incluido el periodo de extensión de la garantía técnica), el Proveedor deberá realizar, sin costos adicionales para el MSP, al menos dos visitas al año para ejecuciones de mantenimiento preventivo y limpieza del equipamiento requerido, esto en coordinación con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del MSP.	
SLA del Servicio aplicable para la Librería de Cintas y Equipo Servidor: El tiempo de respuesta ante eventos de falla en el hardware adquirido será de acuerdo al siguiente SLA. El SLA se aplicará dentro del esquema de atención 8x5x365:	Obligatorio

Prioridad	Descripción	Modalidad de Comunicación inicial para registro de incidente/requerimiento	Tiempo Respuesta para iniciar trabajos de diagnóstico y/o solución de incidentes	Tipo Soporte
Alta	Se requiere del soporte especializado para solventar requerimientos y/o	La notificación inicial de un incidente o requerimiento se lo realizará a través de	1 Hora contada a partir del registro del incidente al Proveedor por parte del MSP[1].	

[1] MSP o Ministerio de Salud Pública del Ecuador

	incidentes determinados por la DNTIC del MSP como urgentes y de alto impacto.	correo electrónico, al contacto indicado por el proveedor para constancia y registro de incidente o requerimiento respectivo a fin de reflejar la hora de inicio del tiempo de respuesta del SLA. En caso de que, al momento de generarse el incidente o requerimiento, el Ministerio de Salud Pública no cuente con el servicio de correo electrónico disponible, se realizará una llamada telefónica y el inicio de la misma será registrada por el administrador del contrato. El Ministerio de Salud Pública definirá la Prioridad del incidente al momento de su registro.	Menor o igual a 2 horas contadas a partir de registro del incidente al Proveedor por parte del MSP.	En sitio (centro de datos del MSP) en coordinación del personal de la DNTIC del MSP, y el(los) especialista(s) en la solución provistos por el Proveedor.
Moderada	Se requiere del soporte especializado para solventar requerimientos determinados por la DNTIC como moderados o de impacto bajo.		Menor o igual a 2 horas contadas a partir de registro del incidente al Proveedor por parte del MSP.	Vía acceso remoto a los equipos en coordinación del personal de la DNTIC del MSP, con soporte y comunicación telefónica por parte del(los) especialista(s) en la solución provistos por el Proveedor del servicio.
			Menor o igual a 4 horas contadas a partir de registro del incidente al Proveedor por parte del MSP.	En sitio (centro de datos del MSP) en coordinación del personal de la DNTIC del MSP, y el(los) especialista(s) en la solución provistos por el Proveedor.
Baja	Se requiere de soporte especializado para solventar requerimientos determinados por la DNTIC como programados o controlados. (Planificados)		Menor o igual a 24 horas contadas a partir de registro de incidente/requerimiento	Vía acceso remoto a los equipos en coordinación del personal de la DNTIC del MSP o en sitio si la DNTIC lo requiere.

El Ministerio de Salud Pública remitirá sus contactos técnicos respectivos para que la empresa adjudicada pueda coordinar acciones para la resolución de Tickets de incidentes.

En todos los casos y prioridades de los eventos definidos en el SLA, el hardware de los equipos físicos ofertados mantendrán soporte directo del fabricante del equipo durante el periodo de vigencia de la garantía (incluido el periodo de extensión de la garantía técnica), que cubra reposición de partes y piezas, mano de obra y atención en sitio sin ningún costo adicional para el Ministerio De Salud Pública, mínimo en modalidad 8x5x365 (las 8 horas

del día, los cinco días laborables de la semana, los 365 días del año), con un tiempo máximo de reemplazo de partes y piezas defectuosas o con fallas, de 6 horas contadas a partir del registro del incidente por parte del MSP. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública, mientras se encuentre vigente la garantía técnica de los equipos.	
Se requiere se firme un compromiso de confidencialidad de manera que se garantice que la información y detalles propios de la institución guarden los criterios de reserva, confidencialidad y propiedad, como exclusiva del Ministerio de Salud Pública del Ecuador.	Si, Obligatorio

e) Solución de Almacenamiento "Stage" para Respaldos

SOLUCIÓN DE ALMACENAMIENTO DE RESPALDOS	
El cumplimiento de todas y cada una de las especificaciones debe ser completamente respaldado con catálogos, manuales hojas técnicas de los servicios o software asociado al servicio, los cuales deben adjuntarse obligatoriamente a la oferta en formato digital.	
CARACTERÍSTICA TÉCNICA	**ESPECIFICACIÓN DEL SERVICIO**
Cantidad	Uno
Formato	El dispositivo debe permitir realizar el respaldo y recuperación de información basado en discos duros, mediante un mecanismo de optimización de deduplicación; dicha deduplicación deberá de realizarse en línea, durante la ingesta de los datos.
Tipo	La solución debe estar basada en un equipo appliance con propósito específico de respaldos con características de deduplicación y compresión.
Licenciamiento	El sistema debe incluir el licenciamiento de funcionalidad de de-duplicación de los bloques de los datos de los respaldos. La de-duplicación se define como la funcionalidad que permite la eliminación de segmentos redundantes con el fin de aprovechar de manera óptima la capacidad de almacenamiento.
Protección de datos	El sistema debe soportar la falla simultánea de hasta dos discos, el arreglo debe contar con protección de hardware RAID-6 o similar.
Monitoreo:	El software debe presentar estadísticas de rendimiento y ahorros debido a la compresión y deduplicación, debe permitir enviar alertas vía correo y SNMP
Grabación:	Debe contar con la capacidad de emular y escribir en formato de tecnologías de cintas LTO. Debe soportar los protocolos CIFS y NFS para presentar volúmenes y realizar respaldos por LAN. Deberá incluir protocolo de aceleración de respaldo, el cual permita duplicar el rendimiento de escritura de los datos.
Compatibilidad:	Debe ser compatible con software de respaldos solicitado en este proyecto.
Conectividad:	La solución propuesta debe contar con un mínimo de 4 puertos de 10Gbps SFP+, 2 puertos de 16Gbps FC HBA y mínimo 4 puertos Ethernet de 1Gb.
Conectividad a Housing	El Proveedor deberá entregar como mínimo 16 patch cords de fibra óptica multimodo conector LC/LC. La longitud de los cables debe ser la adecuada para permitir una organización y peinado eficientes en cada

	rack, se debe garantizar el radio de curvatura indicado en las especificaciones técnicas de los cables. El Proveedor deberá etiquetar y peinar todo el cableado de FO solicitado en este apartado, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo a los lineamientos de la Corporación Nacional de Telecomunicaciones y la DNTIC. Todo el cableado de FO y Cobre que el Proveedor instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes de mínimo 5 años.
Disponibilidad	El dispositivo debe incluir fuentes de poder y ventiladores redundantes y reemplazables en caliente.
Tipo de Disco	Los discos duros que conforman esta solución deben ser de tipo SAS. Los discos duros SAS deben ser de capacidad mínima de 4TB y una velocidad mínima de 7.2K RPM.
Rendimiento:	La librería virtual deberá disponer de un nivel de rendimiento de escritura de mínimo 15TB/hora.
Capacidad requerida:	El dispositivo deberá suministrarse con al menos 50 TB usables sin deduplicar (Considerando este almacenamiento solo para las transacciones especificadas en GEN-004), debidamente licenciados, el equipo deberá tener la capacidad de almacenar la información lógica retenida en cinco años.
Discos reserva (Hot Spare)	El proveedor deberá incluir como mínimo 6 discos en espera, independientes a los requeridos para suministrar la capacidad ofertada.
Protección:	La solución propuesta debe contar con el nivel de protección en RAID 6, dicho RAID se deberá de realizar a nivel de hardware y no vía software.
De-Duplicación de datos:	La solución propuesta debe incluir la funcionalidad de deduplicación. La deduplicación deberá efectuarse en línea, durante la ingesta de datos.
Administración:	El dispositivo debe contar con un software de gestión propio que permita su administración vía GUI o Web. Debe tener la capacidad de generar y enviar correos electrónicos o alarmas a una consola de gestión y soporte de SNMP Traps. Debe Permitir exportar información de monitoreo, log de errores, etc. hacia "fuera" del dispositivo.
Servicios de Instalación:	Los servicios de instalación y puesta en marcha deben ser ejecutados directamente por el Proveedor
Servicios de notificación de eventos:	El arreglo de discos debe contar con la funcionalidad de notificación en forma automática (a través de internet utilizando protocolo TCP/IP) los eventos hacia el centro de soporte del fabricante.
Fuente de poder y ventiladores	El equipo de almacenamiento deberá incluir fuentes de poder y ventiladores 100-240 VAC redundantes y hot-swap. El tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC-320 C13/14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del MSP.
Cables de poder y adicionales	El proveedor deberá incluir todos los cables eléctricos que permitan la interconexión eléctrica de toda la solución ofertada y de manera redundante. Adicionalmente deberá incluir los rieles de montaje para rack estándar de centro de datos.
Consola o interface web de administración	El equipo de almacenamiento se deberá entregar con licenciamiento de tipo perpetuo y a nombre del Ministerio de Salud Pública del Ecuador. Debe permitir la administración de la solución ofertada, desde una consola (interface gráfica) o desde un browser, para toda la capacidad requerida. Protocolos Web-based GUI; SSH CLI; SMI-S; SNMP

<table>
<tr><td>Administración, monitoreo y estadísticas de desempeño</td><td>El software de administración del equipo de almacenamiento ofertado deberá: dotar de estadísticas para un rápido diagnóstico, solución de problemas y optimización de la carga. Visualizar en tiempo real el desempeño de I/O tanto en escritura como de lectura. Visualizar en tiempo real el uso de: CPU, sistema cache, discos, red y volúmenes. soporte de SMI-S. Soporte de SNMP.</td></tr>
<tr><td>Servicios y garantía</td><td>Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 24x7x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 24x7x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor.
La garantía técnica de fabricante (incluido el periodo de extensión de garantía técnica) deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio incluido sin ningún costo adicional para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública.</td></tr>
<tr><td>Servicios y garantía</td><td>El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de micro código (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.</td></tr>
<tr><td>Servicios de Horas de Soporte Especializado</td><td>El proveedor, como parte de adquisición del equipamiento, proporcionará un pool de 40 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica) sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la infraestructura de procesamiento y software relacionado, que se encuentra detallado en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):
<table>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo Respuesta para iniciar trabajos de soporte especializado</th><th>Tipo Soporte</th></tr>
<tr><td rowspan="2">Alta</td><td rowspan="2">Se requiere del soporte especializado canal para solventar</td><td>Hasta 2 horas</td><td>Remoto y/o Teléfono</td></tr>
<tr><td>De 3 – 4 horas</td><td>En sitio</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td>requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.</td><td></td><td></td></tr>
<tr><td>Moderada</td><td>Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.</td><td>5 – 6 horas</td><td>En sitio, Remoto o Telefónico</td></tr>
<tr><td>Baja</td><td>Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.</td><td>24 horas</td><td>En sitio, Remoto o Telefónico</td></tr>
</table>
Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.
Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.
</td></tr>
<tr><td>Servicios de fábrica</td><td>El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas:

El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:</td></tr>
</table>

NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA						
Prioridad	**Descripción**	**Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente**	**Modalidad de comunicación**	**Tiempo máximo de diagnóstico del incidente o problema**	**Forma de Trabajo, para diagnóstico o solución**	**Tiempo de Cambio de Repuestos y solución a incidentes.**
Alta	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.	2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	4 horas posteriores al resultado del diagnóstico
Media	Herramienta continúa en funcionamiento, causa molestias pero no se paralizar	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o	12 horas posteriores al resultado del diagnóstico

		á la producción en el corto plazo		registro respectivo.	contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	resolución de incidente	
	Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico
Documentación	El proveedor deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de cada uno de los componentes de hardware y software que conforman la solución en forma detallada a manera de procedimiento técnico documentado. Este manual técnico debe permitir la re instalación de cualquier componente de hardware y/o software que conforman la solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.						
Transferencia de Conocimientos	El proveedor deberá realizar la transferencia de conocimientos en el manejo y administración de toda la solución a adquirirse tanto del hardware como software/firmware del equipamiento y configuraciones realizadas; para un mínimo de 5 analistas que la DNTIC designe. La						

	transferencia de conocimientos se deberá organizar en dos grupos de funcionarios y los horarios serán coordinados con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública, con una duración mínima de 20 horas por grupo. Se deberá incluir y documentar una capacitación en todas las funcionalidades o features del equipo ofertado. Al finalizar la transferencia se deberá entregar un certificado de culminación a cada participante.

f) Solución de Almacenamiento para Base de Datos

SISTEMA DE ALMACENAMIENTO DE BDD	
El cumplimiento de todas y cada una de las especificaciones debe ser completamente respaldado con catálogos, manuales, hojas técnicas de los equipos ofertados, los cuales deben adjuntarse obligatoriamente a la oferta en formato digital.	
PARÁMETRO	**ESPECIFICACIONES SOLICITADAS**
Cantidad:	Uno
Marca:	El oferente deberá especificar la marca del equipo de almacenamiento ofertado el cual debe estar en el cuadrante de líderes de Gartner.
Modelo:	El oferente deberá especificar el modelo del equipo ofertado.
Condiciones de equipo	El equipo ofertado deberá ser nuevo de fábrica, (No re-manufacturados) última tecnología o generación liberada por el fabricante, con año de fabricación mínimo 2021.
Arquitectura	El equipo ofertado deberá incluir como mínimo dos controladoras o nodos redundantes en clúster activo-activo, sin punto único de falla, sus componentes deben ser independientes y redundantes de procesador, memoria cache, puertos hacia los hosts, puertos hacia los discos. Deberá soportar crecimiento de controladoras en cluster.
Disponibilidad del equipo	El equipo ofertado debe garantizar una disponibilidad de mínimo el 99.999%, para lo cual el oferente deberá adjuntar un certificado del fabricante. Redundancia en rutas de datos, fuentes de alimentación, conexiones de unidades y controladoras de almacenamiento, todos con funcionalidades de reemplazo en caliente sin que esto afecte al rendimiento del equipo. Las actualizaciones de firmware, parches o sistema operativo no deberán implicar la salida de servicio o afectación a la operación del sistema de almacenamiento.
Número de puertos	El equipo ofertado deberá contar con el siguiente número de puertos de host: Mínimo 8 puertos fibra canal de 16 Gbps o superior, los puertos no deben estar en switchs integrados al sistema de almacenamiento. Para administración LAN: al menos 2 puertos de 1 Gbps.
Memoria cache	El equipo ofertado deberá tener instalado mínimo 32GB de memoria cache por cada controladora expandible a mínimo 128GB. El equipo de almacenamiento deberá incluir mecanismos que garanticen la permanencia de la información en un dispositivo permanente (no volátil) en el caso de falta en el suministro de energía.
Volúmenes	Debe permitir la creación de volúmenes con mínimo los siguientes modos de ahorro de capacidad: Ningún ahorro, aprovisionamiento ligero, compresión.
Tipos de discos soportados	SAS, SSD, NL-SAS, Flash System
Niveles raid soportados	El equipo ofertado deberá soportar como mínimo niveles de raid 0, 1, 5, 6, 1+0.
Capacidad inicial	Debe incluir mínimo 50TB de capacidad efectiva en discos de tipo Estado Sólido (SSD - 12 Gbps) y mínimo 30 TB de capacidad efectiva requerida en

requerida/ Tipo de Tecnología de Discos	discos sobre tecnología rotacional (SAS a 15K RPM - 12 Gbps). La capacidad efectiva debe ser calculada sobre RAID 6 para ambas capacidades y tecnologías de disco.
Hot Spare	Si, debe incluir como mínimo 6 discos adicionales por cada uno de los tipos de tecnología de discos requerida, para asignar a Hot Spare. El sistema de almacenamiento debe asignar automáticamente las unidades Hot Spare en caso de requerirse.
Aprovisionamiento virtual	El sistema de almacenamiento debe permitir el aprovisionamiento virtual, es decir asignar mayor capacidad de la que dispone físicamente.
Sistemas operativos soportados	z/VM, z/VSE, AIX, VIOS, IBM i, HP-UX, Solaris, Linux, NetWare, MacOS, Windows, Citrix Xen, VMware
Características SAN	El equipo deberá soportar ambiente unificados de SAN, deberá soportar protocolos FC , iSCSI,
Clones y Snapshot's	El equipo de almacenamiento deberá incluir una herramienta, que permita realizar copias tipo clones y Snapshot's de escritura, para LUN's individuales y de un grupo de LUN's asociadas a un equipo, a fin de generar otros ambientes, almacenando solo los datos modificados. Licenciada en toda la capacidad requerida.
Migración	El equipo debe incluir herramienta de migración de datos a través de la SAN y dicha migración debe ser en forma no disruptiva.
Movimiento datos	El equipo de almacenamiento deberá entregar el movimiento de datos en forma no disruptiva, desde los diferentes tipos de discos instalados: SAS y SSD.
Replicación remota	El equipo de almacenamiento deberá incluir la configuración de réplicas consistentes tanto locales como remotas
Thin provisioning	El equipo de almacenamiento se deberá entregar y estar configurado en toda la capacidad requerida.
Fuente de poder y ventiladores	El equipo de almacenamiento deberá incluir fuentes de poder 100-240 VAC y ventiladores redundantes hot-swap. El tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC-320 C13/14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del MSP.
Conectividad con Housing	El Proveedor deberá etiquetar y peinar todo el cableado de FO y Cobre solicitado en este apartado, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo a los lineamientos de la Corporación Nacional de Telecomunicaciones y la DNTIC. Todo el cableado de FO y Cobre que el Proveedor instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes de mínimo 5 años.
Cables de poder y adicionales	El proveedor deberá incluir todos los cables eléctricos que permitan la integración a la red eléctrica, de toda la solución ofertada y de manera redundante. Adicionalmente deberá incluir los rieles de montaje para rack estándar de centro de datos.
Consola o interface web de administración	El equipo de almacenamiento se deberá entregar con licenciamiento de tipo perpetuo y a nombre del Ministerio de Salud Pública del Ecuador. Debe permitir la administración de la solución ofertada, desde una consola (interface gráfica) o desde un browser, para toda la capacidad requerida. Protocolos Web-based GUI; SSH CLI; SMI-S; SNMP
Administración, monitoreo y estadísticas de	El software de administración del equipo de almacenamiento ofertado deberá: dotar de estadísticas para un rápido diagnóstico, solución de problemas y optimización de la carga. Visualizar en tiempo real el desempeño de I/O tanto en escritura como de lectura. Visualizar en tiempo real el uso de: CPU, sistema cache, discos, red y volúmenes. soporte de SMI-S. Soporte de SNMP.

<table>
<tr><td>desempeño</td><td>Adicionalmente deberá disponer de las siguientes características generales:
Licenciamiento perpetuo
Software de administración accesible vía HTML-5</td></tr>
<tr><td>Servicios de notificación de eventos</td><td>El equipo de almacenamiento deberá incluir la funcionalidad de notificación en forma automática vía email, de los eventos. adicionalmente, deberá enviar el estado del equipo hacia el centro de soporte del fabricante.</td></tr>
<tr><td>Servicios y garantía</td><td>Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas, deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 24x7x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 24x7x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor. La garantía técnica de fabricante (incluido el periodo de extensión de garantía técnica) deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio sin ningún costo adicional para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública.</td></tr>
<tr><td>Servicios y garantía</td><td>El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de micro código (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.</td></tr>
<tr><td>Horas de Soporte Especializado</td><td>El proveedor como parte de adquisición del equipamiento proporcionará un pool de 40 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica) sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la infraestructura de procesamiento y software relacionado, que se encuentra detallado en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):
<table>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo Respuesta para iniciar trabajos de soporte especializado</th><th>Tipo Soporte</th></tr>
<tr><td rowspan="2">Alta</td><td rowspan="2">Se requiere del soporte especializado canal para solventar requerimientos</td><td>Hasta 2 horas</td><td>Remoto y/o Teléfono</td></tr>
<tr><td>De 3 – 4 horas</td><td>En sitio</td></tr>
</table>
</td></tr>
</table>

		determinados por el Administrador del Contrato como urgentes y de alta necesidad.		
	Moderada	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.	5 – 6 horas	En sitio, Remoto o Telefónico
	Baja	Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.	24 horas	En sitio, Remoto o Telefónico

Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.

Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.

Servicios y garantía	El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas: El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo,

queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA						
Prioridad	**Descripción**	**Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente**	**Modalidad de comunicación**	**Tiempo máximo de diagnóstico del incidente o problema**	**Forma de Trabajo, para diagnóstico o solución**	**Tiempo de Cambio de Repuestos y solución a incidentes.**
Alta	Herramienta en producción se paraliza	Treinta (30) minutos	Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.	2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	4 horas posteriores al resultado del diagnóstico
Media	Herramienta continúa en funcionamiento, causa molestias pero no se paralizará la	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratis	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de	12 horas posteriores al resultado del diagnóstico

		producción en el corto plazo		respectivo.	ta en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	incidente	
	Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico
Documentación	El proveedor deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de *cada uno de los componentes de hardware y software que conforman la solución en forma detallada a manera de procedimiento técnico documentado*. Este manual técnico debe permitir la re instalación de cualquier componente de hardware y/o software que conforman la solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.						
Transferencia de Conocimientos	El proveedor deberá realizar la transferencia de conocimientos en el manejo y administración de toda la solución a adquirirse tanto del hardware como software/firmware del equipamiento y configuraciones realizadas; para un mínimo de 5 analistas que la DNTIC designe. La transferencia de conocimientos se deberá organizar en dos grupos de funcionarios y los horarios serán coordinados con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública, con una duración mínima de 20 horas por grupo. Se deberá incluir y documentar una						

	capacitación en todas las funcionalidades o features del equipo ofertado. Al finalizar la transferencia se deberá entregar un certificado de culminación a cada participante.
SWITCHS SAN	
El cumplimiento de todas y cada una de las especificaciones debe ser completamente respaldado con catálogos, manuales hojas técnicas de los servicios o software asociado al servicio, los cuales deben adjuntarse obligatoriamente a la oferta en formato digital.	
ESPECIFICACIONES TÉCNICAS SOLICITADAS	
Cantidad	Dos equipos
Modelo	Especificar, el equipo ofertado deberá ser nuevo de fábrica, (No re-manufacturados) última tecnología o generación liberada por el fabricante, con año de fabricación mínimo del 2021
Marca	Especificar
Tamaño de cada equipo	1 Unidad de Rack
Tecnologías de soporte en puertos FC	Cada switch dispondrá de puertos con soporte para las siguientes tecnologías y/o anchos de banda: 4, 8, 16, 32 Gbps FC.
Capacidad	Cada Switch deberá poseer mínimo 24 puertos capaces de operar a 16, 32 Gbps FC según sea la necesidad y con sus respectivos transceivers incluidos.
Buffer del equipo	Cada switch tendrá un tamaño de buffer de mínimo de 15.360
Ancho de banda del equipo	Cada switch tendrá un ancho de banda de mínimo de 2TB/s
Cada switch debe soportar como mínimo las siguientes características de networking.	AES-GCM-256 encryption on ISLs DH-CHAP FCAP switch aurthentication HTTPS IPsec IP filtering LDAP with IPv6 OpenLDAR Port Binding, RADIUS TACACS+ User-defined Role-based Access Control (RBAC) Secure Copy (SCP) Secure RPC Secure Syslog SSH v2 SSL Switch Binding Trusted Switch
Fuente de poder y ventiladores	Obligatorio. Adicionalmente el tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC-320 C13/14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del MSP.
Cables de poder y adicionales	El proveedor deberá incluir todos los cables eléctricos que permitan la integración a la red eléctrica de toda la solución ofertada. Adicionalmente deberá incluir los rieles de montaje para rack estándar de centro de datos.
Conectividad a Housing	El Proveedor deberá entregar como mínimo 4 patch cords UTP 6A administrables. La longitud de los cables debe ser la adecuada para permitir una organización y peinado eficientes en cada rack, se debe garantizar el radio

	de curvatura indicado en las especificaciones técnicas de los cables. El Proveedor deberá etiquetar y peinar todo el cableado de Cobre solicitado en este apartado, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo a los lineamientos de la Corporación Nacional de Telecomunicaciones y la DNTIC. Todo el cableado de Cobre que el Proveedor instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes de mínimo 5 años.
Licenciamiento y Consola o interface web de administración	Los equipos Switch SAN se deberán entregar con licenciamiento perpetuo para toda la capacidad requerida y a nombre del Ministerio de Salud Pública del Ecuador. Para administración de la solución ofertada se deberá disponer de una consola (interface gráfica) o desde un browser, Protocolos Web-based GUI, SSH CLI, SNMP
Servicios y garantía	Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 24x7x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 24x7x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor. La garantía técnica de fabricante (incluido el periodo de extensión de garantía técnica) deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio incluido sin ningún costo adicional para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública.
Servicios y garantía	El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de micro código (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.
Servicios y garantía	El proveedor como parte de adquisición del equipamiento proporcionará un pool de 20 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica) sin costo adicional para el Ministerio de Salud Pública. Estas horas de soporte servirán para ejecutar eventuales reconfiguraciones, adicionamiento de nuevas funcionalidades y en general cualquier requerimiento que plantee el Ministerio de Salud Pública del Ecuador relacionado a la administración y operación/reconfiguración de la infraestructura de procesamiento y software relacionado, que se encuentra detallado en este documento. Se establecen los siguientes horarios de soporte (SLA). El soporte técnico deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):

Prioridad	Descripción	Tiempo Respuesta para iniciar trabajos de soporte especializado	Tipo Soporte
Alta	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.	Hasta 2 horas	Remoto y/o Teléfono
		De 3 – 4 horas	En sitio
Moderada	Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.	5 – 6 horas	En sitio, Remoto o Telefónico
Baja	Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.	24 horas	En sitio, Remoto o Telefónico

Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01 PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.

Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.

Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.

<table>
<tr>
<td>Servicios y garantía</td>
<td>
El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas:

El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

<table>
<tr><th colspan="7">NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA</th></tr>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente</th><th>Modalidad de comunicación</th><th>Tiempo máximo de diagnóstico del incidente o problema</th><th>Forma de Trabajo, para diagnóstico o solución</th><th>Tiempo de Cambio de Repuestos y solución a incidentes.</th></tr>
<tr><td>Alta</td><td>Herramienta en producción se paraliza</td><td>Treinta (30) minutos</td><td>Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.</td><td>2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365</td><td>Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente</td><td>4 horas posteriores al resultado del diagnóstico</td></tr>
<tr><td>Media</td><td>Herramienta continúa</td><td>Cuarenta y cinco (45)</td><td>Vía telefónica y/o e-</td><td>4 horas posteriores a la</td><td>Respuesta inicial</td><td>12 horas posteri</td></tr>
</table>
</td>
</tr>
</table>

		en funcionamiento, causa molestias pero no se paralizará la producción en el corto plazo	minutos	mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	ores al resultado del diagnóstico
	Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico
Documentación	El proveedor deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de cada uno de los componentes de hardware y software que conforman la solución de Switches SAN, en forma detallada, a manera de procedimiento técnico documentado. Este manual técnico debe permitir la re instalación/re configuración de cualquier componente de hardware y/o software/firmware que conforman la						

	solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.
Transferencia de Conocimientos	El proveedor deberá realizar la transferencia de conocimientos en el manejo y administración de toda la solución a adquirirse tanto del hardware como software/firmware del equipamiento y configuraciones realizadas; para un mínimo de 5 analistas que la DNTIC designe. La transferencia de conocimientos se deberá organizar en dos grupos de funcionarios y los horarios serán coordinados con la Dirección Nacional de Tecnologías de la Información y Comunicaciones del Ministerio de Salud Pública, con una duración mínima de 10 horas por grupo. Se deberá incluir y documentar una transferencia en todas las funcionalidades o features del equipo ofertado. Al finalizar la transferencia se deberá entregar un certificado de culminación a cada participante.

g) Balanceador de Carga

ESPECIFICACIONES TÉCNICAS SOLICITADAS	
Solución de balanceo de carga basado en Appliance físico o Hardware	Se requiere la implementación de dos (2) balanceadores tipo “Appliance” físico. El proveedor deberá incluir los servicios de instalación de la solución de balanceo de carga descrita en este documento, con la finalidad de dejarla operativa y lista para la implementación de políticas de balanceo conforme a los requerimientos y necesidades que la DNTIC del MSP plantee dentro de la implementación. Esto incluye la instalación de certificados SSL provistos por el MSP, configuración de networking, VLANs, etc.
Condiciones de equipo	Los equipos ofertados deberán ser nuevos de fábrica, (No re-manufacturados) última tecnología o generación liberada por el fabricante, con año de fabricación mínimo 2021
Parámetros de Calidad/ Madurez de la Solución	La solución ofertada debe encontrarse en el diagrama de líderes de Gartner al menos por los últimos 10 años. El Proveedor deberá incluir la documentación que se requiera para evidenciar lo solicitado en este párrafo.
Alta Disponibilidad - HA	La solución debe contemplar la capacidad de configurarse en Alta Disponibilidad: Activo/Pasivo o Activo/Activo. En Ambos casos la configuración se debe aplicar en un solo nodo y replicada al restante. El Proveedor deberá incluir la configuración de alta disponibilidad de los equipos balanceadores requeridos en este documento. Adicionalmente deberá incluir cualquier otro hardware/software o firmware que se requiera para la implementación de HA.
Balanceo de carga	La solución deberá tener la posibilidad de detectar y compensar la sobrecarga de solicitudes a los servidores para no evidenciar lentitud y/o indisponibilidad de servicio.
Capacidad	La solución debe soportar al menos 400.000 HTTP requests por segundo.
Crecimiento	La solución ofertada debe tener la capacidad de crecimiento sin necesidad de cambiar el appliance físico, para soportar como mínimo 900.000 HTTP requests por segundo.
Servicios de soporte incluidos dentro de la solución de balanceo	El proveedor, como parte de adquisición del equipamiento, proporcionará un pool de 80 horas de soporte técnico especializado canal mientras dure la garantía de los equipos (incluido el periodo de extensión de garantía técnica) sin costo adicional para el Ministerio de Salud Pública y de acuerdo al SLA detallado en estas especificaciones técnicas. Las horas de soporte podrán ser utilizadas para realizar el análisis, diseño, migración/reconfiguración de reglas de balanceo, red, Interfaces, VLANs, Rutas, DNS, direcciones IPs, puertos de servicio, usuarios y roles, y en general para solventar cualquier configuración o requerimientos planteado por el MSP, relacionados con la operación y despliegue de los balanceadores y funcionalidades adicionales que incluya el “Appliance”.
Transferencia de Conocimiento	El Proveedor deberá incluir la transferencia de conocimiento de toda la solución de balanceo para cinco (5) analistas de la DNTIC. La transferencia de conocimientos deberá estar enfocada en el manejo y configuración de todas las “features” o funcionalidades del software/firmware del “Appliance” ofertado, incluidas las funcionalidades de Web App Firewall, configuración de reglas de balanceo, troubleshooting, interpretación de logs del sistema, configuración de interfaces, y en general todas las características técnicas correspondientes al modelo de “Appliance”

	ofertado por el Proveedor. La transferencia deberá durar como mínimo 60 horas. Se deberá entregar un certificado de culminación a cada participante al finalizar la transferencia.
Throughput general del sistema de balanceo	La solución ofertada debe soportar al menos un Throughput Nominal de 1 Gbps para balanceo en condiciones de máxima carga. El equipo deberá tener la capacidad de crecer hasta un máximo de 10 Gbps sin necesidad de adicionar más hardware.
Interfaces	Cada equipo debe incluir al menos 2 puertos 10G Ethernet SFP+ y 6 puertos 1000BASE-X. Debe soportar transceivers: 10G Ethernet SFP+: SR, LR. El Proveedor debe incluir los transceivers para todos los puertos requeridos en este apartado.
Interconexión con Housing	El Proveedor deberá entregar como mínimo 8 patch cords de fibra óptica multimodo conector LC/LC y 8 patch cords UTP 6A administrables. La longitud de los cables debe ser la adecuada para permitir una organización y peinado eficientes en cada rack, se debe garantizar el radio de curvatura indicado en las especificaciones técnicas de los cables. El Proveedor deberá etiquetar y peinar todo el cableado de FO y Cobre solicitado en este apartado, dentro de los racks designados por el Ministerio de Salud Pública para la interconexión de los equipos requeridos, de acuerdo a los lineamientos de la Corporación Nacional de Telecomunicaciones y la DNTIC. Todo el cableado de FO y Cobre que el Proveedor instale, deberá contar con certificación de categoría y una garantía técnica sobre todos sus componentes de mínimo 5 años
Interconexión	Para patch cords LAN RJ45, se debe considerar de categoría 6A Administrable. Los patch cords de Fibra Óptica deberán ser de tipo LC-LC OM3.
Fuentes de Poder y Cables eléctricos	La solución ofertada debe contar con fuentes de poder redundantes, entradas de voltaje de 100 a 240 VAC. Adicionalmente el tipo de conector de los cables de interconexión eléctrica (terminal que se conectará a la PDU del Rack) deberán ser de tipo IEC-320 C13/14 debido a restricciones de tomas disponibles dispuestas por el proveedor de Housing del MSP.
Características físicas	El equipo ofertado debe tener una altura no mayor a 2 unidades de Rack.
Funciones de administración de tráfico	Soporte de switching y balanceo en capas L4-L7 para servicios IP
	El servicio ofertado deberá realizar funciones de Balanceo de Tráfico de aplicaciones basadas en IP (TCP, UDP) y Servicios Web.
	La solución ofertada deberá soportar al menos los siguientes protocolos Capa 7 (Aplicación): FTP, SFTP, MQ, HTTP, HTTPS, DNS (TCP and UDP), SIP (over UDP), RTSP, RADIUS, DIAMETER, SQL, RDP, IS-IS, POP, IMAP, TLS, SMTP, NTP.
	La solución debe permitir la definición de dirección IP y puerto virtual para la prestación de un servicio, que permita atenderlo mediante una granja de servidores identificados mediante una dirección IP y un puerto del servicio igual o diferente del presentado al público.
	La solución debe permitir hacer control de balanceo de tráfico local o global según se defina con varios tipos de algoritmos especializados definidos en la solución de balanceo: - Round Robin - Respuesta rápida - Conexiones mínimas - Análisis de carga - Hash de URL
	La solución debe ser capaz de identificar fallos en servidores y servicios especificados para redundancia de las aplicaciones.
	La solución debe realizar monitoreo de la salud de los Servidores que gestione el appliance de Balanceo de tráfico, por medio de: - Ping. - Chequeo a nivel de TCP y UDP a puertos específicos

	- Monitoreo HTTP y HTTPS - Verificación de la salud de una combinación de servicios, permitiendo tomar la decisión del estado de salud aplicando varios monitores simultáneos. - Configurar monitores predefinidos y personalizados que permitan comprobar y verificar la salud y disponibilidad de los componentes de la aplicación y de la red. - Monitoreo en línea, donde el funcionamiento de la aplicación determine el estado de salud de la misma
	La solución deberá soportar el Monitoreo de aplicaciones/protocolos del mercado: LDAP, FTP, DNS, SMTP, POP3, MySQL, RADIUS, SIP, SNMP.
	Deberá permitir hacer persistencia de conexiones hacia la aplicación con base en cualquier información contenida en cualquier parte del paquete completo, esto para poder adaptar la solución a las necesidades de las diferentes aplicaciones. El control de persistencia de las conexiones se debe realizar por los siguientes métodos: - Dirección IP origen - Dirección IP destino - Cookies - SIP: Debe permitir definir el campo SIP sobre el cual hacer persistencia - Sesiones SSL
	La solución debe tener la capacidad de ampliarse para soportar la creación de Clúster geográficos (GSLB), con el objetivo de habilitar alta disponibilidad entre Data Centers o sitios en nube.
Funciones de aceleración de tráfico	La solución debe incluir la capacidad de compresión de tráfico a nivel de aplicaciones
	La solución debe ofrecer características de compresión de tráfico: - El sistema deberá permitir compactar el tráfico http a través del estándar GZIP, Deflate y compatible con browsers MS Internet Explorer, Google Chrome, Mozilla Firefox, Safari, etc. - La solución debe permitir la optimización del tráfico TCP - Cliente Servidor. - La solución debe permitir la administración y almacenamiento en memoria cache de contenido web.
Funciones de Seguridad	Soporte de seguridad SSL: - La solución debe incluir el soporte de Aceleración SSL - La solución debe soportar mínimo 1.300 transacciones por segundo SSL con llaves de 2048 bits - La solución debe tener la capacidad de soportar mínimo 1 Gbps de Throughput SSL. - Soporte de llaves SSL de 1024, 2048 y 4096 bits
	La solución ofertada debe manejar AES256; SHA1/MD5 y soporte a algoritmos de llave pública: RSA, Diffie-Hellman
	La solución ofertada debe incluir protección y licencias contra ataques de DoS para las capas L4/L7
	La solución ofertada debe incluir un portal para la autenticación de tráfico HTTP integrable con fuentes de autenticación externa.
	La solución debe incluir un firewall de aplicaciones que permita cumplir con el standard PCI-DSS.
	La solución ofertada debe disponer de un firewall de aplicaciones que debe incluir firmas que se puedan auto-actualizar en el tiempo.
	La solución ofertada debe estar preparada para poder cubrir los siguientes ataques: o Buffer overflow o Manipulación de CGI o Manipulación de campos de HTML o Envenenamiento de Cookies o Ataques de tipo XSS o Inyección de comandos SQL o Robo de información sensitiva o Errores de configuración de servidores o Ataques de SOAP o Filtrado de contenido

	La solución ofertada debe permitir la configuración de reputación de IP. La solución ofertada debe soportar el análisis y control de tráfico SSL mediante un PROXY que cuente la herramienta
Estándares de Red	La solución ofertada debe Soportar VLAN 802.1q, VLAN tagging
	La solución ofertada debe Soportar de 802.3ad para definición de múltiples troncales
	La solución ofertada debe disponer de Soporte de protección ante picos de demanda y colas de prioridad.
	La solución deberá soportar el protocolo RISE para la integración con switches de varios fabricantes de la industria
Administración del Sistema	La solución debe permitir el acceso para la administración del equipo appliance vía CLI (Interfaz de línea de comandos) por SSH2, interfaz de administración gráfica basada en Web seguro (HTTPS).
	La solución ofertada debe integrarse con Directorio Activo Windows 2008 o superior, LDAP, RADIUS. Debe incluir el licenciamiento del software requerido para la autenticación de administradores/supervisores al equipo.
	La solución ofertada debe incluir comunicación cifrada para acceder a la administración de la solución de manera segura
Reportes	La solución ofertada debe incluir reportes para la visibilidad de las principales variables.
	La solución debe permitir dar visibilidad del balanceo del tráfico web, para identificar las aplicaciones más utilizadas, las URLs accedidas, los clientes con más accesos y los servidores más requeridos.
	La solución ofertada debe permitir dar visibilidad del acceso a las aplicaciones y escritorios virtualizados por VirtualApps y VirtualDesktops, para identificar datos de los usuarios como ancho de banda consumido y latencia, además de las aplicaciones y escritorios accedidos
Visibilidad	La solución ofertada debe integrar una herramienta que proporcione visibilidad para obtener información que permita facilitar la gestión del Departamento de IT.
	La herramienta que forme parte de la solución debe proporcionar la información de manera gráfica, de tal forma que permita identificar de manera más rápida y oportuna, alguna falla/anomalía en la entrega del servicio al usuario final.
	La solución ofertada debe disponer de una consola de administración centralizada en donde se puedan ver y administrar los equipos.
	La solución debe almacenar un historial del monitoreo de las aplicaciones web configuradas en la herramienta.
	El Proveedor deberá incluir la instalación de una solución para realizar el análisis exhaustivo del estado, el rendimiento y la seguridad de las aplicaciones; permita la administración, monitoreo, análisis y resolución de los problemas de los “Appliances” de balanceo de carga, desde una consola unificada. El Proveedor deberá incluir, las tareas de instalación y configuración de esta solución dentro de una máquina virtual a ser provista por el MSP, de acuerdo a los lineamientos y necesidades planteadas por la institución y las recomendaciones del fabricante. El Ministerio de Salud Pública del Ecuador, proveerá los recursos de procesamiento, memoria RAM y almacenamiento dentro de su centro de datos y que serán necesarios para la instalación de la solución requerida en este apartado.
Servicios y garantía	Todo el hardware, software y firmware que conforman la solución requerida en estas especificaciones técnicas deberán disponer de una garantía técnica de fabricante vigente por 3 años en modalidad 24x7x365. Además, el Proveedor deberá incluir una extensión de la garantía técnica de fabricante por 2 años adicionales, en modalidad 24x7x365. El Ministerio de Salud Pública, ante un evento de aplicación de garantía técnica, se reservará el derecho de aplicar la misma directamente con el fabricante o por medio del Proveedor. La garantía técnica de fabricante (incluido el periodo de extensión de garantía técnica) deberá cubrir el reemplazo, en caso de fallas, de todas las partes y piezas que los conforman, con mano de obra y atención en sitio incluido sin ningún costo adicional

<table>
<tr><td></td><td>para el Ministerio de Salud Pública, en modalidad 24 horas los 7 días de la semana y con un tiempo de reemplazo de partes y piezas de máximo 4 horas contadas a partir de la apertura del incidente por parte del Ministerio de Salud Pública. El proveedor se encargará de tramitar cualquier cambio de partes (RMA) ante el fabricante, sin costo adicional para el Ministerio de Salud Pública.</td></tr>
<tr><td>Servicios y garantía</td><td>El proveedor realizará dos mantenimientos preventivos presenciales anuales de toda la infraestructura de hardware detallada en este documento y mínimo una actualización anual de micro código (firmware), durante la vigencia de la garantía técnica de fábrica (incluido el periodo de extensión de garantía técnica); sin costo adicional para el Ministerio de Salud Pública. La fecha y hora de ejecución de estas actividades serán definidas por la DNTIC del Ministerio de Salud Pública con la finalidad de causar el menor impacto en sus operaciones tecnológicas.</td></tr>
<tr><td>Servicios de Soporte- SLA de Horas de Soporte</td><td>El soporte técnico especializado deberá estar disponible para el Ministerio de Salud Pública en el horario de 8:00 a 17:00 bajo esquema 8x5x365 sin perjuicio de aplicarse fuera del horario definido anteriormente para lo cual se aplicará el siguiente nivel de servicio (SLA Horas de Soporte):
<table>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo Respuesta para iniciar trabajos de soporte especializado</th><th>Tipo Soporte</th></tr>
<tr><td rowspan="2">Alta</td><td rowspan="2">Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como urgentes y de alta necesidad.</td><td>Hasta 2 horas</td><td>Remoto y/o Teléfono</td></tr>
<tr><td>De 3 – 4 horas</td><td>En sitio</td></tr>
<tr><td>Moderada</td><td>Se requiere del soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como moderados o de necesidad media.</td><td>5 – 6 horas</td><td>En sitio, Remoto o Telefónico</td></tr>
<tr><td>Baja</td><td>Se requiere de soporte especializado canal para solventar requerimientos determinados por el Administrador del Contrato como programados o de necesidad baja.</td><td>24 horas</td><td>En sitio, Remoto o Telefónico</td></tr>
</table>
Esquema de horarios de atención y consumo de horas de soporte:

Las horas de soporte técnico ejecutadas fuera del horario de oficina (de 17:01</td></tr>
</table>

<table>
<tr><td></td><td>PM a 07:59 AM del siguiente día) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas fuera del horario de oficina (fines de semana durante todo el día y la noche) se contabilizan por una hora y media.
Las horas de soporte técnico ejecutadas en días feriados (determinados oficialmente por el Gobierno Ecuatoriano) (durante todo el día y la noche) se contabilizan por dos horas.

Las horas de soporte técnico ejecutadas en días normales de trabajo, en horario de oficina (de 8:00 AM a 17:00 PM) se contabilizan por una (1) hora.</td></tr>
<tr><td>Servicios y garantía de Fabricante</td><td>El tiempo de respuesta ante fallas de hardware, software y firmware que conforman la solución, durante el período contratado, deberá tener las siguientes características mínimas:

El proveedor deberá dar atención en el análisis de daños y resolución de incidentes que se presenten en la infraestructura de hardware, software y firmware detallada en este documento. Las actividades serán ejecutadas por el proveedor del servicio, y de ser necesario, en asistencia del fabricante de los equipos sin ningún costo para el Ministerio de Salud Pública; sin embargo, queda bajo criterio del Ministerio de Salud Pública aplicar el siguiente SLA:

<table>
<tr><th colspan="7">NIVELES DE SERVICIO PARA SOPORTE Y MANTENIMIENTO HARDWARE DE INFRAESTRUCTURA ACTUALIZADA</th></tr>
<tr><th>Prioridad</th><th>Descripción</th><th>Tiempo máximo de Respuesta Inicial (comunicación inicial), posterior a apertura de Ticket de Incidente</th><th>Modalidad de comunicación</th><th>Tiempo máximo de diagnóstico del incidente o problema</th><th>Forma de Trabajo, para diagnóstico o solución</th><th>Tiempo de Cambio de Repuestos y solución a incidentes.</th></tr>
<tr><td>Alta</td><td>Herramienta en producción se paraliza</td><td>Treinta (30) minutos</td><td>Vía telefónica, y/o e-mail, al contacto indicado por el Proveedor, para constancia y registro respectivo.</td><td>2 horas posterior a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad</td><td>Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente</td><td>4 horas posteriores al resultado del diagnóstico</td></tr>
</table>
</td></tr>
</table>

					7x24x365		
	Media	Herramienta continúa en funcionamiento, causa molestias pero no se paralizará la producción en el corto plazo	Cuarenta y cinco (45) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	4 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	12 horas posteriores al resultado del diagnóstico
	Baja	Herramienta continúa en funcionamiento, si no se toman acciones, afectará a producción en corto plazo o mediano plazo.	Sesenta (60) minutos	Vía telefónica y/o e-mail, al contacto indicado por el proveedor, para constancia y registro respectivo.	6 horas posteriores a la comunicación inicial, o definido por mutuo acuerdo con la contratista en función de la complejidad y recursos necesarios para la atención. Modalidad 7x24x365	Respuesta inicial Telefónica y/o remoto. En sitio para diagnóstico y/o resolución de incidente	24 horas posteriores al resultado del diagnóstico
Documentación	El proveedor deberá entregar documentación de la arquitectura desplegada, así como manual técnico de instalación y configuración de cada uno de los componentes de hardware y software que conforman la solución, en forma detallada, a manera de procedimiento técnico documentado. Este manual técnico debe permitir la re instalación/re configuración de cualquier componente de hardware y/o software/firmware que conforman la solución ofertada, con base al procedimiento técnico documentado a ser entregado por el Proveedor.						

h) Firewall de Seguridad Perimetral

El firewall deberá considerar los aspectos necesarios para abastecer el volumen de recetas diarias estimadas en el requerimiento GEN-004, considerando el filtrado del de las peticiones para el servidor de aplicaciones, así como un filtrado para el servidor de base de datos.

El proveedor alineará su solución al firewall institucional del MSP, sin embargo, deberá proporcionar en su solución los mecanismos de seguridad necesarios para validar entradas

de datos (haciendo este componente las veces de firewall de base de datos) y evitar inyecciones de código malicioso en ellas, ya sea a nivel de código SQL como de código HTML, JavaScript, y el código que utilice su solución.

3.3 REQUERIMIENTOS DE SOPORTE Y MANTENIMIENTO

3.3.1 SOPORTE

- Se espera que el soporte y la operación se base en las buenas prácticas de ITIL, cubriendo la coordinación y ejecución de las actividades y procesos necesarios para que los servicios mantengan los niveles de disponibilidad y rendimiento acordados. Este soporte deberá tener un cubrimiento en soporte de 7x24x365. El proveedor debe indicar el gobierno de su servicio de soporte, los canales utilizados para solicitar dicho servicio (canales de comunicación) y matriz de escalamiento y responsabilidades.
- Se debe contar con un único punto de contacto entre los usuarios finales y el equipo de soporte con las siguientes características:
    - Proporcionar las herramientas necesarias para la prestación de los servicios de soporte al usuario final.
    - Establecer los flujos de proceso necesarios para la atención y resolución de todas las incidencias y/o peticiones que los usuarios finales escalen, garantizando en todo momento el cumplimiento de los ANS establecidos.
    - Establecer los niveles de soporte que garanticen una correcta asistencia al usuario, permitiendo el escalamiento de los casos (petición o incidencia) a niveles de soporte de acuerdo con la complejidad de la solución.
- El soporte de segundo y tercer nivel estará a cargo del proveedor de la o las soluciones que contemple el presente pliego, de manera similar los subsistemas, servicios web y/o interfaces que hagan parte general e integral del presente pliego estarán a cargo del proveedor en todos los ambientes que se dispongan para cubrir las peticiones del MSP, de esto se deberá hacer cargo el proveedor desde el día cero de los despliegues en cada uno de los diferentes ambientes, bajo los lineamientos y políticas del MSP.
- El soporte desde el proveedor deberá cubrir tanto incidentes, eventos y la liberación de nuevas versiones de la o las soluciones.
- Las aplicaciones, módulos e integraciones que hagan parte de la solución ofrecida, deben estar monitorizadas por la o las herramientas que deberá disponer el proveedor tanto a nivel de aplicación como de hardware y software base, teniendo presente que se debe visualizar rendimiento particular de la aplicación, poder hacer seguimiento a nivel de código de la misma, medir la experiencia de usuario y efectuar el monitoreo de rendimiento, funcionalidad y disponibilidad de la plataforma y la solución integralmente.
- El proveedor deberá proveer una consola de monitorización centralizada de fácil usabilidad e interpretación, donde se pueda visualizar el desempeño de la plataforma desde una perspectiva técnica y una perspectiva de negocio, todo esto enfocado hacia la identificación de la experiencia del usuario.
- El MSP podrá delegar la gestión y/o administración completa de la aplicación o aplicaciones e infraestructura, que conforman la solución al proveedor o un tercero quién debe tener la capacidad para atender la demanda que esto signifique, para ello, el proveedor deberá brindar las capacitaciones pertinentes en las herramientas e infraestructura que comprende la solución de manera integral, garantizando así la prestación del servicio dentro de los marcos de calidad y ANS esperados.
- Dentro de las tareas de administración se incluye:
    - Instalación de software nuevo o actualizar el existente
    - Cambio de configuración de hardware de los equipos
    - Realizar configuración de red
    - Gestionar cuentas de usuarios (creación, modificación, bloqueo, asignación permisos)

- Administrar almacenamiento local y compartido
- Generar diagnósticos y afinar el sistema operativo
- Configurar tareas programadas a nivel de sistema operativo o de base de datos
- Gestionar tareas de backup y restauración de información, teniendo presente que estas deben cubrir tanto datos, configuraciones y entornos virtuales.
- Indicar el tiempo de retención que se debe mantener la información en los sistemas de backup del proveedor.
- Generar los informes que soliciten los diferentes fabricantes (hardware y software)
- Generar los informes o reportes solicitados por auditorías internas o externas del MSP
- Control y Ejecución de despliegues de nuevas versiones y cambios de la solución programados o de emergencia
- Presentar y ejecutar plan de mantenimiento periódico de la solución
- Resolver los incidentes y requerimientos asociados a la solución que está administrando
- Escalar al fabricante para los incidentes que así lo requieran
- En el caso de detectar un correlacionamiento incorrecto, el proveedor deberá solucionarlo en un plazo inferior a 24 horas corridas y reprocesar toda la información a que hubiese lugar.
- Monitorización constante sobre el todo de la solución ofrecida
- Especificar las condiciones de backup y los datos a respaldar, de todas las herramientas que hagan parte de la solución integral, teniendo presente que las políticas a aplicar deben estar acordes con las políticas de la compañía.

3.3.2 MANTENIMIENTO CORRECTIVO

El mantenimiento correctivo se refiere a fallas, errores, defectos o funcionamientos diferentes a los requeridos, que se encuentren en desarrollos específicos, adaptaciones funcionales o parametrizaciones. Incluye el mantenimiento certificado de cada componente de hardware o software que requiera la solución implantada.

El proveedor deberá realizar el mantenimiento correctivo de los módulos de la solución, desde el momento en que se pongan en producción y hasta la entrega definitiva al MSP.

3.3.3 MANTENIMIENTO PREVENTIVO

El servicio de mantenimiento preventivo tiene como objetivo que el proveedor, de manera proactiva, revise el código y configuración de los sistemas de información de la solución propuesta, así como sus integraciones, e implemente la corrección de errores, sin que estos hayan sido reportados por el MSP. Dentro de las actividades requeridas para este fin, se deben incluir:

- Definición de reglas, umbrales máximos y mínimos, que definirán la necesidad de alertas de funcionamiento no adecuado de la solución (disponibilidad, tiempo de respuesta a solicitudes, almacenamiento)
- Implementación de una herramienta de monitoreo de la solución y sus interfaces.
- Identificación y gestión de los problemas e incidencias repetitivas (detección, resolución, seguimiento y documentación).
- Provisión de las herramientas y los desarrollos que automaticen las tareas de mantenimiento y faciliten el soporte y mantenimiento a través de la capa de aplicación.

- Comunicación a la gerencia del proyecto, por parte del MSP, sobre las nuevas versiones de la solución implantada y que supongan una mejora en la seguridad, en la estabilidad o en el funcionamiento de los distintos componentes.

3.3.4 MANTENIMIENTO ADAPTATIVO

- El proveedor debe incluir dentro de la propuesta una bolsa de horas que cubra los requerimientos de ley que puedan surgir durante la ejecución del proyecto, considerando lo siguiente:
  - El mantenimiento adaptativo deberá incluir las adaptaciones de las funcionalidades (parametrizaciones, adaptaciones funcionales y desarrollos específicos) ante requerimientos legales, normativos y organizativos.
  - El proveedor deberá realizar el mantenimiento adaptativo de la solución desplegada, hasta la entrega definitiva al MPS.
  - Para cada solicitud, el proveedor deberá realizar un análisis de impacto de los cambios requeridos y generar una oferta independiente. No se debe iniciar ningún mantenimiento adaptativo sin la aprobación explícita y formal por parte de MSP.
  - El proveedor deberá informar semestralmente a MSP sobre la evolución de los productos objeto de este contrato, especialmente de aquellas evoluciones que pretendan dar cumplimiento a una nueva legislación o normatividad. Para cambios originados por una nueva legislación, el proveedor deberá realizar las actualizaciones requeridas, en los plazos estipulados por la nueva legislación, sin costo adicional alguno para MSP.
  - No habrán pagos adicionales por parte del MSP, a los estimados por el proveedor en esta parte de la propuesta económica.

3.3.5 MANTENIMIENTO EVOLUTIVO

El servicio de mantenimiento evolutivo deberá incluir el servicio de desarrollo y/o parametrización de nuevas funcionalidades o ampliación de las existentes, de forma que mejoren el funcionamiento y características tecnológicas de la solución.

Los diferentes componentes entrarán en mantenimiento evolutivo tras la estabilización de la puesta en producción y la aceptación técnica y funcional de la solución construida por el proveedor. Para cada solicitud, el proveedor deberá realizar un análisis de impacto de los cambios requeridos y generar una oferta independiente. No se debe iniciar ningún mantenimiento evolutivo sin la aprobación explícita y formal por parte del MSP.

3.4 REQUERIMIENTOS DE GESTIÓN DEL DESARROLLO

El proveedor se compromete a aplicar las mejores prácticas en la construcción de nuevas versiones, parches o nuevos desarrollos, para lo cual debe demostrar que cuenta, dentro de su esquema de prestación del servicio, con una metodología de desarrollo alineada con los entregables requeridos, con los procesos, herramientas y profesionales que garanticen:

- La gestión del proyecto.
- La gestión del cambio.
- La gestión de procesos.

  - La gestión de la calidad.
  - La gestión de la seguridad de la información
  - La gestión de la configuración.
  - La gestión del conocimiento.

- Antes de iniciar el desarrollo, se requiere que el proveedor realice el levantamiento de requerimientos y entregue la documentación requerida para validación del MSP, la cual será ajustada, de acuerdo con las recomendaciones dadas.
- Antes de iniciar el desarrollo se requiere que el proveedor presente el mapa de navegación sugerido, acompañado por prototipos, que serán validados por el MSP en cuanto a usabilidad y experiencia de usuario. El proveedor debe realizar los ajustes solicitados por el MSP.
- Durante el desarrollo, se deben implementar pruebas unitarias, de forma que estas cubran, como mínimo, un 80% del código desarrollado.
- Se requiere que el proveedor implemente procesos de integración y despliegue continuo.
- Al finalizar el desarrollo, el proveedor debe ejecutar pruebas funcionales y no funcionales que garanticen la calidad de los desarrollos realizados.
- Los desarrollos deben tener, por lo menos, un cumplimiento del 90% de las reglas de codificación establecidas por el MSP.
- Se requiere que el proveedor implemente pruebas automáticas para, por lo menos, el 60% de los casos de prueba considerados, dando prioridad a los flujos transaccionales de negocio.
- El MSP, bien sea con sus medios o a través de terceros, realizará un análisis de vulnerabilidades al código. En este caso, se requiere que el proveedor ejecute, antes del paso a producción, un plan de acción para corregir las vulnerabilidades críticas o mayores, que hayan sido identificadas.
- Una entrega se considerará correcta cuando el proveedor copie al repositorio los artefactos que componen dicha entrega, y éstos sean validados por el MSP o quien éste delegue.
- Es obligación del proveedor la custodia del código de la solución y su parametrización específica para el MSP. El incumplimiento de esta obligación será considerado una falta muy grave.
- Se requiere que el proveedor entregue el modelo y diccionario de datos de cada herramienta, desarrollo o componente que integre la plataforma y que esta información pueda ser accedida, mediante consultas a la respectiva base de datos. Las ofertas que no cumplan con este punto serán excluidas. Se requiere que la plataforma, producto de este proceso de consultoría e implementación, pueda ser evolucionada por el personal técnico del MSP o quien el MSP delegue.

3.5 REQUERIMIENTOS DE CAPACITACIÓN/TRANSFERENCIA DE CONOCIMIENTO

El proveedor deberá incluir en su oferta un plan de formación en función de la solución propuesta, que contemple, al menos, los siguientes aspectos:

- **Formación al personal de desarrollo del MSP o quien sea designado**: Esta formación incluye la arquitectura de la solución, en sus diferentes vistas, así como temas relacionados con herramientas de desarrollo, componentes, plugins, API's y otros artefactos requeridos para el buen funcionamiento del sistema. De ser necesario, incluirá las certificaciones oficiales necesarias de fabricante o soporte profesional oficial que permitan la modificación de la solución implantada y el mantenimiento de la garantía de fabricante o soporte profesional oficial.
- **Formación al personal de soporte del MSP o quien sea designado**: Esta formación debe ir orientada al personal que brinda los servicios de operación y soporte técnico, incluye la administración de la aplicación y los sistemas que la componen.
- **Formación al área de Administración y Monitoreo**: Para el conocimiento de la administración y monitoreo de la solución propuesta, el proveedor realizará la formación requerida por el MSP.

Para la solución funcional relacionada con el intercambio de datos en procesos de prescripción, dispensación, validación, gestor de catálogos y el índice maestro de pacientes, el modelo de formación es el siguiente:

- **Formación a formadores:** Para el plan de formación de la plataforma se han identificado dos grupos de trabajo:
  - **Grupo:** profesionales de la salud y de dispensación de medicamentos (técnicos, regentes de farmacia) quienes intervendrán en los procesos de definición de documentación para la construcción de la plataforma a quienes la capacitación estará orientada más a conceptos técnicos de su proceso tales como gestor de catálogos maestros, terminologías, receta electrónica, dispensación de medicamentos, herramientas de análisis de datos, herramientas para gestionar reglas y flujos de trabajo
  - **Grupo Profesionales de salud usuarios finales de las plataformas** quienes serán los formadores de los tres procesos principales de este proyecto (prescripción, validación, dispensación). La capacitación estará enfocada al uso de los distintos módulos y funcionalidades que componen la aplicación.

- **Formación en línea o autoformación:** el proveedor deberá generar el contenido necesario que sirva de guía/apoyo a todos los usuarios potenciales de la solución propuesta para la Plataforma de interoperabilidad de prescripción/dispensación. El contenido se basará en contenidos audiovisuales, con referencias puntuales a la documentación de la propia aplicación.

La actividad de formación se realizará de manera presencial o remota en horario laboral. Podrá participar todo el personal que el MSP considere oportuno en función de sus necesidades.

El proveedor entregará en la oferta una planificación detallada que explique el alcance de los contenidos de formación, en la que se deberá indicar el número de horas previstas de formación para los diferentes tipos.

El proveedor mantendrá actualizada la base de datos de conocimiento de formación durante la ejecución del contrato, con base en los cambios realizados sobre la solución tecnológica propuesta.

3.6 ACUERDO DE NIVELES DE SERVICIO

La calidad del servicio prestado en las fases de soporte y devolución del servicio se medirá con base en unos indicadores clave (KPI, por Key Performance Indicator) sobre los que se establecerán unos niveles objetivos. Estos indicadores se agregarán de forma ponderada en un único indicador que representará la calidad del servicio prestado. Sobre este indicador agregado se definirá un acuerdo de nivel de servicio (ANS).

Es posible que situaciones excepcionales provoquen que el volumen de casos supere el volumen previsto. Para evitar que estos valores anormales afecten el cálculo del ANS, un indicador quedará sin efecto si el total de casos supera el umbral de volumen definido.

En la siguiente tabla se define la configuración del ANS. Posteriormente se detalla el significado de cada uno de los indicadores:

ANS de infraestructura y soporte: el MSP requiere de unos niveles de servicio acordes con la operación que se manejará en la plataforma que compone el servicio, para ello se detalla, en los siguientes cuadros, los ANS esperados para infraestructura y soporte.

ANS de arquitectura: MSP requiere de unos niveles de servicio acordes con la definición de arquitectura para la plataforma, para ello se detalla, en los siguientes cuadros, los ANS esperados para arquitectura

Categoría	Nombre ANS	Descripción	Periodicidad	Cumplimiento Esperado	Penalidad
Infraestructura	**Disponibilidad**	Está determinada la disponibilidad de servicio de sistemas que soportan las aplicaciones y servicios	Mensual	99,999%	Indisponibilidad acumulada (% Mes) | NC sobre la facturación del mes 99.0% a 99,998% | 5% 95,0% a 99,0% | 10% 90,0% a 95,0% | 15% 80,0% a 90,0% | 30% 50% a 80,0% | 50% < 50% | 100%
Infraestructura	**Atención**	Gestión a requerimientos e incidentes	Mensual	98% -Incidentes Críticos (Máxima prioridad) 95% -Incidentes bajo impacto (Mínima Prioridad)	Plazo de respuesta (por horas) DESDE HASTA(Inclusive) CRÉDITO 0 3 5% 3 5 10% 5 10 15% 10 EN ADELANTE 30%
Soporte	Soporte y solución de incidentes	Corresponde a una interrupción no planificada o una reducción de la calidad de un servicio de TI. El fallo de un elemento de configuración que no haya afectado todavía al servicio.	Mensual	98% Incidentes Críticos 96% Incidentes altos, medios y bajos	En caso de presentar indicadores inferiores al mínimo, la penalidad será del 5% por SLA, sobre el valor de facturación ante incidentes críticos antes de IVA. En caso de presentar indicadores inferiores al mínimo, la penalidad será del 3% por SLA, sobre el valor de facturación ante incidentes altos, medios y bajos antes de IVA. En caso de presentar un indicador inferior al 85% El Proveedor asumirá el 50% de la factura antes de IVA
Soporte	Soporte y solución de requerimientos	Corresponde a una solicitud de un cambio o mejora sin que se afecte el servicio.	Mensual	96%	En caso de presentar indicadores inferiores al 95%, la penalidad será del 3% por SLA, sobre el valor de facturación antes de IVA. En caso de presentar un indicador inferior al 85% El Proveedor asumirá el 50 % de la facturación antes de IVA
Calidad	Tiempo de respuesta para la solución definitiva de incidencias posterior a la puesta en producción y durante el tiempo de garantía.	Definir los tiempos de respuesta para el análisis y solución técnica de incidencias identificadas en producción durante el tiempo de garantía.		Excelente: ITR >= (85%) Bueno: ITR >= (75%) Regular: ITR >= (40%) Deficiente: ITR < (40%)	•Si ITR = Regular, se penalizará con el 5% del total de la estimación del proyecto. •Si ITR = Deficiente, se penalizará con el 10% del total de la estimación del proyecto.
Arquitectura	Índice de cumplimiento de los lineamientos definidos por arquitectura	Evaluar las diferencias presentadas entre el diseño documentado y los lineamientos de arquitectura de la organización. Esto se realiza manualmente por parte de un arquitecto. Garantizar el mantenimiento de la coherencia entre las políticas y lineamientos internos y el diseño propuesto por un proveedor. Dentro de cada proyecto se pueden justificar y negociar excepciones con el área de arquitectura. Acordado previamente en fases de arquitectura y diseño. Para dar cumplimiento a este punto se deben realizar los siguientes pasos entre las partes acordadas. 1. El documento de definición de arquitectura debe ir acorde a los lineamientos de arquitectura acordados. 2. El desarrollo no puede ser iniciado sin obtener antes una aprobación del diseño de arquitectura del MSP		LA = 100%	No se hace recepción del entregable sino se cumple con este requisito.

3.7 ENTREGABLES

Fase	Entregables
Análisis e implementación	• Project charter que incluya cronograma detallado que incorpore todas las fases del proyecto • Documento detallado de la arquitectura tecnológica implementada en el Centro de Datos del MSP • Plan de mantenimiento preventivo y correctivo de la solución de acuerdo con ITIL v3 • Plan de gestión del cambio de la solución donde se describa detalladamente los procedimientos formales para instalar nuevos desarrollos y actualizar los existentes • Modelo de privacidad y seguridad • Master Patient Index • Documento de políticas y estándares • Especificación detallada de integraciones • Arquitectura de Integración de Datos • Modelación de datos del negocio • Arquitectura de datos relacionados • Modelación lógica y física • Modelación de estándares • Entrega de los artefactos elaborados por el contratista para realizar la implementación de los servicios en el ESB • Especificación de requerimientos de calidad • Metodología de certificación y auditoría de la calidad • Catálogos maestros y terminologías que incluyen todos los especificados en este alcance • Matriz de entidad de dato/función de negocio • Matriz de sistema/dato • Diagrama de difusión de datos • Diagrama o matriz de seguridad de datos • Diagrama de ciclo de vida del dato • Arquitectura objetivo en cada uno de los subdominios: Sistemas de información, interoperabilidad, datos, seguridad y privacidad e infraestructura • Roadmap • Ecosistema tecnológico • Estándares • Mejores prácticas • Plan de capacitación funcional, técnica y administrativa

Fase de desarrollo	• Documento de casos de uso
	• Documento de diseño técnico de alto nivel
	• Mapa de navegación y wireframes
	• Documento de diseño que contenga:
	  o Diagrama de componentes
	  o Diagrama de despliegue
	  o Diagrama de casos de uso
	  o Diagrama de integración
	  o Diagrama del modelo entidad-relación
	  o Diagramas de secuencia
	  o Diagramas de estado (si es necesario para dar claridad a un requerimiento)
	• Documento de servicios (Service Profile)
	• Pruebas funcionales
	  o Plan de pruebas

	○ Casos de pruebas ○ Evidencia de la ejecución de pruebas ○ Certificación de pruebas • Gestión de privacidad y seguridad de la solución ○ Memoria técnica de los controles de seguridad y privacidad implementados conforme a la ley de protección de datos personales y a las políticas y lineamientos del MSP. ○ Plantilla de aseguramiento de equipos y aplicaciones. ○ Informe de una prueba de seguridad de código estático SAST. ○ Informe de detección de vulnerabilidades de seguridad, donde se evidencie que no se han identificado issues relacionados con: ■ Inyección de código ■ Autenticación Rota ■ Exposición de Datos Sensibles ■ Entidades Externas de XML (XXE) ■ Control de Acceso Roto ■ Security misconfigurations ■ Cross Site Scripting (XSS) ■ Deserialización Insegura ■ Componentes con vulnerabilidades conocidas ■ Registros y monitoreos insuficientes • Manual de despliegue • Manual de usuario • Código fuente. • Ejecutables / URL's • Scripts de bases de datos. • Otros artefactos requeridos para el correcto funcionamiento de la solución.
Fase de entrega del servicio	• Guía de soporte con errores conocidos y dudas funcionales • Guía de operaciones de mantenimiento habituales • Guía de administración de la arquitectura hardware implementada • Guía de copias de seguridad necesarias • Guía de administración de aplicación de la solución implementada • Guía de monitorización de la solución

3.8 ACREDITACIÓN DE EXPERIENCIA

El MSP requiere seleccionar un proveedor con experiencia comprobada en implementaciones a gran escala de sistemas en salud que incluyan: Análisis, Consultoría e Implementación en:

- Implementación de estrategias, servicios y productos que garanticen la unicidad del paciente dentro de contextos de interoperabilidad
- Gestión de reglas y flujos de negocio
- Diseño e implementación de modelos de seguridad de la información y privacidad de datos para sistemas de salud
- Diseño y construcción de repositorios de datos asistenciales, clínicos y empresariales
- Adquisición, integración y unificación de datos
- Diseño y gestión de catálogos maestros de datos
- Interoperabilidad de datos asistenciales, clínicos y empresariales

- Diseño y gestión de interfaces para intercambio de información entre diversas fuentes

La solución propuesta deberá incluir el RoadMap tecnológico, el plan de implementación y su ejecución para la plataforma de salud en Ecuador, inicialmente para la RPIS y el operador logístico, pero con capacidad de integración con plataformas tecnológicas de salud a nivel nacional que contemplen los aspectos regulatorios, seguridad de la información, privacidad de datos, de idioma, monetarios y geográficos.

El proveedor debe presentar al menos dos certificaciones de experiencia en proyectos similares al alcance de la solución ofrecida con la siguiente información:

- Razón social de la empresa o entidad contratante.
- Objeto del contrato o descripción de las obligaciones, relacionadas con el objeto del presente proceso de selección.
- Valor total ejecutado del contrato, expresado en dólares. El valor total sumado de las certificaciones.
- Tiempo de duración en años y meses con fechas de inicio y de terminación, de manera que se pueda establecer el tiempo de ejecución.
- Porcentaje de participación en el Consorcio o Unión Temporal, si la certificación se expide para un contrato ejecutado bajo alguna de estas figuras.
- Fecha, firma, cargo y datos de contacto del funcionario que expide la certificación y a quien se puede contactar para confirmar las referencias.
- Constancia de recibido a satisfacción por el contratante o que de la certificación se infiera el cumplimiento o ejecución del contrato.

Se evaluará experiencia adicional del proponente, para lo cual puede acreditar más proyectos de implementación en la solución ofrecida: ESB (Enterprise Service Bus), MPI, SRR (Service Register and Repository) y servicios de integración, en los últimos 5 años.
Se considerará un puntaje adicional al proveedor que acredite experiencia en la implementación de servicios de integración con estándares FHIR R4.

3.9 REQUISITOS TÉCNICOS MÍNIMOS – TÉRMINOS DE RESPUESTA

El proveedor oferente deberá tener en cuenta los siguientes puntos para dar
respuesta al presente RFP, con el fin de garantizar homogeneidad en el proceso recepción y de evaluación.

- El proveedor deberá adherirse y manifestar expresamente su cumplimiento con los ANS aquí definidos
- El proveedor deberá incluir este archivo diligenciado en su totalidad como respuesta al presente RFP, éste es un requisito indispensable para el proceso de evaluación.
- Costos por componente. Se espera que el proveedor dentro de su oferta incluya costos individuales por componente para tenerlos en cuenta en el proceso evolutivo de la plataforma. Discriminar en la propuesta económica todos los impuestos aplicables para componentes de la solución.
- Anexar acreditaciones de experiencia, de acuerdo a lo estipulado en el punto 6.9
- Confirmar la estructura del equipo humano mínimo y dedicación requerido
- Entregar una propuesta técnica que tenga como mínimo el siguiente contenido:
  - Descripción de la solución propuesta. El proponente debe describir su solución tecnológica y como esta se encuentra alineada con la arquitectura de referencia definida por el MSP
  - Descripción de la arquitectura física de la solución. El proponente debe incluir en su propuesta técnica, un diagrama de ubicación o de despliegue en el cual se describan la distribución física de la solución propuesta en el Centro de Datos del MSP. Deben quedar identificados los puntos de integración con la infraestructura actual.

- Descripción del proceso y metodologías de desarrollo. El proponente debe describir la metodología que usará para desarrollar los servicios de integración sobre la plataforma ofertada.
- Plan de capacitación. El proponente debe elaborar el plan de capacitación definido para cumplir con el servicio de "Capacitación de la Solución" mencionado en el capítulo 6.5 de este documento.
- Plan de Operación de servicios de TI. El proponente debe entregar su plan de operación de servicios alienado al Modelo de operación e interacción de servicios de TI presentados en este documento.
- Modelo de licenciamiento. El proveedor debe presentar un modelo de licenciamiento que se ajuste a las condiciones de dimensionamiento en los apartados anteriores y a las determinadas por el Operador Logístico, escalable en referencia a los requerimientos de interoperabilidad de la RPIS.
- El proponente debe especificar si cumple o no con cada uno de los entregables solicitados en el punto 6.8 de este documento y una descripción de como cumple o en que parte de la propuesta técnica se especifica.

3.10 GLOSARIO, SIGLAS Y CONCEPTOS

Para un mejor entendimiento del documento, describimos a continuación algunos conceptos clave que usaremos durante el desarrollo de este:

- **RPIS:** Red Pública Integral de Salud**.** Las entidades prestadoras de servicios de salud en Ecuador que pertenecen a la RPIS conformada por el Ministerio de Salud son:
  - IESS (Instituto Ecuatoriano de Seguridad Social)
  - ISSFA (Instituto de Seguridad Social de las Fuerzas Armadas)
  - ISSPOL (Instituto de Seguridad Social de la Policía Nacional)
  - RED PÚBLICA COMPLEMENTARIA

- **INEC**: Instituto Nacional de Estadísticas y Censos del Ecuador.

- **ACCESS:** Agencia de Aseguramiento de la Calidad de los Servicios de Salud y Medicina Prepagada de Ecuador.

- **SERCOP:** El Servicio Nacional de Contratación Pública, Sercop, es la entidad rectora del Sistema Nacional de Contratación Pública (SNCP), responsable de desarrollar y administrar el Sistema Oficial de Contratación Pública del Ecuador y de establecer las políticas y condiciones en la materia, a nivel nacional.

- **ARCSA**: La Agencia Nacional de Regulación, Control y Vigilancia Sanitaria (Arcsa), es la entidad pública adscrita al Ministerio de Salud Pública (MSP) que se encarga de controlar y vigilar las condiciones higiénico – sanitarias de los productos de uso y consumo humano, además de brindar servicios que facilitan la obtención de permisos de funcionamiento y Notificaciones Sanitarias.

- **MINTEL:** Ministerio de Telecomunicaciones y Sociedad de la Información (MINTEL) es una organización del Estado de Ecuador, para definir y coordinar la política de Telecomunicaciones que promueva la masificación de las Tecnologías de la Información y Comunicación en el territorio ecuatoriano.

- **Profesional de la salud**: una persona especialmente capacitada que brinda servicios de atención médica como un médico de cabecera, especialista, enfermera, obstetra, dentista y farmacéutico.

- **Actor del sistema**: sistema de información que apoya una función particular en el ámbito de la farmacia.

- **Actor humano**: individuo (médico, farmacéutico, enfermera) que suele utilizar un actor del sistema para realizar una actividad en el ámbito de la farmacia electrónica.

- **Receta Digital:** Es el documento digital válido en el contexto de atención en salud creado y firmado a través de los sistemas de prescripción electrónica por un profesional de la salud autorizado, quien, prescribe a un paciente, medicamentos y/o bienes estratégicos para ser administrados, aplicados o consumidos, cuando el paciente lo requiera.

- **Receta Electrónica:** Se usa este término para los documentos electrónicos de receta que no cuentan necesariamente con firma digital del profesional, y solo están firmados con firma electrónica.

- **Sistema de prescripción**: Es el sistema de información con funcionalidades que le permiten al profesional de la salud permite crear una receta digital. El sistema proveen funcionalidades que permiten a los profesionales médicos la identificación del paciente, los medicamentos y cada uno de los componentes de la receta.

- **Medicamento:** Un medicamento es uno o más fármacos, integrados en una forma farmacéutica, presentado para expendio y uso industrial o clínico, y destinado para su utilización en las personas o en los animales, dotado de propiedades que permitan el mejor efecto farmacológico de sus componentes con el fin de prevenir, aliviar o mejorar el estado de salud de las personas enfermas, o para modificar estados fisiológicos.

- **Bien estratégico en salud:** los constituyen todo tipo de bien determinado por la Autoridad Sanitaria Nacional en el marco de sus competencias, que sea necesario y se encuentre relacionado directamente con la prestación de servicios de salud

- **Denominación Común Internacional** (**DCI**): Es el nombre oficial único a nivel mundial, no comercial, genérico utilizado para identificación de un principio activo contenido en un medicamento.

- **Medicamento Genérico:** Medicamento que se distribuye o expende rotulado con el nombre del medicamento con su principio activo expresado en Denominación Común Internacional (DCI), es decir, sin ser identificado con una marca de fábrica o marca comercial.

- **Principio activo:** Principio o sustancias activas es toda sustancia o mezcla de sustancias destinadas a la fabricación de un medicamento y que, al ser utilizadas en su producción, se convierten en un componente activo de dicho medicamento destinado a ejercer una acción farmacológica, inmunológica o metabólica con el fin de restaurar, corregir o modificar las funciones fisiológicas, o de establecer un diagnóstico.

- **Preparación Magistral.** Es el preparado o producto farmacéutico elaborado por un Químico Farmacéutico para atender una prescripción médica, de un paciente individual, que requiere de algún tipo de intervención técnica de variada complejidad. La preparación magistral debe ser de dispensación inmediata.

- **Medicamento de Control Especial:** Medicamentos que crean dependencia; su uso inadecuado conlleva al manejo ilícito de los mismos, por lo que es necesario fortalecer los sistemas de vigilancia, seguimiento y control.

- **Forma Farmacéutica:** Forma física que caracteriza al producto farmacéutico terminado (Ej. comprimidos, cápsulas, jarabes, supositorios, etc.)

- **Vía de Administración:** Ruta de entrada por la cual los medicamentos son introducidos al organismo para producir sus efectos. Ejemplo: Vía oral, vía enteral, etc.

- **Indicación:** Los usos a los cuales se destina un producto (medicamento, dispositivo médico, suplemento alimentario, etc.) después que se ha probado científicamente que su empleo para una finalidad determinada es efectivo y seguro.

- **Problemas Relacionados con Medicamentos (PRM):** Corresponden a problemas relacionados con los medicamentos que pueden ser clasificados en problemas de efectividad, seguridad y necesidad.

- **Problemas Relacionados con la Utilización de Medicamentos (PRUM):** Corresponden a causas prevenibles de problemas relacionados con medicamentos, asociados a errores de medicación (prescripción, dispensación, administración o uso por parte del paciente o cuidador), incluyendo los fallos en el Sistema de Suministro de Medicamentos, relacionados principalmente a la ausencia en los servicios de procesos administrativos y técnicos que garanticen la existencia de medicamentos que realmente se necesiten, acompañados de las características de efectividad, seguridad, calidad de la información y educación necesaria para su utilización correcta.

- **Error de Medicación:** Cualquier incidente prevenible que pueda causar daño al paciente o dé lugar a una utilización inapropiada de los medicamentos (profesional de la salud, paciente o consumidor).
  Pueden ser debidos a la práctica profesional, productos sanitarios, procedimientos y sistemas, incluyendo la prescripción, la comunicación de la orden, etiquetado, envase y denominación del producto, composición, dispensación, distribución, administración, monitorización y utilización.

- **Validación farmacéutica**: la acción realizada por un farmacéutico para aprobar / modificar o rechazar una receta antes de que sea entregada al paciente.

- **Asesoramiento/validación farmacéutica**: el resultado del análisis farmacéutico;

- **Interoperabilidad:** Habilidad de dos o más sistemas para intercambiar información y utilizar entre estos mismos la información.

- **Mensaje:** Modo en que se intercambia la información entre sistemas informáticos. Su sintaxis está dada por el estándar de mensajería HL7, en el cual se detalla el lenguaje, la estructura, la codificación.

- **Segmento**: Corresponde a cada una de las líneas de un mensaje, cada segmento posee su propio sentido semántico por lo que contienen información específica.

- **OID:** Acrónimo del término en el idioma inglés “Object Identifier”. Un identificador único global creado mediante el uso de reglas establecidas en el estándar ISO 9834. Término en plural: OIDs.

- **Seguridad:** son los procesos y herramientas destinados a garantizar la privacidad, confidencialidad, integridad y accesibilidad de los datos guardados en un sistema de información.

- **Privacidad:** Es la facultad de una persona –física o jurídica- de prevenir la difusión de datos personales que, sin ser difamatorios ni perjudiciales, ésta desea que no sean expuestos. Esto contempla a un convenio de confidencialidad explícito o tácito con los actores del sistema de salud con acceso a esa información.

- **Confidencialidad:** Son los datos que no puede ser divulgada o comunicada a terceros, salvo a persona autorizada por el titular de estos.

- **Integridad:** Capacidad técnica que garantiza que la información guardada coincide plenamente con la ingresada por el actor de salud y no puede ser alterada por un usuario no autorizado.

- **Identificación:** Proceso que permite que los actores del sistema (pacientes, prestadores, farmacéuticos) sean reconocidos por un sistema de información en salud.

- **Firma electrónica:** Son los datos electrónicos que están integrados, ligados o asociados de manera lógica a otros datos electrónicos o información. Es un concepto legal que equivale a la firma manuscrita y que tiene el objetico de dar fe de la voluntad del firmante o acreditar su validez.

- **Firma digital:** La firma digital consiste en aplicar mecanismos criptográficos al contenido de un mensaje o documento con el objetivo de demostrar al receptor del mensaje que el emisor del mensaje es real (autenticación), que éste no puede negar que envió el mensaje (no repudio) y que el mensaje no ha sido alterado desde su emisión (integridad). La firma digital entonces, debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.