TÉRMINOS DE REFERENCIA

SERVICIO DE SUSCRIPCIÓN ANUAL DE COMPUTACIÓN EN LA NUBE – CLOUD COMPUTING

1. AREA USUARIA

Oficina de Tecnologías de la Información e Innovación del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud.

2. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de suscripción anual de computación en la Nube - Cloud Computing para el Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud.

3. ANTECEDENTES

Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud, atendiendo a los lineamientos y objetivos estratégicos de impulsar y desarrollar proyectos de Tecnologías de Información, cuyo resultado permita el mejoramiento de la infraestructura informática de la entidad, con el objetivo de permitir a los usuarios procesar información eficientemente de tal manera que dichas actividades coadyuven al logro de las metas y objetivos institucionales.

El servicio requerido permitirá la continuidad operativa y permitirá salvaguardar la información que se almacena en los servidores críticos, con la finalidad de evitar incidentes de perdida de información, las mismas que permitan cumplir con el objetivo de la entidad, para lo cual es necesario contratar el Servicio de suscripción anual de computación en la nube – Cloud Computing para el Centro de Procesamiento de Datos para que el Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud ofrezca altos niveles de disponibilidad y seguridad.

4. FINALIDAD PÚBLICA

La ejecución de este servicio tiene como finalidad implementar una infraestructura de contingencia flexible, segura, escalable y sostenible en el tiempo, el cual permitirá brindar un mejor servicio de los sistemas informáticos del CENARES, asegurando la disponibilidad de los servicios, en cumplimiento de los fines institucionales del CENARES.

5. ACTIVIDAD DEL POI

AOI000134500704 Gestión de Tecnologías de la Información.

6. OBJETIVO DE LA CONVOCATORIA

Objetivo General

Se requiere la contratación de un servicio de suscripción anual de computación en la nube – Cloud Computing de contingencia, el cual provisionará una plataforma de sistemas, flexible, segura, escalable, elástica y sostenible en el tiempo. El cual incluye la implementación de nuestros sistemas informáticos en la nube, capacitación en el uso adecuado y soporte por el periodo del servicio.

Objetivos Específicos

- Contratar a una empresa para que nos brinde el servicio Cloud Computing (nube) de infraestructura de contingencia, el cual permitirá tener nuestros sistemas en la nube.
- Brindar a nivel de todas las sedes una conexión más eficiente, segura y de rápido acceso a los sistemas del CENARES, los cuales formará parte de site de contingencia del centro de datos del os servidores de la Sede Central.

7. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

El servicio de solución corporativa Cloud Computing (Nube) estará compuesto por los siguientes servicios:

Prestación	Cantidad	Unidad de Medida	Descripción
Principal	1	Servicio	Servicio de implementación y migración
	1	Servicio	Servicio de suscripción anual de computación en la nube – Cloud Computing
Accesoria	1	Servicio	Soporte Técnico
	1	Servicio	Capacitación

7.1 CONSIDERACIONES GENERALES:

7.3.1 El CONTRATISTA se encargará de la implementación y migración de todos los servidores listados en la tabla 01, puesta en marcha, y todas las actividades necesarias para la implementación y migración del servicio solicitado, en coordinación con la Oficina de Tecnologías de la Información e Innovación.

7.3.2 El CONTRATISTA levantará información técnica dentro del alcance del presente TDR, para elaborar el Plan de Trabajo oportunamente, conjuntamente con el especialista de la Oficina de Tecnologías de la Información e Innovación.

7.3.3 El CONTRATISTA deberá considerar el personal, equipos, licencias de Windows y SQL Server en la nube, herramientas y cualquier otro recurso necesario dentro del alcance del presente TDR, para llevar a cabo la correcta implementación y migración del Servicio sin que genere un costo adicional para CENARES.

7.3.4 El CONTRATISTA dentro del plazo de implementación y migración, deberá ejecutar un protocolo de pruebas, el cual no deberá contar con observaciones para dar la conformidad de la implementación, migración y firmar el Acta de implementación del servicio.

7.3.5 El CONTRATISTA es el responsable de la implementación en su totalidad, incluyendo la ejecución de los protocolos de pruebas.

7.3.6 CENARES autorizará el ingreso a las instalaciones al personal del CONTRATISTA, de requerirlo, previa solicitud detallada, donde deberán presentar por correo electrónico lo siguiente:

- Datos del personal
- N° de DNI
- Lista de materiales y/o equipos a ingresar de ser el caso
- Fechas y horarios de ingreso
- Actividades a realizar
- Áreas y/o servicios afectados, en caso de corte de servicio.

7.3.7 EL CONTRATISTA deberá contar con un sistema de gestión de ticket para el registro de las incidencias y requerimientos de todos los servicios.

7.3.8 El CONTRATISTA en caso solicite el cambio del personal clave, este deberá ser ingresado por mesa de partes virtual, y no podrá cambiar el Personal clave hasta que la Entidad apruebe de manera formal mediante correo electrónico o Carta, la aceptación de dicho cambio; así mismo el CONTRATISTA deberá concretar una reunión para la transferencia de funciones, la cual debe ser como máximo a los 5 (cinco) días calendarios de remitida dicha aprobación al CONTRATISTA, donde CENARES deberá participar.

7.3.9 En el caso que el personal clave se ausente por un caso fortuito de fuerza mayor, el CONTRATISTA en un plazo no mayor a 2 días calendarios contabilizado desde el día siguiente de lo ocurrido, deberá remitir la documentación fehaciente a CENARES por mesa de partes virtual, sustentando los hechos suscitados; una vez revisada y validada la documentación, se otorgará al Contratista siete (07) días calendarios para el cambio del personal clave, los cuales se contabilizaran desde la validación de la salida del personal clave, la cual se remitirá a través de Carta al Contratista.

7.3.10 Se precisa que, en la actualidad, el CENARES tiene implementados sus servicios On-Premise (Infraestructura local).

7.3.11 La nube deberá cumplir con los Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano de la PCM (Presidencia de Consejos de Ministros) establecidas a través de Secretaria de Gobierno Digital (SEGDI), el cual indica que se deberá presentar un certificado seguridad de la información ampliamente reconocido y basado en estándares internacionales, el mismo que tiene que ser emitido por una organización de auditoría independiente, como: Federal Risk and Authorization Management Program (FedRAMP) o similar. Los certificados de seguridad con el que tiene que acreditar la nube son los ISOs: ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, los cuales deberán presentarse para el **perfeccionamiento del Contrato**.

7.3.12 EL CONTRATISTA deberá ser certificado o autorizado o partner o representante, en solución de la nube que oferte en el presente servicio. Se aceptará también "cartas estándar" de la nube en donde indique que EL CONTRATISTA es certificado o autorizado o partner o representante de la nube ofertada. Dicho documento deberá presentarse a la **presentación de la oferta.**

7.3.13 EL CONTRATISTA deberá contar y/o activar con el soporte directo de la nube propuesta para el servicio Cloud Computing. Deberá acreditar con un Contrato que indique lo solicitado y/o suscripción al servicio de soporte advantage o prioritario o business y/o pago/suscripción de soporte y/o con una Carta emitida por la nube indicando lo solicitado, o documento similar que precise lo solicitado; dicho documento deberá **presentarse al perfeccionamiento del Contrato.**

7.3.14 EL CONTRATISTA deberá integrar la nube propuesta.

7.3.15 EL CONTRATISTA deberá considerar lo necesario para que la implementación del servicio se realice fuera del horario de oficina administrativa, con el fin de no afectar los servicios actuales del CENARES, exceptuando aquellas actividades que no afecten los servicios actuales en coordinación con la Oficina de Tecnologías de la Información e Innovación. En lo posible se optará por una implementación de manera remota. Se detallan los horarios sugeridos de implementación:

- Fuera de horario – oficina administrativa: lunes a viernes de 6:00 p.m. a 7:00 a.m., y sábados y domingos las 24 horas.

7.3.16 El CONTRATISTA y la nube deberá garantizar la confidencialidad y secreto de la información facilitada por el CENARES, a cualquier persona que por su relación con EL CONTRATISTA deba tener acceso a dicha información. Esto se debe suscribir en un documento de ACUERDO DE CONFIDENCIALIDAD, entre CENARES y el CONTRATISTA, como anexo al contrato parte del Plan de Trabajo.

7.3.17 EL CONTRATISTA deberá asegurar que la nube, servicios y propuestas solución propuesta soporten el protocolo IPv4 e IPv6.

7.3.18 La solución debe ser una solución de recuperación ante desastres en la nube brindado por un proveedor de servicio en nube (hyperscaler), que protege máquinas virtuales VMware vSphere mediante la replicación y recuperación en un entorno definido por software.

7.3.19 La solución gestionada debe permitir la habilitación de protección y configuración de métodos de recuperación sin preocupaciones por la gestión de infraestructura.

7.3.20 La solución debe ofrecer una arquitectura gestionada que permita la habilitación de la protección y configuración de métodos de recuperación, sin requerir la gestión directa de la infraestructura.

7.3.21 La solución debe tener la capacidad de lograr una recuperación rápida sin intervención y la opción de dar prioridad a cargas de trabajo para lograr un rendimiento similar al de producción.

7.3.22 la solución debe ofrecer una experiencia de administración sencilla y familiar, garantizando la integridad de los datos respaldados, y un modelo de precios simplificado asociado a la cantidad de máquinas virtuales y datos totales.

7.3.23 Los componentes de la solución deben incluir los conectores necesarios e instalados en el entorno de VMware vSphere, en conjunto con el orquestador de servicios en la nube, ofreciendo una interfaz de usuario y capacidades de orquestación.

7.3.24 El servicio debe proporcionar un sistema de archivos en nube para almacenar respaldos eficientemente y un entorno en la nube para pruebas y fallos.

7.3.25 Debe permitir a los usuarios gestionar tanto el sitio de recuperación en la nube como los sitios de producción mediante el uso de VMware vCenter, manteniendo acceso a los elementos familiares de vSphere, como clusters, recursos, datastores y switches virtuales, tras un fallo.

7.3.26 Se requiere un sistema de comprobación de integridad de datos a diario para asegurar que los respaldos estén listos y utilizables cuando sean necesarios.

7.3.27 El producto debe aprovechar la elasticidad de la computación en la nube, activando la infraestructura de VMware sobre la nube del hyperscaler únicamente durante eventos de prueba o falla de recuperación, lo que reduce los costos de recuperación de desastres.

7.3.28 Deberá incluir hasta un máximo de 6 días de pruebas de disaster recovery por año y/o hasta 2 pruebas por año.

7.3.29 Deberá incluir hasta un máximo de 5 días en caso de failover sin que la entidad incurra en gastos adicionales por uso de los recursos de la nube. Deberá cubrir un tráfico de salida de 2 TB.

7.3.30 Deberá incluir el análisis en tiempo real para proteger las VM en nube de ataques de Ransomware nativas de VMware u otros productos para protegerer ataques de Ransomware.

7.3.31 La solución propuesta por el postor debe ser del tipo IaaS y provista mediante la modalidad de "Nube Pública".

7.3.32 La solución deberá estar alojada en un centro de datos de clase mundial, con certificaciones internacionales como las del Uptime Institute.

7.3.33 La solución deberá proveer el consumo de equipamiento de forma dedicada para la ejecución de las cargas productivas de la Entidad. No se deberá proveer recursos compartidos como pueden ser: Reserva de recursos sobre hardware compartido, Tenants, u otros similares que no sean dedicados exclusivamente a las cargas de la Entidad.

7.3.34 El fabricante de la solución de virtualización ofrecida deberá brindarle soporte continuo a la plataforma de operación de la plataforma o Datacenter Definido por Software, siendo responsable por la actualización de parches, security fixes y versiones, mantenimientos y respaldos de todos los módulos de administración que son parte de la plataforma. Asimismo, deberá permitir la apertura de casos de soporte a fin de atender los requerimientos de la Entidad, asegurando el continuo soporte para toda la solución de producción a operar en el entorno de Nube. Asimismo, todo licenciamiento asociado a la plataforma de Centro de Datos definido por software, deberá

estar incluido sin costo para la Entidad y cubriendo todos los elementos que precisen ser licenciados.

7.3.35 El proveedor deberá asegurar un Uptime no menor a 99.9% para la provisión de las plataformas ofrecidas.

7.3.36 El equipamiento ofrecido deberá ofrecer equipamiento 100% certificado para ejecutar la solución de centro de datos definido por software ofrecido por el proveedor de nube.

7.3.37 El equipamiento ofrecido deberá estar basado en discos SSD del tipo NVME para el almacenamiento persistente de los datos, no aceptándose otro tipo de almacenamiento.

7.3.38 La solución ofertada deberá ofrecer elasticidad para el crecimiento y reducción de las cargas solicitadas, y este requerimiento deberá poder efectuarse desde un portal web donde se encuentren registrados los recursos de la Entidad.

7.3.39 Desde dicho portal, la Entidad podrá efectuar, como mínimo, las siguientes operaciones, de forma centralizada.

- Escalar en recursos de cómputo mediante la adición de mayor cantidad de nodos según la demanda.
- Decrecer la capacidad de recursos.
- Contar con umbrales de carga específicos, que le permitan a la plataforma escalar en recursos, adicionando el equipamiento necesario cuando sea preciso.
- Contar con la capacidad de administrar servicios de virtualización de servidores, almacenamiento virtual, servicios de redes virtuales con microsegmentación y servicios de Firewall Virtual. El proveedor del servicio debe asegurar la continuidad operativo de todos los servicios administrativos de la solución, así como la protección periódica de dicho ambiente.

7.3.40 La solución deberá ofrecer compatibilidad para su interacción con plataformas On Premise, y debe permitir lo siguiente:

- Establecimiento de túneles privados del tipo VPN Site to Site o equivalente (Utilizando servicios estándar como IPSec o IKE para el establecimiento), entre la plataforma On premise y los servicios en nube, para movilidad de máquinas virtuales, migraciones de datos, consumo de servicios de forma bidireccional entre las facilidades de la Entidad y los servicios alojados en nube.
- Capacidad de gestionar de forma centralizada los recursos desplegados dentro de la plataforma de la Entidad, y los recursos en nube. Las herramientas provistas para estos efectos deberán pertenecer al proveedor de servicios en nube y no se aceptará la provisión de software de terceros.

7.3.41 La solución deberá permitir que se ejecute el mismo tipo de formato de la máquina virtual que se utiliza en el centro de datos On premise, de modo tal que no precisen migraciones a nivel de formato de VM, reajustes, rediseños o migraciones complejas a nivel de servicios de máquina virtual.

MINISTERIO DE SALUD - Chile
Oficina de Tecnologías de la Información y Comunicación en Salud
D. TORRES
V°B°
Subsecretaría de Recursos Financieros

7.2 TIPOS DE CAPACIDADES

Característica	Especificación
Administración	Basada en HTML5, deberá permitir la gestión centralizada de toda la solución ofrecida. La plataforma deberá tener los recursos destinados a la administración de la solución en su propia reserva de recursos, siendo el proveedor del servicio el responsable de la protección de estos. Los recursos de administración deben ser exclusivos para la gestión de la solución en nube de la Entidad.
Servicios	Debe permitir como mínimo el acceso a las siguientes acciones: • Encender una o más máquinas virtuales. • Apagar una o más máquinas virtuales. • Crear máquinas virtuales • Crear plantillas • Agregar y remover un servidor físico desde la consola de gestión • Crear grupos de permisos y asociar a usuarios. • Crear y apagar alarmas de monitoreo.
CREACIÓN DE MÁQUINAS VIRTUALES	• La herramienta de virtualización debe soportar la creación rápida de nuevas máquinas virtuales usando plantillas de máquinas virtuales. • La solución de virtualización debe tener la capacidad de creación y ejecución simultánea de múltiples máquinas virtuales sobre un mismo servidor físico. • La solución debe proveer un repositorio de imágenes centralizado que puede sincronizarse con el repositorio On premise, para su uso para la creación de nuevas VMs.
SISTEMA OPERATIVO	Debe soportar en sus máquinas virtuales para los siguientes sistemas operativos: Windows 10, Windows 2012 server, Windows 2016 server, Windows Server 2019, Windows Server 2022 y diferentes versiones de Linux.
DISPONIBILIDAD	Soporte para activar un modo de mantenimiento de tal modo que cada vez que se requiera realizar mantenimiento a los recursos de la solución, las máquinas virtuales se muevan automáticamente a nuevos recursos alternativos y en línea. Esto debe entregarse como parte del servicio y no debe generar disrupción en la operación de la solución. La herramienta de virtualización debe permitir configurar Alta Disponibilidad para que las máquinas virtuales afectadas puedan reiniciarse automáticamente en otros recursos disponibles de la solución. La plataforma deberá asegurar el regreso de las máquinas virtuales en caso de que esta falle, sin que esto incurra en costos adicionales para la

MINISTERIO DE SALUD - Oficina de Tecnologías de la Información - D. TORRES - Visto - Oficina de Abastecimiento de Recursos Estratégicos en Salud

	Entidad. La solución debe incluir el balanceo automático de carga que distribuya las máquinas virtuales entre los nodos de la solución según políticas configurables, esto debe ser configurado como parte del requerimiento. Debe soportar la configuración de switches virtuales distribuidos.
ALMACENAMIENTO BASADO EN SOFTWARE	La solución debe entregar el almacenamiento definido por software, que permita utilizar productivamente el espacio requerido por la Entidad. La solución debe considerar: - Integración al 100% con la solución de virtualización ofrecida como parte del servicio, esta integración debe ocurrir al nivel del Kernel del mismo, y se debe gestionar desde la misma consola de administración. - Deduplicación y compresión de datos activas y operativa para el repositorio ofrecido en el proveedor de nube. - Soporte de FTT=1, FTT=2 o equivalentes de la industria a ellos. - La solución deberá entregar el almacenamiento con el uso de discos NVME de forma exclusiva.
REDES VIRTUALES Y SEGURIDAD	La solución debe incluir la funcionalidad de redes virtuales integradas dentro de la oferta, y deberá considerar: - Integración al 100% con la solución ofertada, y se debe gestionar desde la misma consola de administración. - Debe ofrecer servicios de switching y routing distribuidos para los servicios contratados. - Soporte de IPV4 e IPV6 - Deberá utilizar VxLAN ó GENEVE como protocolos de overlay. - Firewall distribuido para VMs que se ejecuten sobre la plataforma de virtualización. La solución deberá permitir configurar políticas de acceso para los servicios de gestión de la solución, así como también para los servicios de producción. - Protección del tráfico en esquemas Norte-Sur y Este-Oeste.

MINISTERIO DE SALUD · Oficina de Tecnologías de la Información y Comunicaciones · Oficina Ejecutiva de Abastecimiento de Recursos Estratégicos en Salud
D. TORRES
V°B°

	- Microsegmentación de redes. - Servicios de NAT (SNAT, DNAT) y VPN Site to Site incorporados en la oferta. El postor deberá poder efectuar una VPN contra los dispositivos del CENARES utilizando protocolos estándar de la industria, como IKE. - Soporte de integración con Active Directory
OFERTA	El postor debe entregar los siguientes recursos de cómputo para que la Entidad pueda ejecutar sus cargas: - 72 cores de CPU físicos - 1 TB de RAM - 41 TB RAW en discos SSD del tipo NVME, con soporte de deduplicación y compresión de datos activo y operativo El postor deberá proveer esta plataforma por un espacio de 36 meses, en modelo de suscripción. El servicio debe considerar el servicio de internet para que los servicios a desplegar sobre la misma cuenten con este servicio. Asimismo, se debe considerar el establecimiento de los servicios de conectividad con el centro de datos de CENARES. La Entidad brindará facilidades desde el lado de su equipamiento perimetral para permitir dicha conectividad. El postor debe asegurar, como mínimo: - Una capacidad de acceso a internet que considere ingreso de datos sin restricciones, y un tráfico de salida de al menos 2 TB por mes.

MINISTERIO DE SALUD - CENARES
Oficina de Tecnologías de la Información y Telecomunicaciones
Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud
D. TORRES
V°B°

7.3 PRESTACIÓN PRINCIPAL:

7.3.1 SERVICIO DE IMPLEMENTACIÓN Y MIGRACIÓN

EL CONTRATISTA deberá contemplar lo siguiente, para realizar la implementación y la migración de todos los servidores listados en la tabla 01 desde la actual infraestructura del CENARES ubicadas localmente:

a. La plataforma "Cloud Computing", así como cada uno de sus componentes, software, eventos, sistemas operativos y configuraciones, debe estar sincronizada con un servicio de NTP ("Network Time Protocol") donde la precisión del reloj y representación de información/eventos/gráficos deberá figurar en GMT -5 (zona horaria correspondiente a Perú). Se precisa que, el servicio NTP podrá ser un servicio nativo de nube o un recurso de cómputo dedicado.

b. EL CONTRATISTA deberá instalar e implementar y migrar los servidores, servicios, base de datos, conexiones, arquitectura de red y sistemas del CENARES hacia la plataforma Cloud

ofertada, para lo cual EL CONTRATISTA deberá proponer una arquitectura de acuerdo a lo solicitado a los Términos de Referencia del presente proceso.

c. EL CONTRATISTA deberá realizar la configuración de todas las redes virtuales necesarias para habilitar el servicio en la plataforma Cloud Computing, previa validación de la Oficina de Tecnologías de la Información e Innovación de CENARES.
d. EL CONTRATISTA entregará un inventario de accesos a todas las consolas de administración de servidores, bases de datos y servicios a la finalización de la implementación. La información deberá ser remitida a la Oficina de Tecnologías de la Información e Innovación de CENARES.
e. EL CONTRATISTA es responsable de la cuenta de administración asignada para la gestión y soporte de la solución.
f. Se precisa que CENARES brindará al Contratista, en la etapa de la implementación y migración, el acceso de nivel administrador a todos los servidores y bases de datos, acceso de solo lectura a las consolas de gestión de entorno local e inventario de servidores y aplicaciones. El Contratista deberá realizar el relevamiento de información para complementar los datos que considere necesarios.

7.3.2 HABILITACIÓN DE AMBIENTES CLOUD

EL CONTRATISTA deberá asegurar y garantizar, que el Servicio de Cloud Computing que oferte, cuente de forma inicial con todas las capacidades especificadas en las Características actuales de los servicios del CENARES descritos en la Tabla N° 01, con una utilización del 100%.

Tabla N° 01 - Características actuales de los servicios del CENARES

Nro	ID	Zona	Entorno	Tipo	Sistema Operativo	Servicio
1	SERVIDOR 1	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_01
2	SERVIDOR 2	Produccion	Aplicaciones Web	IaaS	Windows Server 2016	App_02
3	SERVIDOR 3	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_03
4	SERVIDOR 4	Produccion	Aplicación de escritorio	IaaS	Windows Server 2019	SIGA y SIAF
5	SERVIDOR 5	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
6	SERVIDOR 6	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
7	SERVIDOR 7	Produccion	Directorio Activo	IaaS	Windows Server 2019	DIRECTORIO ACTIVO
8	SERVIDOR 8	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
9	SERVIDOR 9	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
10	SERVIDOR 10	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
11	SERVIDOR 11	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
12	SERVIDOR 12	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
13	SERVIDOR 13	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
14	SERVIDOR 14	Produccion	NTP	IaaS	Linux	NTP
15	SERVIDOR 15	Produccion	Central IP	IaaS	Linux	CENTRAL IP
16	SERVIDOR 16	Produccion	Central IP	IaaS	Linux	CENTRAL IP
17	SERVIDOR 17	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
18	SERVIDOR 18	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
19	SERVIDOR	Produccion	Aplicaciones	IaaS	Windows	App_04

	19		Web		Server 2019	
20	SERVIDOR 20	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
21	SERVIDOR 21	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
22	SERVIDOR 22	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_05
23	SERVIDOR 23	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
24	SERVIDOR 24	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
25	SERVIDOR 25	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_06
26	SERVIDOR 26	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_07
27	SERVIDOR 27	Produccion	Aplicaciones Web	IaaS	Linux	App_08
28	SERVIDOR 28	Produccion	Aplicaciones Web	IaaS	Linux	App_08
29	SERVIDOR 29	Produccion	Aplicaciones Web	IaaS	Linux	App_09
30	SERVIDOR 30	Produccion	Aplicaciones Web	IaaS	Linux	App_10
31	SERVIDOR 31	Produccion	Aplicaciones Web	IaaS	Linux	App_11
32	SERVIDOR 32	Produccion	Aplicaciones Web	IaaS	Linux	App_12
33	SERVIDOR 33	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
34	SERVIDOR 34	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
35	SERVIDOR 35	Produccion	Aplicación de escritorio	IaaS	Windows Server 2016	Bonovo

7.3.3 SERVICIOS DE APLICACIONES WEB

EL CONTRATISTA deberá considerar lo siguiente durante la implementación y migración de los servidores asociados a los servicios de aplicaciones web:

Nro	Servidor	Servicio	SO	Tipo
1	SERVIDOR 1	APP WEB	Windows	Net Core / .Net
2	SERVIDOR 2	APP WEB	Windows	Net Core / .Net
3	SERVIDOR 3	APP WEB	Linux	Payara
4	SERVIDOR 19	APP WEB	Linux	Payara
5	SERVIDOR 22	APP WEB	Windows	Net Core / .Net
6	SERVIDOR 25	APP WEB	Windows	Net Core / .Net
7	SERVIDOR 26	APP WEB	Linux	Payara
8	SERVIDOR 27	APP WEB	Linux	Payara
9	SERVIDOR 28	APP WEB	Linux	Payara
10	SERVIDOR 29	APP WEB	Linux	Payara
11	SERVIDOR 30	APP WEB	Linux	Payara
12	SERVIDOR 31	APP WEB	Linux	Payara
13	SERVIDOR 32	APP WEB	Linux	Payara

- EL CONTRATISTA deberá configurar cada plataforma para que pueda conectarse a los servicios de bases de datos Microsoft SQL, y a los servicios de Active Directory y Servidor de archivos.
- EL CONTRATISTA deberá configurar las plataformas para que escalen en forma horizontal y/o vertical, de manera automatizadas basada en patrones de comportamiento (uso de CPU, uso de RAM) definiendo límites mínimos y máximos de crecimiento, para lo cual podrá solicitar ventanas de mantenimiento para los casos de escalamiento vertical.

7.3.4 SERVICIOS DE BASE DE DATOS

EL CONTRATISTA deberá considerar lo siguiente durante la implementación y migración de los servidores asociados a los servicios de bases de datos:

a. EL CONTRATISTA deberá proveer servicios administrados y/o plataformas administradas para los entornos de bases de datos Microsoft SQL, incluyendo la gestión del sistema operativo, motor de base de datos, acciones de monitoreo, mantenimiento y optimización de plataforma, con el fin de asegurar la disponibilidad y no degradación del servicio. Se aclara que el acceso administrador a las consolas de nube publica y a los sistemas operativos y bases de datos, es responsabilidad del Contratista. El CENARES, podrá solicitar acceso para gestionar los datos almacenados en los esquemas y base de datos. Se precisa que se permite la implementación mediante IaaS (Infrastructure-as-a-Services).
b. EL CONTRATISTA deberá contar con personal especialista, para implementar y gestionar los entornos de base de datos de acuerdo a las buenas prácticas de cada fabricante.
c. EL CONTRATISTA deberá implementar conexiones de "Linked-Server" entre las bases de datos Microsoft SQL, para un mínimo de 10 "linked-server" entre los diferentes entornos de Bases de Datos (Producción).
d. EL CONTRATISTA deberá configurar las plataformas para que escalen en forma automatizada basada en patrones de comportamiento (uso de CPU, uso de RAM) definiendo límites mínimos y máximos de crecimiento, para lo cual se podrán programar paradas de mantenimiento en coordinación con CENARES.

7.3.5 SERVICIOS DE DIRECTORIO ACTIVO

EL CONTRATISTA deberá considerar lo siguiente durante la implementación y migración de los servidores asociados a los servicios de directorio activo (autenticación):

a. EL CONTRATISTA deberá implementar los servidores necesarios e integrarlos a los dominios correspondientes.
b. EL CONTRATISTA deberá garantizar una correcta integración / replicación de datos en los servidores implementados para los servicios de directorio activo.
c. EL CONTRATISTA deberá garantizar la no afectación de acceso a los usuarios durante la implementación del servicio.

7.3.6 ALMACENAMIENTO

El CENARES requiere una provisión de almacenamiento a demanda desde el inicio del servicio, provisto de acuerdo al uso del mismo y basado en almacenamiento de tipo "SSD".

a. EL CONTRATISTA deberá implementar de forma inicial el almacenamiento actual utilizado por CENARES:

Nro	Servidor	Zona
1	SERVIDOR 6	Produccion
2	SERVIDOR 8	Produccion
3	SERVIDOR 11	Produccion
4	SERVIDOR 12	Produccion
5	SERVIDOR 17	Produccion

6	SERVIDOR 21	Produccion
7	SERVIDOR 23	Produccion

b. EL CONTRATISTA deberá verificar y configurar las particiones/discos de todos los servidores descritos en la Tabla Nro 1, de tal forma que se permita su crecimiento de forma autónoma sin interrupción de servicios.

7.3.7 SERVICIO DE DNS PÚBLICO

Se precisa que el CENARES cuenta con un (01) dominio público en internet, mediante el cual gestiona los registros DNS de los sistemas públicos de la entidad, que reciben en promedio 2 millones de queries/mes.

EL CONTRATISTA deberá implementar y gestionar un servicio de DNS público para albergar los dominios DNS del CENARES:

Nro	Ámbito	Dominio
1	Administrativo	cenares.gob.pe

7.3.8 SERVICIOS DE RED

a. EL CONTRATISTA deberá definir e implementar las reglas de ruteo y comunicación entre las redes de la plataforma de nube, previa validación de la OTII del CENARES.
b. EL CONTRATISTA deberá contar con una infraestructura (Región o Zona de disponibilidad) capaz de brindar y garantizar una latencia máxima de 100 ms o menor e interconexión adecuada para que el uso de los servicios, aplicaciones, sistemas y bases de datos del CENARES se desarrollen de manera correcta y eficiente.
c. EL CONTRATISTA deberá incluir servicios de conexión VPN segura y de puertas de enlace NAT para las redes Cloud, que permita establecer sesiones seguras y privadas con túneles de IP security (IPSEC) y seguridad de la capa de transporte (TLS), con certificado SSL/TLS v3, cuya llave deberá ser generada dentro de la plataforma de nube.
d. Conectividad dentro de la nube, el contratista deberá garantizar una latencia promedio de 1ms (1 milisegundo) en todas las conexiones de red internas dentro de la nube.
e. Conectividad entre nubes, en el caso que el contratista contemple la implementación de múltiples nubes, servicios de Cloud Computing deberá proveer lo siguiente:
    - Interconectar las nubes entre sí mediante conexión VPN-Site-to-Site o similar, con el fin de establecer una red privada segura.
    - Proveer una conectividad con latencia promedio de 10ms (10 milisegundos) en la comunicación entre nubes.
f. f) Conectividad con CENARES, el contratista deberá interconectar la nube hacia la red privada del CENARES mediante VPN-Site-to-Site o similar, a través de los enlaces a internet del CENARES. Se precisa que el CENARES cuenta con equipos de seguridad Next-Generation / PAN.
g. Conectividad a Internet, EL CONTRATISTA deberá incluir las IP Públicas necesarias de acuerdo al número de servicios publicados hacia internet en la nube que proponga:
    - EL CONTRATISTA deberá garantizar el acceso a internet de los servidores y servicios implementados en la nube,

MINISTERIO DE SALUD - CENARES - Oficina de Tecnologías de la Información y Comunicación - Oficina Central de Abastecimiento de Recursos Estratégicos en Salud - D. TORRES - V°B°

estableciendo mecanismos de filtrado y restricción, de acuerdo a las políticas de seguridad que determine el CENARES y contemplar un ancho de banda mínimo de 200Mbps.

- Se precisa que inicialmente se publicarán 13 servicios web hacia internet.

7.3.9 SEGURIDAD

a. Toda la solución requerida deberá contar con mecanismos de seguridad que garanticen la confidencialidad, integridad y disponibilidad de la información.
b. La solución proporcionada por EL CONTRATISTA deberá de manejar alguno de los siguientes protocolos de cifrado: AES o TDES o RSA o ECC para la protección de la transmisión de datos de todo el(los) entorno(s) Cloud Computing implementado(s).
c. Los servicios de nube(s) deben soportar la seguridad de datos de acuerdo con lo siguiente:
    - Datos en tránsito: con capacidad de cifrado con llave externa proporcionada por la nube.
    - Datos en reposo: con capacidad de cifrado de datos proveído por la plataforma y capacidad de cifrado de la(s) unidades de almacenamiento con llave externa proporcionada por la nube.
d. EL CONTRATISTA deberá habilitar medidas de seguridad a nivel de red que minimicen el impacto y/o alcance de ciberataques a los servicios.
e. El CONTRATISTA deberá de proporcionar un servicio de Protección Perimetral de internet, considerando como mínimo las funcionalidades de: Next Generation Firewall, IPS, Antivirus (con protección contra malware de día cero), DLP, Control de aplicaciones, Sandboxing (con capacidad de revisión mínima de 100 archivos/hora), antiDDoS y VPN (SSL & IPSEC), y esto podrá ser brindado por un firewall en modalidad IaaS en la medida que se cumpla técnica y funcionalmente todas las características indicadas. Opcionalmente podrá proveer mecanismos de evaluación en la adopción de mejores prácticas del fabricante de la solución propuesta y opcionalmente podrá prevenir la fuga de credenciales de la Entidad. Se precisa que, lo solicitado es que la soporte IPv4 e IPv6 para todo el entorno, de acuerdo al Decreto Supremo N°081-2017-PCM (Transición al protocolo IPv6 para las entidades de la Administración Pública), para su posterior implementación. La solución propuesta opcionalmente podrá estar acreditada o certificada por algún organismo internacional para su funcionamiento en IPv6. El servicio deberá tener una efectividad de seguridad mayor o igual al 90% de acuerdo a los reportes del 2021 o 2022 o 2023; de NSS Labs para Next Generation Firewall, el cual se acreditará mediante copia simple de constancias y/o certificados y/u otros documentos, según corresponda. Este documento deberá adjuntarse para el **perfeccionamiento del Contrato.**
f. EL CONTRATISTA deberá implementar la protección perimetral en alta disponibilidad, mediante la implementación en múltiples zonas de disponibilidad, de tal forma que cumplan con la disponibilidad requerida en la sección "Disponibilidad del Servicio" del presente TDR.

MINISTERIO DE SALUD - CENARES - Dirección de Tecnologías de la Información y Gestión - Dirección de Abastecimiento de Recursos Estratégicos en Salud
D. TORRES
V°B°

g. El servicio debe permitir que CENARES restrinja el acceso a determinados recursos basados en protocolos, URL's y direcciones IP, tanto para los servidores como plataformas y servicios. Así mismo opcionalmente podrá sugerir la adopción/modificación de políticas en base al tráfico cursado en el servicio, con la finalidad de afinar las políticas existentes.
h. EL CONTRATISTA deberá considerar la publicación de servicios para su acceso desde internet.
i. EL CONTRATISTA deberá proveer, a través de las tecnologías de la nube, un servicio de mitigación de ataques DDoS desde internet.

7.3.10 COPIAS DE SEGURIDAD / BACKUP

a. EL CONTRATISTA deberá proveer un servicio de backup (copias de seguridad) que incluya funcionalidades de: configurar políticas de copia de seguridad (frecuencia por hora), programación de los puntos de recuperación, configuración del periodo de conservación (diaria, semanal o mensual) y mecanismos que permitan su verificación (integridad de la información).
b. El proveedor debe contemplar un respaldo full backup inicial y luego incremental para todo el periodo del servicio, considerando lo siguiente: Considerar la retención de archivos de backup inicialmente por treinta (30) días en un ambiente de acceso frecuente. Al cumplirse el tiempo inicial estimado, debe pasar a un ambiente de acceso infrecuente durante 90 días. Al culminar este segundo periodo, debe pasar a un ambiente de archivamiento. Considerar que solo se deben mantener hasta las tres (3) últimas versiones del respaldo archivado.

7.3.11 DISASTER RECOVERY

a. La relación de equipos a contar con el servicio en nube de Disaster Recovery son los siguientes:

Nro	ID	Zona	Entorno	Tipo	Sistema Operativo	Servicio
1	SERVIDOR 1	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_01
2	SERVIDOR 2	Produccion	Aplicaciones Web	IaaS	Windows Server 2016	App_02
3	SERVIDOR 3	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_03
4	SERVIDOR 4	Produccion	Aplicación de escritorio	IaaS	Windows Server 2019	SIGA y SIAF
5	SERVIDOR 5	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
6	SERVIDOR 6	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
7	SERVIDOR 7	Produccion	Directorio Activo	IaaS	Windows Server 2019	DIRECTORIO ACTIVO
8	SERVIDOR 8	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
9	SERVIDOR 9	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
10	SERVIDOR 10	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
11	SERVIDOR 11	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
12	SERVIDOR 12	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
13	SERVIDOR 13	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
14	SERVIDOR 14	Produccion	NTP	IaaS	Linux	NTP
15	SERVIDOR 15	Produccion	Central IP	IaaS	Linux	CENTRAL IP
16	SERVIDOR 16	Produccion	Central IP	IaaS	Linux	CENTRAL IP

17	SERVIDOR 17	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
18	SERVIDOR 18	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
19	SERVIDOR 19	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_04
20	SERVIDOR 20	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
21	SERVIDOR 21	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
22	SERVIDOR 22	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_05
23	SERVIDOR 23	Produccion	File Server	IaaS	Windows Server 2019	FILE SERVER
24	SERVIDOR 24	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
25	SERVIDOR 25	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_06
26	SERVIDOR 26	Produccion	Aplicaciones Web	IaaS	Windows Server 2019	App_07
27	SERVIDOR 27	Produccion	Aplicaciones Web	IaaS	Linux	App_08
28	SERVIDOR 28	Produccion	Aplicaciones Web	IaaS	Linux	App_08
29	SERVIDOR 29	Produccion	Aplicaciones Web	IaaS	Linux	App_09
30	SERVIDOR 30	Produccion	Aplicaciones Web	IaaS	Linux	App_10
31	SERVIDOR 31	Produccion	Aplicaciones Web	IaaS	Linux	App_11
32	SERVIDOR 32	Produccion	Aplicaciones Web	IaaS	Linux	App_12
33	SERVIDOR 33	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
34	SERVIDOR 34	Produccion	BD	IaaS	Windows Server 2019	SQL SERVER
35	SERVIDOR 35	Produccion	Aplicación de escritorio	IaaS	Windows Server 2016	Bonovo

7.3.12 MONITOREO DE SERVICIOS

El Contratista deberá contar con una o más plataformas de monitoreo basados en nube, de acuerdo a lo siguiente:

a. Las herramientas y plataformas deberán realizar un monitoreo en modalidad 24x7x365.
b. El alcance del monitoreo es requerido para todos los servicios, servidores, bases de datos y aplicaciones web, de la Tabla N°1 y los que sean implementados por el Contratista en los entornos de nube.
c. Se deberá monitorear la disponibilidad de los servicios implementados a nivel de puertos, protocolos y servicios instalados.
d. Se deberá registrar la estadística de utilización de ancho de banda de todos los servicios, servidores y redes implementadas en la nube, en el consumo entre servidores, entre servicios, entre nube y hacia/desde internet.
e. Se deberá monitorear las tareas de respaldo de la información que ha sido almacenado durante el mes.
f. El servicio de monitoreo deberá almacenar información estadística de los últimos 12 meses.
g. Todos los servicios monitoreados deberán contar con umbrales de alerta y notificación por correo electrónico u otros medios como slack, telegram o similares.
h. Performance de Servidores y Servicios
    - Se deberá registrar la estadística de monitoreo de los componentes de servicios y servidores: uso de CPU, memoria, almacenamiento, tasas de lectura y escritura en disco.

MINISTERIO DE SALUD - OGTIES - Oficina de Tecnologías de la Información y Innovación - Oficina Nacional de Abastecimiento de Recursos Estratégicos en Salud
D. TORRES
V°B°

- Se deberá monitorear el estado de procesos, servicios y aplicaciones implementados, como servicios web, apache, nginx, IIS, glassfish, y otros servicios que se identifiquen durante la implementación.
- La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros.

i. Performance de Bases de Datos
   - Se deberá contar con estadísticas del rendimiento de las bases de datos, con el fin de evaluar la carga de trabajo, detectar problemas de rendimiento e identificar instrucciones SQL que causan sobrecarga.
   - La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros

j. Performance de Aplicaciones Web
   - Se deberá contar con un monitoreo de aplicaciones de tipo APM (Application Performance Monitoring), que permita realizar un seguimiento al comportamiento de las aplicaciones, medir el impacto en los usuarios finales en tiempo real
   - Se deberá contar con rastreo de errores y excepciones en la arquitectura de las aplicaciones y obtener visibilidad completa del rendimiento de cada aplicación
   - Se deberá contar con métricas de performance por aplicación.
   - Deberá soportar aplicaciones de tipo .Net, .Net Core 3, NodeJS 10.19, Glassfish, Java 8.2, .Net Framework 3.5,
   - La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros.

k. Analítica de eventos
   - EL CONTRATISTA deberá implementar un servicio de recopilación y normalización de eventos (logs), que incluya conectores para reunir los registros de varias fuentes, analizar los datos y mostrarlos en un formato de lectura común.
   - Se deberá recoger información de los eventos en todos los servicios, servidores y componentes implementados en la(s) nube(s), incluyendo a los eventos de los servicios de copia de seguridad.
   - Así mismo, el servicio debe registrar los eventos (logs) generados sobre cualquier alteración (alta, baja, modificación) de los componentes y configuraciones habilitados en la plataforma de nube(s), como supervisión de auditoría a las operaciones de usuarios administradores.

l. La solución podrá ser provista con soluciones nativas de nube, soluciones disponibles en marketplace's de nube o soluciones de terceros.

MINISTERIO DE SALUD - Gobierno de Chile - Dirección de Tecnologías de la Información y Estadísticas - Departamento de Abastecimiento de Recursos Estratégicos
D. TORRES
V°B°

7.3.13 PROTOCOLO DE PRUEBAS FUNCIONALES

a. EL CONTRATISTA, dentro del plazo de implementación y migración, deberá ejecutar un protocolo de pruebas para cada uno de los servicios, servidores y aplicaciones.
b. CENARES brindará un inventario de pruebas a realizar referente a los servicios, servidores y aplicaciones desarrolladas por la Entidad.
    - Validación funcional, se validarán los requisitos de funcionalidad de los componentes y servicios, en ambos lados del esfuerzo de migración a la nube.
    - Rendimiento, se medirán los rendimientos de una aplicación en condiciones reales como capacidad para manejar volúmenes de datos, cargas de cargas de capacidad y uso de vCPU y memoria.
    - Integración, se validarán los vínculos que puedan existir con otros servicios y/o servidores y/o aplicaciones para compartir datos, en la nube y en las instalaciones.
c. CENARES brindará el inventario de pruebas dentro de los siete (07) días calendarios, contabilizado desde el día siguiente de suscrito Contrato, considerando que dicho documento deberá ser trabajado en conjunto con el Contratista durante la fase de levantamiento de información.
d. EL CONTRATISTA deberá asegurarse, mediante reuniones de trabajo, la operatividad de las funcionalidades descritas en el inventario de pruebas, así como complementarlas con pruebas adicionales que identifique durante las reuniones de trabajo.
e. El protocolo de pruebas será aplicado durante la etapa de "Pre-Producción" y "Pase a Producción", para lo cual no deberá contar con observaciones en su ejecución, como requisito para la conformidad del servicio de implementación.

7.3.14 PRUEBAS DE ESTRÉS

a. EL CONTRATISTA, dentro del plazo de implementación y migración, deberá ejecutar un protocolo de pruebas de estrés para cada una de las aplicaciones desplegadas. Se aclara que, lo que se busca es medir la capacidad de la infraestructura, los tiempos de respuesta de las aplicaciones correspondiente a un número incremental de usuarios y el número límite de usuarios antes de la denegación de servicio de la plataforma.
b. El Contratista deberá considerar la cantidad de ciclos necesarios para garantizar el correcto funcionamiento de las aplicaciones; en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.
c. El Contratista deberá considerar la cantidad de escenarios necesarios para garantizar el correcto funcionamiento de las aplicaciones, en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.
d. Las pruebas de estrés son pruebas diferentes al protocolo de prueba funcionales. CENARES brindará un inventario de flujos de pruebas por cada aplicación web.
e. EL CONTRATISTA deberá emitir un informe de rendimiento por cada aplicación sujeta a estrés, describiendo el alcance máximo en concurrencia de usuarios.
f. El Contratista deberá considerar la cantidad de ciclos necesarios para garantizar el correcto funcionamiento de las aplicaciones;

en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.

g. El Contratista deberá considerar la cantidad de escenarios necesarios para garantizar el correcto funcionamiento de las aplicaciones, en las condiciones de mayor carga, alta concurrencia y el número límite de usuarios antes de la denegación de servicio de la plataforma.

7.3.15 SERVICIOS PROFESIONALES:

El proveedor deberá asegurar la provisión de los siguientes servicios:

a. Con respecto a la solución de recuperación:
   - Despliegue de un Gateway de conexión sobre la infraestructura VMware del cliente.
   - Conexión con la plataforma del SDDC a fin de establecer el canal de comunicaciones requerido.
   - Configuración de hasta 2 grupos de protección con las políticas de replicación requeridas.
   - Replicación de datos y validación de la integridad de esta.
   - Pruebas de operatividad.

b. Con respecto a los servicios de nube publica:
   - Deberá asegurar el despliegue de todos los elementos operativos en la solución de nube pública, necesarios a fin de asegurar que la plataforma se encuentre preparada para poder recibir cargas virtuales.
   - Deberá crear las políticas iniciales de seguridad, para garantizar lo siguiente:
     - El acceso a los servicios de administración desde direcciones IP públicas selectas, específicamente aquellas indicadas por La Entidad.
     - La configuración del entorno operativo base, que considere:
       - La inicialización de los recursos sobre un segmento de red ofrecido por el proveedor de nube pública para ello, y destinado exclusivamente para el uso de la Entidad
       - El establecimiento de las funcionalidades de Alta Disponibilidad, Balanceo de Carga, Deduplicación y Compresión de datos en la plataforma de operación.
       - El establecimiento de hasta dos (02) segmentos virtuales para alojar máquinas virtuales en diferentes segmentos de red.
       - El establecimiento de servicios de enrutamiento del tipo Este – Oeste, de modo que los segmentos diferentes dentro de la plataforma de nube puedan comunicarse sin necesidad de utilizar dispositivos de enrutamiento upstream, como pueden ser firewalls o routers externos.
         - ✓ Solamente los servicios que sean estrictamente necesarios deberán ser permitidos entre los

MINISTERIO DE SALUD - CNSG - Oficina de Tecnologías de la Información y Innovación - Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud
D. TORRES
V°B°

segmentos configurados, los que serán explícitamente indicados por la Entidad a fin de minimizar la comunicación entre VMs.

- ✓ Cualquier otro servicio que no sea aprobado, deberá ser restringido.

- El establecimiento de servicios Norte-Sur, para asegurar la comunicación de los servicios externos hacia otras redes o hacia Internet, los que deben considerar, como mínimo:
  - ✓ Enrutamiento desde el proveedor de nube hacia el centro de datos de la Entidad. Para ello, el proveedor previamente deberá establecer un túnel de comunicaciones del tipo VPN Site to Site con La Entidad.
- La Entidad será responsable de asegurar el acceso a internet, el ancho de banda de acceso y el uso de dispositivos de acceso perimetral que soporten protocolos estándares de la Industria, como IKE o Ipsec, a fin de poder establecer dicho Tunel. La Entidad será responsable de configurar los parámetros de la solución VPN de su lado, recibiendo la información que el proveedor configurará en el extremo de nube, esta información comprenderá los certificados digitales, claves de acceso, configuraciones del protocolo estándar o los necesarios para que se pueda establecer el canal de comunicaciones seguro entre ambos ambientes.
- El acceso de las VM hacia los servicios disponibles dentro de la Entidad deberá ser restringido a aquellos necesarios, tales como DNS, Active Directory, consultas a bases de datos o ICMP, debiendo impedir la salida del resto de servicios. En caso algún servidor virtual precise una salida particular, esto será informado al proveedor a fin de que solamente dicha VM cuente con ello.
  - ✓ Enrutamiento de salida hacia internet, el que deberá restringir los accesos mínimos necesarios que consuman las VM de la Entidad, como son DNS, HTTP, HTTPS, ICMP, debiendo impedir la salida del resto de servicios. En caso algún servidor virtual precise una salida particular, esto será informado al proveedor a fin de que solamente dicha VM cuente con ello. Para este particular,

MINISTERIO DE SALUD - CENARES - Oficina de Tecnologías de la Información y Gestión de Datos - Unidad de Asesoramiento de Recursos Estratégicos en Salud
D. TORRES
V°B°

todas las VM deberán ser ocultadas detrás de una dirección IP pública utilizando NAT para ello.

- ✓ Redirección de puertos desde internet hacia los servidores que precisen ser publicados. El postor debe asegurar la configuración de los servicios de NAT y de seguridad perimetral para que se asegure que solamente los servicios autorizados accedan desde internet, restringiendo el resto de los servicios.

- El establecimiento de las reglas de seguridad al entorno de administración en la nube, para que solamente se cuente con el ingreso autorizado desde las direcciones IP adecuadas. Esto será indicado por la Entidad al momento del despliegue.
- El despliegue de los servicios requeridos en el centro de datos de La Entidad, a fin de asegurar que se establezcan los servicios de comunicaciones y administración del ambiente On Premise de la Entidad y el entorno operativo en Nube, desde un solo punto de control. El ambiente de administración presentado para estos efectos deberá permitir la ejecución de las labores administrativas comunes como pueden ser la creación, modificación o eliminación de máquinas virtuales, despliegue de sistemas operativos y asignación de segmentos de redes.
- La disposición de un repositorio común disponible para el entorno de La Entidad y sincronizado para el consumo de los recursos en nube, a fin de que se puedan crear plantillas de máquinas virtuales, o se puedan disponer de los elementos de arranque de las máquinas virtuales para sus implementaciones individuales.

c. El proveedor del servicio de nube, debe asegurar:
   - La continuidad operativa de todos los servicios que soportan las VM a ser montadas en la nube.
   - La continuidad operativa de todos los servicios administrativos dispuestos para ello, considerando para los mismos las copias o protecciones de seguridad necesarios.
   - La actualización de la plataforma, la provisión de parches, fixes u otros necesarios que garanticen la integridad de la solución operativa.
   - La provisión de soporte técnico en un esquema 24x7 durante todo el periodo de la contratación, a fin de

resolver problemas operativos asociados a la plataforma o a elementos que no respondan según la documentación de la solución.
- Un SLA certificado de 99.9 % para la solución donde se ejecutarán los servicios de la Entidad.

d. La Entidad será responsable por:
   - Las facilidades necesarias de su lado para establecer los servicios de comunicaciones con el entorno productivo en nube.
   - Los enlaces de comunicaciones necesarios
   - Provisionar procesamiento para poder efectuar la interfaz de conexión y administración con el entorno de nube.
   - El anuncio con los proveedores del servicio de internet a fin de que la publicación de sus servicios no tenga inconvenientes.

7.4 PRESTACIÓN ACCESORIA:

7.4.1 SOPORTE TÉCNICO PROVISTO POR EL PROVEEDOR:

a. Como parte de la oferta integral, el proveedor deberá considerar la provisión de al menos diez (10) horas al mes, para poder acompañar a la Entidad en la administración y operación de la plataforma desplegada.
b. El soporte técnico brindado por el contratista estará orientado a cubrir situaciones de Break and Fix, es decir, inconvenientes con el funcionamiento de las soluciones listadas, entendiendo que el producto o software no responde según esperado.
c. El servicio deberá cubrir:
d. Revisión de componentes afectados para diagnóstico de inconvenientes.
e. Asistencia en la apertura de casos con el fabricante para atenciones de soporte
f. Asistencia en configuraciones administrativas generales asociadas a la solución.
g. Las horas se utilizarán en modalidad 24X7 para incidencias nivel 1 (Cliente sin servicio o servicio severamente degradado), y 5x9 para el resto de los casos.
h. La solicitud y respuesta podrá brindarse vía telefónica y/o por correo electrónico.
i. La atención será brindada de forma remota.
j. El servicio de soporte no cubre instalaciones, reinstalaciones, modificaciones de la arquitectura de la plataforma, adición de nuevos componentes, configuraciones complejas que no pertenezcan a las comunes administrativas, upgrades de versiones, u otros que no estén asociados directamente a eventos Break and Fix.

7.4.2 SERVICIOS DE CAPACITACIÓN:

El proveedor deberá ofrecer un curso taller en la administración de la plataforma ofertada, por un espacio de tiempo no menor a las doce (12) horas, a fin de cubrir todos los elementos necesarios para garantizar la correcta administración de la plataforma.

7.4.3 ACUERDO DE NIVEL DE SERVICIO

Para el registro de incidentes se utilizarán los medios de comunicación oficiales: sistema de tickets y/o teléfono y/o correo electrónico, los cuáles serán presentados al inicio del servicio.

Los acuerdos de niveles de servicio (SLA) para la atención de solicitudes de soporte técnico son:

Tiempos de respuesta:

Descripción	Tiempo respuesta máximo (*)
Tiempo de respuesta	01 hora

(*) El tiempo de respuesta se contabiliza a partir de la emisión, vía sistema de tickets y/o teléfono y/o correo electrónico, *del registro del incidente por parte del CENARES, hasta el inicio de la atención de soporte técnico por parte del contratista comunicado al CENARES.*

Tiempos de solución:

Urgencia del incidente	Tiempo solución máximo (**)
Alta	04 horas
Media	06 horas
Baja	12 horas

(**) El inicio del tiempo de solución se contabiliza a partir del tiempo de respuesta máximo correspondiente.

Alta: Son incidentes que necesita un tratamiento especial para la organización por su alto impacto; su inatención inmediata afecta o podría afectar significativamente la operación de algún componente de la de la infraestructura tecnológica.
Media: Son incidentes con un tiempo de atención intermedio; su inatención afecta o podría afectar moderadamente a la operación de algún componente de la infraestructura tecnológica.
Baja: Son incidentes con un tiempo de atención menor; su inatención afecta o podría afectar levemente a la operación de algún componente de la infraestructura tecnológica.

La clasificación de la urgencia la realizará el personal del CENARES en el registro del incidente.
El personal del CENARES verificará que se haya dado la solución al incidente antes de aceptar el fin del tiempo de solución.

7.4.4 SOPORTE TÉCNICO

El contratista deberá brindar soporte técnico durante la ejecución del servicio y de acuerdo con las siguientes características:

- Soporte técnico remoto a demanda disponible 7 días a la semana por 24 horas.
- Atención de incidentes: 7 días a la semana por 24 horas.
- Capacidad de registrar incidentes por Teléfono o por correo electrónico o por sistema de ticket.

8.0 PERFIL DEL POSTOR

- EL POSTOR debe contar con RUC activo y habido.
- EL POSTOR debe contar con RNP vigente.
- EL POSTOR no debe encontrarse impedido de contratar con el estado.
- EL POSTOR, debe ser representante autorizado o partner de la nube ofertada, el cual será acreditado con carta o certificado del fabricante. Con una vigencia no mayor a un año.
- EL POSTOR en su oferta debe acreditar mediante una carta y/o declaración jurada que cuenta con una mesa de servicio propia firmada por el representante legal de la empresa postora, que debe operar 24x7 y estará instalada en territorio nacional, brindando soporte a la gestión de incidencias, requerimientos por el tiempo de duración de la garantía comercial. Especificando la matriz de escalamiento en la cual precise nombres y apellidos, correo electrónico y número del contacto.
- EL POSTOR deberá detallar los nombres comerciales de los servicios que serán contratados para brindar el servicio a la Entidad; En el caso que la información técnica sea elaborada por el postor, deberá estar acompañada de información emita por el fabricante de la marca del producto ofertado, tales como brochures, fichas, enlaces, o similares, en el idioma original o traducciones. En el caso que la información técnica sea emitida por el fabricante, no será necesario acompañarla de información adicional, siempre que se precise cada uno de los apartados que son solicitados.
- El POSTOR deberá presentar para la firma del contrato los documentos que acrediten el grado académico del personal clave, así como su experiencia en la solución ofertada y las respectivas certificaciones (copia simple de los certificados), según el siguiente detalle:

- Un (01) Gestor de Proyectos:

- Un (01) Especialista de Implementación:
  - ✓ Arquitecto en la nube ofertada o certificado oficial en seguridad de la nube ofertada, o certificado de Arquitecto nivel experto o nivel profesional de Servicios de la nube ofertada o certificado en virtualización de Datacenter y especialista certificado en la solución de virtualización sobre la nube ofertada validado por una entidad certificadora internacional, pudiendo ser visualizado en www.credly.com.

9.0 PERSONAL CLAVE

9.1. JEFE DE PROYECTO

9.1.1 Cantidad:

Uno (01).

9.1.2 Requisitos:

- Título universitario en Ingeniería de Sistemas o Ingeniería Informática o Ciencias de la Computación o Ingeniería de Telecomunicaciones o Ingeniería Electrónica, del personal clave requerido como Gestor de Proyecto.
- Certificación PMP activa.
- Certificación ITIL activa.
- Cuatro (04) años de experiencia en proyectos de la plataforma propuesta u otros proyectos asociados a nube pública o privada como Gestor o coordinador o jefe de Proyectos.

9.1.3 Acreditación:

El postor deberá acreditar a su personal con:

- El título profesional requerido, que será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/. y Títulos a cargo del Ministerio de Educación a través del siguiente link :http://www.titulosinstitutos.pe/, según corresponda.
- En caso el título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
- La experiencia se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
- De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

9.2. ESPECIALISTA DE IMPLEMENTACIÓN

9.2.1 Cantidad:

Uno (01).

9.2.2 Requisitos:

- Título técnico, universitario o bachiller en Ingeniería de Sistemas o Ingeniería Informática o Ciencias de la Computación o Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Computación e informática, del personal clave requerido como Especialista de Implementación.
- Un (01) año de experiencia en soluciones de la plataforma propuesta como Especialista en Implementación de la solución ofertada.

9.2.3 Acreditación:

El postor deberá acreditar a su personal con:

- El título profesional requerido, que será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/. y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda.
- En caso el título profesional no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
- La experiencia se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
- De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

10.0 PRODUCTO(S) O RESULTADO(S) A OBTENER

Servicio de Infraestructura en la nube para recuperación ante desastres y aprovisionamiento de recursos.

11.0 LUGAR DE ENTREGA O EJECUCIÓN DE LA PRESTACIÓN

El servicio se realizará en la plataforma virtual de la marca ofertada.

12.0 PLAZO DE DURACIÓN DEL SERVICIO E INSTALACIÓN

El plazo de ejecución del servicio será de 1095 días calendarios, contados a partir del día siguiente de haber culminado la etapa de implementación y migración del servicio.

Para el inicio del proyecto el contratista y CENARES firmarán el Acta de Inicio de Proyecto en mutua coordinación; para la contabilización de las fechas en cada etapa.

Las etapas por desarrollarse serán las siguientes:

Etapa	Plazo	De la entidad
Entrega del Plan de Trabajo	El contratista presentará dentro de los cinco (05) días calendarios como máximo contabilizados a partir del día siguiente de suscrito el contrato y/o emitida la Orden de Servicio a través de mesa de partes.	La OTI (Oficina de Tecnología de la Información) del CENARES aprobará dicho plan y lo notificará mediante correo electrónico dentro de los dos (02) días calendarios contabilizados a partir del día siguiente de recibido por mesa de partes.
Capacitación	Se realizará dentro de los diez (10) días calendarios como máximo contabilizados a partir del día siguiente de aprobado el Plan de Trabajo.	El contratista entregará los certificados o constancias y el acta de cumplimiento de capacitación a la Entidad a través de correo electrónico a la cuenta licencias@cenares.gob.pe, dentro de los dos (02) días calendarios siguientes de culminada la capacitación.
Implementación y migración del servicio	Se realizará dentro de los sesenta (60) días calendarios como máximo contabilizados a partir del día siguiente de aprobado el Plan de Trabajo.	Se suscribirá el Acta de Implementación y migración.
Inicio del servicio para producción	Se determinará mediante acta suscrita por el contratista y CENARES, al día siguiente de realizada la implementación y migración del servicio y haber entregado el Acta de cumplimiento de capacitación.	Se suscribirá el Acta de Inicio de Servicio. y a partir del día siguiente de suscrita dicha acta se iniciará la contabilización de los mil noventa y cinco (1095) días calendarios de prestación del servicio, según lo acordado.

De existir observaciones en la presentación del Plan de Trabajo, se levantará un informe y se comunicará al contratista a través de la unidad funcional encargada de las Contrataciones, indicándose claramente el sentido de éstas, dándose al

contratista un plazo prudencial para la subsanación, en función a la complejidad del servicio.

Dicho plazo no podrá ser menor de dos (02) ni mayor de cuatro (04) días calendarios. La subsanación a las observaciones será presentada por correo electrónico a licencias@cenares.gob.pe, debiendo el Contratista presentar la subsanación y entrega de la parte observada completa de la etapa correspondiente.

13.0 ENTREGABLES POR EL SERVICIO

Una vez culminada la instalación, configuración y pruebas se suscribirá un acta de implementación del servicio, para ello el proveedor deberá entregar la siguiente documentación técnica:

- Acta de suscripción del servicio.
- Acta donde se haya realizado un test de velocidad.
- Relación de equipos de comunicación instalados o renovados o configurados.
- Una matriz de contactos directos como número de teléfono, correo electrónico, y guía para abrir casos de ticket de incidencia.
- El proveedor deberá incluir un Diagrama de la arquitectura (interconexión, redes, protocolos, etc.) de la solución oferta, incluyendo todo lo que constituye lo implementado una vez finalizando la implementación.

14.0 GARANTÍA DEL SERVICIO

La garantía que el postor brinde al servicio realizado entrará en vigencia a partir del inicio del servicio; y tendrá una duración mínima de (36) meses.

15.0 CONFORMIDAD

La conformidad será emitida por la Oficina de Tecnologías de la Información e Innovación previa presentación de los entregables.

16.0 FORMA DEL PAGO

El pago será realizado en forma mensual, luego de haber sido entregada el informe sobre el diagnóstico de la línea dedicada y la conformidad del servicio por la Oficina de Tecnologías de la Información e Innovación.

17.0 ADELANTOS

No aplica.

18.0 MODALIDAD DEL SISTEMA DE CONTRATACIÓN

Suma Alzada.

19.0 PENALIDAD

a. Penalidades por mora

El incumplimiento de la entrega de los equipos y prestación de los servicios, estará sujeto a la aplicación de penalidades, de conformidad con lo dispuesto en el artículo 116 de Reglamento.

"La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto}}{F \times \text{plazo en días}}$$

Donde F tendrá los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días, para bienes, servicios en general, consultorías y ejecución de obras: F = 0.40.

b) Para plazos mayores a sesenta (60) días:

b.1) Para bienes, servicios en general y consultorías: F = 0.25.

b.2) Para obras: F = 0.15."

b. Otras Penalidades

Serán evaluadas durante el plazo máximo de responsabilidad del CONTRATISTA y aplicadas según el caso cuando el PROVEEDOR incurra en falta. Para tal finalidad se utilizará lo establecido en el siguiente cuadro:

N°	SUPUESTO DE APLICACIÓN DE PENALIDAD	FORMA DE CALCULO	PROCEDIMIENTO
1	Cuando el Proveedor supere el tiempo máximo de solución de atención de una avería.	5 % del valor de una (01) UIT.	Mediante informe de la Oficina de Tecnologías de la Información e Innovación del CENARES.
2	No cumplir con la entrega del plan de trabajo dentro del plazo establecido Cuando el Proveedor supere el tiempo de cambio de equipos por falla de los mismos.	10 % del valor de una (01) UIT.	Mediante informe de la Oficina de Tecnologías de la Información e Innovación del CENARES.

20.0 NORMAS ANTICORRUPCION

El PROVEEDOR acepta expresamente que no llevará a cabo, acciones que están prohibidas por las leyes locales u otras leyes anticorrupción, Sin limitar lo anterior, EL PROVEEDOR se obliga a no efectuar algún pago, ni ofrecerá o transferirá algo de valor, a un funcionario o empleado gubernamental o a cualquier tercero relacionado con la adquisición aquí establecido de manera que pudiese violar las leyes locales u otras leyes anticorrupción, sin restricción alguna.

En forma especial, EL PROVEEDOR declara con carácter de declaración jurada que no se encuentra inmerso en ningún procedimiento de carácter penal vinculado a presuntos ilícitos penales contra el Estado Peruano, constituyendo su declaración, la firma del mismo en la Orden de servicio de la que estos términos de referencia forman parte integrante.

21.0 NORMAS ANTISOBORNO

El PROVEEDOR, no debe ofrecer, negociar o efectuar, cualquier pago, objeto de valor o cualquier dádiva en general, o cualquier beneficio o incentivo ilegal en relación al contrato, que pueden constituir un incumplimiento a la Ley, tales como robo, fraude, cohecho o tráfico de influencias, directa indirectamente, o a través de socios, integrantes de los órganos de administración, apoderados, representantes legales,

funcionarios asesores o personas vinculadas, en concordancia o a lo establecido en el artículo 11° de la Ley de Contrataciones del Estado, Ley N° 30225 y sus modificatorias, y el artículo 7 de su Reglamento, aprobado mediante Decreto Supremo N° 344-2018-EF.

Asimismo, el proveedor se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción. Directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes de los órganos de administración apoderados, representantes legales, funcionarios, asesores y personas vinculadas en virtud a lo establecido en los artículos antes citados de la Ley de Contrataciones del Estado y su Reglamento.

Asimismo, el PROVEEDOR se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviere conocimiento; así también en adoptar medidas técnicas, prácticas, a través de los canales dispuestos por el CENARES.

De la misma manera, el proveedor es consciente que, de no cumplir con lo anteriormente expuesto, se someterá a la resolución del contrato a las acciones civiles y/o penales que el CENARES pueda accionar.

22.0 CONFIDENCIALIDAD Y PROPIEDAD INTELECTUAL

El contratista del servicio tiene y asume la obligación, tanto durante la vigencia del contrato, como después de su extinción, de guardar el secreto y la confidencialidad de cualquier información del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud - CENARES a la que tenga acceso como consecuencia del desempeño de su servicio, quedando expresamente prohibido revelar dicha información.

MINISTERIO DE SALUD - CENARES - Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud - Oficina de Tecnologías de la Información y Telecomunicaciones - D. TORRES - V°B°

Por lo expuesto en el párrafo precedente, el proveedor del servicio no podrá:

- Difundir, transmitir o revelar información a terceros.
- Usar la información recopilada para ofrecer, promocionar o brindar información sobre productos o servicios.
- Arrendar ni vender a terceros ningún dato de identificación personal que les haya sido proporcionado por el CENARES o como consecuencia del servicio brindado.
- Invitar al usuario a tomar parte en encuestas sobre productos, servicios, noticias o eventos.

la obligación de confidencialidad no resulta aplicable en los siguientes supuestos:

- Cuando la información en cuestión haya sido de difusión o acceso público;
- Cuando la información en cuestión haya sido publicada antes de haber sido puesta a disposición del postor;
- Cuando la información en cuestión ya obré en poder del postor y no esté sujeta a cualquier otro impedimento o restricción que le haya sido puesto de manifiesto;
- Cuando la información en cuestión haya sido recibida a través de terceros sin restricciones y sin que implique incumplimiento del Contrato;
- Cuando la información en cuestión haya sido independientemente desarrollada por el postor, siempre que no se hubiese utilizado para ello otra información confidencial; o
- Cuando la información en cuestión deba ser revelada a alguna autoridad autorizada para dar cumplimiento a una orden de naturaleza judicial o administrativa, bastando para ello informar a la Entidad la recepción de dicha orden.

23.0 RESPONSABILIDAD POR VICIOS OCULTOS

El contratista será responsable por los vicios ocultos del bien ofertado, conforme a lo indicado en el Artículo 40° de la Ley de Contrataciones y 173° del Reglamento de la Ley de Contrataciones del Estado, por un plazo mínimo de **un (01) año**, el cual será contabilizado a partir de la conformidad otorgada por el Equipo de Informática del CENARES.

ING.DEIVHY PAUL TORRES VARGAS
Director
Oficina de Tecnologías de la Información e Innovación
Centro Nacional de Abastecimiento
de Recursos Estratégicos en Salud - CENARES
MINISTERIO DE SALUD

NOMBRE Y APELLIDO
FIRMA Y SELLO DEL JEFE DEL ÁREA USUARIA

24. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	Requisitos: • El postor deberá contar con la Constancia vigente de estar inscrito en el Registro Nacional de Proveedores como proveedor de Servicios. • El postor deberá contar al menos una de las siguientes certificaciones: ➢ ISO 27001:2013, de seguridad de la información relacionados a los Servicios Cloud, Acceso Dedicado a Internet y Centro de Datos. ➢ ISO/IEC 27017, Controles de seguridad de la información basada en ISO/IEC 27002 específicamente para los servicios en nube. ➢ ISO/IEC 27018, Requisitos para la protección de la información de identificación personal (PII) en sistemas Cloud. ➢ La solución deberá estar alojada en un centro de datos de clase mundial, con certificaciones internacionales como las del Uptime Institute. Importante *De conformidad con la Opinión N° 186-2016/DTN, la habilitación de un postor, está relacionada con cierta atribución con la cual debe contar el proveedor para poder llevar a cabo la actividad materia de contratación, este es el caso de las actividades reguladas por normas en las cuales se establecen determinados requisitos que las empresas deben cumplir a efectos de estar habilitadas para la ejecución de determinado servicio o estar autorizadas para la comercialización de ciertos bienes en el mercado.* Acreditación: • Copia simple de constancia RNP vigente. • Copia simple de certificado ISO 27001 o ISO/IEC 27017 o ISO/IEC 27002 o ISO/IEC 27018. • Copia simple de certificado Uptime Institute. Importante *En el caso de consorcios, cada integrante del consorcio que se hubiera comprometido a ejecutar las obligaciones vinculadas directamente al objeto de la convocatoria debe acreditar este requisito.*

	Acreditación: • *Copia de la constancia vigente de estar inscrito en el Registro Nacional de Empresas y Entidades que realizan actividades de intermediación laboral – RENEEIL, expedida por el Ministerio de Trabajo y Promoción del Empleo.*
B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
	CALIFICACIONES DEL PERSONAL CLAVE
	FORMACIÓN ACADÉMICA
	Un (01) Gestor de Proyectos: Requisitos: ✓ Título universitario en Ingeniería de Sistemas o Ingeniería Informática o Ciencias de la Computación o Ingeniería de Telecomunicaciones o Ingeniería Electrónica, del personal clave requerido como Gestor de Proyecto. **Un (01) Especialista de Implementación:** Requisitos: ✓ Título técnico, universitario o bachiller en Ingeniería de Sistemas o Ingeniería Informática o Ciencias de la Computación o Ingeniería de Telecomunicaciones o Ingeniería Electrónica o Computación e informática, del personal clave requerido como Especialista de Implementación. Acreditación: El título o grado académico será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe// o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda. El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido. En caso el TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

MINISTERIO DE SALUD - OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - D. TORRES - V°B°

	EXPERIENCIA DEL PERSONAL CLAVE
	Un (01) Gestor de Proyectos: Requisitos: ✓ Experiencia mínima de cuatro (04) años en proyectos de la plataforma propuesta u otros proyectos asociados a nube pública o privada como Gestor o coordinador o jefe de Proyectos. **Un (01) Especialista de Implementación:** Requisitos: ✓ Experiencia mínima de un (01) año en soluciones de la plataforma propuesta como Especialista en Implementación de la solución ofertada. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. Importante • *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento* *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.* *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.* • *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*

MINISTERIO DE SALUD - OGTIC
Oficina de Tecnologías de la Información
D. TORRES
V°B°
Oficina de Recursos Estratégicos

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 700,000.00 (setecientos mil y 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: ✓ Servicio de Infraestructura en Nube (Cloud) – IaaS, y/o ✓ Servicios de Infraestructura de Aplicaciones en Internet (Cloud), y/o ✓ Servicio de infraestructura sobre la nube o servicio de centro de datos (Datacenter) de la nube o servicios realizados en administración de infraestructura Cloud Computing y/o hosting de infraestructura gestionada o servicios de alquiler de infraestructura como pueden ser: alquiler de servidores o sistemas de almacenamiento y/o ✓ Contratación de servicio de correo electrónico, mensajería y sites colaborativos a través de la nube y/o ✓ Contratación de servicio de servicio de suite de herramientas de productividad y colaboración en la nube. ✓ Transmisión de vos y datos y/o interconexión (enlace de datos de sedes), y/o Servicio de Ancho de banda y/o internet en general. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso sólo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, sólo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la

MINISTERIO DE SALUD - OGTIES - Oficina de Tecnologías de la Información en Salud - Oficina de Abastecimiento de Recursos Estratégicos en Salud - D. TORRES - V°B°

Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso de que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.**
Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

Importante
• *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.* • *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado*

MINISTERIO DE SALUD - Oficina de Tecnologías de la Información y Estadística - D. TORRES - V°B° - Fortalecimiento de Recursos Estratégicos

25.0 PLAN DE TRABAJO

Dentro de los quince (15) días calendarios siguientes de suscrito el contrato, El CONTRATISTA presentará el Plan de Trabajo con toda la información necesaria que corresponde a la implementación del servicio. El cual deberá ser presentado por mesa de partes en formato digital o impreso. El Plan de Trabajo incluirá:

- Memoria descriptiva de la implementación.
- Propuesta de la mejor arquitectura de la infraestructura tecnológica Cloud Computing que garantice la disponibilidad, integridad, seguridad y funcionalidad de los servicios, aplicaciones, sistemas y bases de datos, incluyendo diagramas, documentos y anexos.
- Cronograma de actividades, fecha de inicio y fin, restricciones, hitos, predecesoras, etc.– Formato Project.
- Documento de configuración de entornos, que deberá incluir:
  - ✓ Características técnicas de los elementos habilitados en la plataforma "Cloud Computing" y configuraciones realizadas en los ambientes.
  - ✓ Características de la región y ubicación geográfica donde se habilitarán los servicios.
- Plan de Disaster Recovery
- Procedimiento para la ejecución y almacenamiento de respaldos.
- Documento de medidas para la protección de datos en tránsito y cifrado en reposo.
- Equipo de trabajo (que deberá incluir al personal clave, contacto, roles y funciones).
- Lista de servicios, sistemas y aplicaciones de CENARES a migrar a la nube.
- Protocolo de pruebas.
- Procedimiento de pase a producción y rollback.
- Temario de capacitación (syllabus)
- Documentos de acreditación de conocimientos del o los Capacitador(es) respecto al Syllabus a dictar.
- Acuerdo de confidencialidad suscrito.

La Oficina de Tecnologías de la Información e Innovación, tendrá como máximo siete (07) días calendarios, una vez recepcionado el plan de trabajo, para comunicar por correo electrónico, la aprobación del plan o alguna observación al contratista.

De existir observaciones, se le comunicará a EL CONTRATISTA, mediante correo electrónico, dándole un plazo de subsanación no menor a dos (02) días calendarios y no mayor a ocho (08) días calendarios, de acuerdo a la complejidad de las mismas.