CAJA DE SEGURO SOCIAL

Dirección Ejecutiva Nacional de Innovación y Transformación

PANAMÁ 2 DE ABRIL DE 2025.

ESPECIFICACIONES TÉCNICAS REQUERIDAS

"SUMINISTRO DE INFRAESTRUCTURA TECNOLÓGICA PARA SISTEMAS CRÍTICOS PARA LA CAJA DE SEGURO SOCIAL (C.S.S.)"

I. ANTECEDENTES.

La Caja de Seguro Social con el fin de cumplir con sus principios de forma diligente, completa y eficiente, garantizando a los asegurados y dependientes la prestación de los servicios de salud y prestaciones económicas con un enfoque integral en la atención y cumpliendo con las funciones que le asigna la Ley 51 de 27 de diciembre de 2005 y al ser esta de orden público e interés social está llamada a garantizar, por medio de la Dirección Ejecutiva Nacional de Innovación y Transformación, la estabilidad y operación ininterrumpida de los diferentes sistemas que conforman la plataforma tecnológica de la institución.

La Caja de Seguro Social cuenta con Cuatro (4) Plataformas Tecnológicas principales: SIPE "Sistema de Ingresos y Prestaciones Económicas", SIS "Sistema de Información de Salud y SAFIRO "Sistema Administrativo y Financiero" y Sistema de Telemedicina, las plataformas tecnológicas actuales presentan deficiencias significativas debido a su obsolescencia y a las limitaciones sustanciales en su infraestructura de hardware. Esta situación impacta

negativamente la eficiencia operativa y restringe la capacidad de adaptación a las demandas tecnológicas emergentes.

1. Sistema de Ingresos y Prestaciones Económicas (SIPE)

En 2008, se implementó el Sistema de Ingresos y Prestaciones Económicas (SIPE) con el objetivo de automatizar procesos críticos. Esto incluyó la afiliación de asegurados, la inscripción de empleadores, la declaración y facturación de planillas, así como la gestión de ingresos y el control de cartera y morosidad. El SIPE se consolidó como un Sistema Integrado de Recaudación de Ingresos a nivel nacional, abarcando los programas de Invalidez, Vejez y Muerte (IVM), Enfermedad y Maternidad (EM) y Riesgos Profesionales, todo ello operando en un entorno de misión crítica disponible las 24 horas del día, los 7 días de la semana.

La implementación del SIPE no se completó satisfactoriamente, lo que ha generado significativas disfunciones operativas. Además, la ausencia de la funcionalidad de prestaciones económicas ha comprometido la generación oportuna de informes financieros institucionales.

2. Sistema de Información de Salud (SIS)

El Sistema de Información en Salud (SIS) fue concebido para revolucionar la atención al paciente, facilitando la interconexión entre hospitales, policlínicas y centros de atención primaria. Su objetivo primordial es consolidar un expediente médico único, accesible desde cualquier unidad ejecutora de la Caja de Seguro Social a nivel nacional. No obstante, la implementación incompleta del SIS y los persistentes problemas de conectividad y rendimiento han generado retrasos significativos en la atención. Esta situación obstaculiza la disponibilidad oportuna de información crítica del paciente, comprometiendo la continuidad y eficacia de

los tratamientos y generando una reticencia entre los usuarios a depender del sistema.

3. Sistema Administrativo Financiero (SAFIRO)

El Sistema Administrativo Financiero (SAFIRO), basado en la plataforma SAP, se introdujo en 2011 con el objetivo de modernizar y consolidar la gestión administrativa y financiera a nivel nacional, abarcando áreas como contabilidad, finanzas, presupuesto y compras, anteriormente gestionadas en el sistema MAINFRAME. Sin embargo, la implementación de SAFIRO ha sido incompleta, alcanzando solo el 54% de su funcionalidad prevista. Esta situación ha obligado a mantener la operación simultánea de SAFIRO (SAP) y MAINFRAME, generando ineficiencias y retrasos significativos en la generación de informes financieros institucionales y el incremento significativo en los costos operativos, lo anterior expuesto reduce la eficiencia y aumenta los riesgos de seguridad.

4. Sistema Telemedicina

La implementación de un sistema de telemedicina en la Caja de Seguro Social (CSS) se inició con el propósito de expandir y fortalecer la prestación de servicios médicos a nivel nacional, especialmente en áreas remotas. Este sistema, que facilita consultas virtuales y optimiza el uso de recursos médicos, ha permitido incorporar especialidades como nefrología y neurología, con planes de expansión hacia cardiología y la evaluación remota de infartos cerebrales (telestroke). A pesar de su potencial para mejorar la interacción médico-paciente mediante videollamadas y reducir la dependencia de traslados y consultas presenciales, la implementación ha sido incompleta y desigual en todo el país. La cobertura limitada y la coexistencia de consultas presenciales y virtuales han disminuido la eficiencia del sistema y su capacidad para reducir la mora médica. Esta situación compromete la disponibilidad de servicios especializados, afecta la capacidad de

respuesta de los centros médicos e impide la optimización de recursos, además de limitar la generación de informes estadísticos cruciales para evaluar la efectividad del sistema.

II. OBJETIVO GENERAL

Modernizar la infraestructura tecnológica para la Dirección Nacional de Informática (DNI), de la Caja del Seguro Social (C.S.S.), a través de la modernización de bienes y servicios, garantizando la disponibilidad de recursos tecnológicos que permita la optimización y eficiencia en el uso de los aplicativos de SIPE "Sistema de Ingresos y Prestaciones Económicas", SIS "Sistema de Información de Salud y SAFIRO "Sistema Administrativo y Financiero" y Sistema de Telemedicina de la institución.

III. OBJETIVOS ESPECIFICOS

- Dotar a la Caja de Seguro Social (C.S.S.), de una infraestructura robusta que incluya las comunicaciones, virtualización, alta disponibilidad, redundancia y escalabilidad de la infraestructura.

- Implementar y optimizar integralmente la plataforma SIPE, asegurando su funcionalidad completa en todos los módulos: afiliación de asegurados, inscripción de empleadores, gestión de planillas, recaudación de ingresos y control de morosidad. Garantizar la operatividad del sistema en un entorno de misión crítica 24/7, cubriendo los programas de IVM, EM y Riesgos Profesionales a nivel nacional.

- Garantizar la implementación y operatividad plena del SIS en todas las unidades ejecutoras de la CSS a nivel nacional, resolviendo integralmente los problemas de conectividad y rendimiento para asegurar el acceso

eficiente al expediente médico único del paciente desde cualquier ubicación, eliminando las causas del 'no uso' del sistema.

- Culminar la implementación de SAFIRO (SAP) al 100%, migrando todas las funciones administrativas y financieras (contabilidad, finanzas, presupuesto, compras) desde MAINFRAME, garantizando la generación oportuna y precisa de informes financieros institucionales mediante la operación exclusiva de SAFIRO.

- Desarrollar e implementar una plataforma de telemedicina nacional integral, con módulos de teleconsulta para atención primaria y especializada. Establecer un sistema integrado de atención remota con disponibilidad 24/7, asegurando la continuidad y confiabilidad del servicio. Implementar rigurosas medidas de protección de datos y ciberseguridad, cumpliendo con las normativas nacionales e internacionales, para garantizar la privacidad de la información de los pacientes.

IV. ALCANCE

La Dirección Nacional de Informática de la Caja de Seguro Social, considera estratégico e inaplazable el fortalecimiento de la infraestructura tecnológica de la entidad. Para tal fin, ha realizado un levantamiento de las necesidades de recursos tecnológicos y el dimensionamiento de los requerimientos de cómputo y almacenamiento, que permita atender las necesidades presentes, y tome en consideración la proyección de demanda que tendrá la entidad en materia de aplicativos y servicios, para los próximos años.

De manera resumida, la infraestructura tecnológica requerida comprende los siguientes componentes:

- Una plataforma hiperconvergente (HCI) con almacenamiento definido por software.
- Servidores optimizados para hiperconvergencia, optimizados y certificados para emplearse con la plataforma HCI que se proponga.
- Equipos activos de comunicaciones (switches).
- Servicios profesionales para la instalación, configuración, soporte, mantenimiento y capacitación.

Para el caso específico del nuevo SIS, que como parte de otro proyecto se ha venido desarrollando en la nube con servicios AWS, será necesario proveer como parte complementaria de la infraestructura tecnológica, servicios AWS para mantener las interfaces de usuario ya desarrolladas y probadas.

La Dirección Nacional de Informática de la Caja de Seguro Social, tendrá a su cargo todos los aspectos relacionados con Ciberseguridad, incluyendo el establecimiento de políticas, normas, procesos, auditoría y remediación de plataformas, servicios y aplicativos. Las obligaciones y responsabilidades del proveedor, en esta materia, están contenidas en los item anexados.

De igual manera, la Dirección Nacional de Informática de la Caja de Seguro Social se encargará de proporcionar los data centers y los espacios necesarios para la instalación de los nuevos sistemas, así como los enlaces de comunicación y el acceso a Internet.

El proveedor acepta que una vez la C.S.S., certifique la recepción a satisfacción de cada uno de los bienes implantados por el Proveedor, de su solución tecnológica para cada data center y debidamente licenciados según corresponda, estos bienes pasarán a ser propiedad de la entidad.

El proveedor deberá aportar documentación de las Especificaciones Técnicas detalladas para las diferentes plataformas a implementar.

PRECIO DE REFERENCIA: Veintisiete Millones Ciento Ochenta y Cinco Mil Trescientos Balboas con 00/100 (B/.27,185,300.00).

V. TIEMPO DE ENTREGA:

Los tiempos de entrega de cada hito están definidos de la siguiente manera:

Hito 1

- Entregable: Plan de Trabajo, Cronograma de Trabajo y Diseño de la Solución.
- Plazo de entrega: 30 días calendario a partir de la notificación de la Orden de Proceder.

___

Hito 2

- Entrega de los equipos especificados en el contrato.
- Plazo de entrega: 120 días calendario a partir de la notificación de la Orden de Proceder.

___

Hito 3

- Entrega de las licencias necesarias para la solución.
- Plazo de entrega: 180 días calendario a partir de la notificación de la Orden de Proceder.

___

Hito 4

- Entrega final de la solución implementada conforme a los requisitos del contrato.
- Plazo de entrega: 270 días calendario a partir de la notificación de la Orden de Proceder.

___

Hito 5 – Entrega mensuales en el año 2026

- Entregable: Informes mensuales de entrega-recepción y avance del proyecto.
- Plazo de entrega: Cada mes, durante el año 2026, con un total de 12 entregas.

- Condición: Cada informe debe ser aprobado por la entidad contratante para dar paso al pago mensual.

___

Hito 6 – Entrega mensuales en el año 2027

- Entregable: Informes mensuales de entrega-recepción y avance del proyecto.
- Plazo de entrega: Cada mes, durante el año 2027, con un total de 12 entregas.
- Condición: Cada informe debe ser aprobado por la entidad contratante para dar paso al pago mensual.

VI. FORMA DE PAGO:

La CSS pagará al proveedor, luego de la presentación de los Informes de Avance en donde se haga constar la ejecución del proyecto al cual se asocia cada uno de los siguientes hitos de pago:

Hito 1 20% del monto asignado
Entrega y Diseño de la Solución.

- Monto: B/. 1, 620,000.00

___

Hito 2 – 40% del monto asignado para el primer año (2025)

- Condición de pago: Entrega y aceptación de los equipos especificados en el contrato.
- Monto: B/. 3, 240,000.00

___

Hito 3 – 20% del monto asignado para el primer año (2025)

- Condición de pago: Entrega y aceptación de las licencias necesarias para la solución.
- Monto: B/. 1, 620,000.00

___

Hito 4 – 20% del monto asignado para el primer año (2025)

- Condición de pago: Entrega final y aceptación de la solución implementada conforme a los requisitos del contrato.
- Monto: B/. 1, 620,000.00

___

Hitos recurrentes por entrega mensual de informes (Años 2 y 3 - 2026 y 2027)

Hito 5 – Pagos recurrentes en 2026

- Monto total: B/. 9, 542,650.00
- Monto mensual: B/. 795,220.83
- Condición de pago: Presentación y aceptación del informe mensual de entrega-recepción.

___

Hito 6 – Pagos recurrentes en 2027

- Monto total: B/. 9, 542,650.00
- Monto mensual: B/. 795,220.83
- Condición de pago: Presentación y aceptación del informe mensual de entrega-recepción.

Condiciones Generales de Pago

- Todos los pagos estarán sujetos a la aceptación por parte de la entidad contratante de las entregas realizadas.
- La no presentación o el rechazo de los informes o entregables en los plazos establecidos podrá afectar el desembolso del pago correspondiente.
- Los pagos serán realizados conforme a los términos establecidos en el contrato, previa presentación de la facturación correspondiente y validación del cumplimiento de cada hito o entrega.

Se deberá entregar manuales y panfletos descriptivos de los equipos propuestos.

VII. ESPECIFICACIONES TÉCNICAS

Item	***Especificaciones Técnicas***
A	**Infraestructura para SIPE (Sistemas de Ingresos y Prestaciones Económicas) y SIS (Sistema de Información de Salud).** Requerimientos mínimos de hardware para la plataforma:
A.1.	Todo el almacenamiento debe estar basado en NVMe para garantizar alto rendimiento y baja latencia.
A.2.	Cada servidor (nodo) ofertado debe tener doble procesador, cada procesador con mínimo 32 núcleos y una frecuencia de reloj mínima de 2.5 GHz por núcleo.
A.3.	Cada servidor (nodo) deberá proporcionar al menos 1024 GB de memoria RAM instalada, en módulos de memoria de 64GB operando a 5600 MHz o superior.
A.4.	Cada servidor (nodo) debe proporcionar almacenamiento distribuido en discos NVMe con al menos ocho (8) discos 7.68TB.
A.5.	Cada servidor (nodo) debe ofrecer mínimo dos (2) tarjetas “dual” de dos (2) puertos SFP de 10/25 GbE, y una (1) tarjeta “dual” de dos (2) puertos GbE BASE-T.
A.6.	Cada servidor (nodo) debe tener fuentes de alimentación redundantes.
A.7.	Cada servidor(nodo) debe incluir los accesorios necesarios para su conectividad a los switches de conectividad front-end (acceso de usuarios). Para esto, se requieren los siguientes accesorios: mínimo cuatro (4) patch cords de fibra óptica LC-LC de 3M; mínimo cuatro (4) Transceivers SFP28 (10Gbps); y un (1) patch Cord de cobre (UTP o STP) CAT6a de 3M por cada servidor.
A.8.	El cluster debe proveer una capacidad mínima de 560 Cores, 9 TB de Memoria y 200 TB de capacidad efectiva de almacenamiento (sin aplicar técnicas de optimización de almacenamiento)

A.9.	Se deben proveer dos (2) clusters, primario y secundario de características similares.
A.10.	Debe ser una plataforma hiperconvergente con almacenamiento definido por software, sin dependencias de infraestructura SAN tradicional y conceptos como LUNs o RAID
A.11.	Debe soportar escalabilidad horizontal, permitiendo la adición de nodos sin afectar la operación del sistema.
A.12.	Debe permitir el crecimiento asimétrico, es decir, agregar nodos con diferentes capacidades de CPU, RAM y almacenamiento.
A.13.	Distribución automática de datos en todos los nodos del clúster para maximizar la eficiencia del almacenamiento.
A.14.	La solución debe incluir funcionalidades de Calidad de Servicio para el acceso al almacenamiento (Storage QoS), que permita al administrador limitar la cantidad de IOPS y el rendimiento de las VMs.
A.15.	La solución ofertada de proveer una administración centralizada para la gestión de máquinas virtuales, almacenamiento redes y servicios suministrados por la plataforma.
A.16.	Debe proveer el balanceo automático y migración en caliente de las VMs.
A.17.	Debe suministrar una operación de red basada en un switch virtual distribuido con soporte para segmentación de redes y VLANs (802.1Q).
A.18.	Debe soportar compresión y deduplicación en línea sin impacto significativo en el rendimiento.
A.19.	Debe proveer microsegmentación de red para restringir el tráfico entre cargas de trabajo virtualizadas (VMs)
A.20.	Debe permitir la orquestación la recuperación ante desastres con secuencias de arranque y automatización.
A.21.	Debe proveer la capacidad de replicación síncrona (RPO=0) y/o asíncrona (con RPO configurable).
A.22.	Debe proveer la protección de snapshots contra eliminación accidental

	o ataques de ransomware.
A.23.	Debe tener la capacidad de monitoreo proactivo con detección de fallos y notificaciones automáticas.
A.24.	Requiere proveer la capacidad de actualizaciones sin downtime para software y firmware de la plataforma de hardware sobre la cual se implementa la solución.
A.25.	Debe tener la capacidad para realizar auditorías automatizadas para cumplimiento de normativas como HIPAA, PCI-DSS, CIS.
A.26.	La plataforma debe proveer hardening automático de la misma y configuración de seguridad sin intervención manual.
A.27.	La solución debe incluir de forma nativa una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un nodo de la solución, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema no debe incorporar elementos que hagan la función de testigo (witness, quorum o similar).
A.28.	Debe proveer capacidades de monitoreo proactivo con detección de fallos y notificaciones automáticas.
A.29.	Debe incluir capacidades nativas para la implementación y gestión de Kubernetes y aplicaciones cloud-native.
A.30.	Debe proporcionar un entorno optimizado para la ejecución de servicios de Kubernetes, incluyendo almacenamiento persistente para contenedores
A.31.	Debe permitir la creación y gestión de clústeres de Kubernetes mediante UI, CLI o YAML.
A.32.	Debe incluir capacidades de gestión del ciclo de vida (LCM) tanto de clústeres de Kubernetes, como de la infraestructura física del clúster, asegurando actualizaciones y mantenimiento sin interrupciones.
A.33.	Debe llevar a cabo la implementación de herramientas dentro del cluster de Kubernetes, para la gestión, monitoreo y servicios de dentro del cluster como:

	o Kubecost o Prometheus o Grafana o Gatekeeper o Reloader o Traefik o Kafka o Zookeeper o Fluentbit o Velero o Istio
A.34.	El proponente deberá entregar el diseño conceptual con la cantidad de servidores

Item	***Especificaciones Técnicas***
B	**<u>Infraestructura para SAFIRO (Sistema Administrativo Financiero)</u>** **Especificaciones Técnicas** Requerimientos mínimos de hardware para la plataforma
B.1.	Almacenamiento basado en NVMe para garantizar alto rendimiento y baja latencia.
B.2.	Cada servidor (nodo) ofertado debe ser certificado para la plataforma SAP HANA.
B.3.	Cada servidor (nodo) ofertado debe tener doble procesador, cada procesador con mínimo 48 núcleos y una frecuencia de reloj mínima de 2.4 GHz por núcleo.
B.4.	Cada servidor (nodo) deberá proporcionar al menos 4096 GB de memoria RAM instalada, en módulos de memoria de 128 GB.

B.5.	Cada servidor (nodo) debe proporcionar almacenamiento distribuido en discos SSD/NVMe con al menos 12 discos de 7.68TB.
B.6.	Cada servidor (nodo) debe ofrecer mínimo cuatro (4) tarjetas “dual” de dos (2) puertos SFP de 10/25 GbE,
B.7.	Cada servidor (nodo) debe tener fuentes de alimentación redundantes.
B.8.	Cada servidor (nodo) debe incluir los accesorios necesarios para su conectividad a los switches de conectividad front-end (acceso de usuarios). Para esto, se requieren los siguientes accesorios: mínimo 16 patch cords de fibra óptica LC-LC de 3M; mínimo 16 Transceivers SFP28; y un (1) patch Cord de cobre (UTP o STP) CAT6a de 3M por cada servidor.
B.9.	El cluster debe proveer una capacidad mínima de 480 Cores, 20 TB de Memoria y 150 TB de capacidad efectiva de almacenamiento (sin aplicar técnicas de optimización de almacenamiento)
B.10.	Se deben proveer dos (2) clusters, primario y secundario de características similares.
B.11.	Debe ser una plataforma hiperconvergente con almacenamiento definido por software, sin dependencias de infraestructura SAN tradicional y conceptos como LUNs o RAID
B.12.	Debe soportar escalabilidad horizontal, permitiendo la adición de nodos sin afectar la operación del sistema.
B.13.	Debe permitir el crecimiento asimétrico, es decir, agregar nodos con diferentes capacidades de CPU, RAM y almacenamiento.
B.14.	Distribución automática de datos en todos los nodos del clúster para maximizar la eficiencia del almacenamiento.
B.15.	La solución debe incluir funcionalidades de Calidad de Servicio para el acceso al almacenamiento (Storage QoS), que permita al administrador limitar la cantidad de IOPS y el rendimiento de

	las VMs.
B.16.	La solución ofertada de proveer una administración centralizada para la gestión de máquinas virtuales, almacenamiento redes y servicios suministrados por la plataforma.
B.17.	Debe proveer el balanceo automático y migración en caliente de las VMs.
B.18.	Debe suministrar una operación de red basada en un switch virtual distribuido con soporte para segmentación de redes y VLANs (802.1Q).
B.19	Debe soportar compresión y deduplicación en línea sin impacto significativo en el rendimiento.
B.20.	Debe tener la capacidad de monitoreo proactivo con detección de fallos y notificaciones automáticas.
	Requiere proveer la capacidad de actualizaciones sin downtime para software y firmware de la plataforma de hardware sobre la cual se implementa la solución.
B.21.	La plataforma debe proveer hardening automático de la misma y configuración de seguridad sin intervención manual.
B.22.	La solución debe incluir de forma nativa una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un nodo de la solución, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema no debe incorporar elementos que hagan la función de testigo (witness, quorum o similar).
B.23.	El proponente deberá entregar el diseño conceptual con la cantidad de servidores

Item	***Especificaciones Técnicas***

C	**A. <u>Infraestructura para Telemedicina</u>** **Especificaciones Técnicas** Requerimientos mínimos de hardware para la plataforma
C.1	Todo el almacenamiento debe estar basado en NVMe para garantizar alto rendimiento y baja latencia.
C.2.	Cada servidor (nodo) ofertado debe tener doble procesador, cada procesador con mínimo 16 núcleos y una frecuencia de reloj mínima de 2.0 GHz por núcleo.
C.3	Cada servidor (nodo) deberá proporcionar al menos 512 GB de memoria RAM instalada, en módulos de memoria de 32 GB.
C.4	Cada servidor (nodo) debe proporcionar almacenamiento distribuido en discos NVMe con al menos 20 discos de 15.36 TB.
C.5	Cada servidor (nodo) debe ofrecer mínimo dos (2) tarjetas “dual” de dos (2) puertos SFP de 10/25 GbE, y una (1) tarjeta “dual” de dos (2) puertos GbE BASE-T.
C.6	Cada servidor (nodo) debe tener fuentes de alimentación redundantes.
C.7	Cada servidor (nodo) debe incluir los accesorios necesarios para su conectividad a los switches de conectividad front-end (acceso de usuarios). Para esto, se requieren los siguientes accesorios: mínimo 4 patch cords de fibra óptica LC-LC de 3M; mínimo 4 Transceivers SFP28; y un (1) patch Cord de cobre (UTP o STP) CAT6a de 3M por cada servidor.
C.8	El cluster debe proveer una capacidad mínima de 380 Cores, 6 TB de Memoria y 1400 TB de capacidad efectiva de almacenamiento (sin aplicar técnicas de optimización de almacenamiento)

C.9	Se deben proveer dos (2) clusters, primario y secundario de características similares.
C.10	Para la implementación del servicio de balanceador se debe proveer un cluster de mínimo un nodo implementado sobre la misma tecnología de hiperconvergencia suministrada, con las siguientes características: o Un procesador físico de 8 núcleos o Memoria de 192 GB en módulos de 32 GB o Dos (2) discos NVMe de 7.68 TB o Dos (2) tarjetas “dual” de dos (2) puertos SFP de 10/25 GbE, y una (1) tarjeta “dual” de dos (2) puertos GbE BASE-T.
C.11	Debe ser una plataforma hiperconvergente con almacenamiento definido por software, sin dependencias de infraestructura SAN tradicional y conceptos como LUNs o RAID
C.12	Debe soportar escalabilidad horizontal, permitiendo la adición de nodos sin afectar la operación del sistema.
C.13	Debe permitir el crecimiento asimétrico, es decir, agregar nodos con diferentes capacidades de CPU, RAM y almacenamiento.
C.14	Distribución automática de datos en todos los nodos del clúster para maximizar la eficiencia del almacenamiento.
C.15	La solución debe incluir funcionalidades de Calidad de Servicio para el acceso al almacenamiento (Storage QoS), que permita al administrador limitar la cantidad de IOPS y el rendimiento de las VMs.
C.16	La solución ofertada de proveer una administración centralizada para la gestión de máquinas virtuales, almacenamiento redes y servicios suministrados por la

	plataforma.
C.17	Debe proveer el balanceo automático y migración en caliente de las VMs.
C.18	Debe suministrar una operación de red basada en un switch virtual distribuido con soporte para segmentación de redes y VLANs (802.1Q).
C.10	Debe soportar compresión y deduplicación en línea sin impacto significativo en el rendimiento.
C.20	Debe tener la capacidad de monitoreo proactivo con detección de fallos y notificaciones automáticas.
C.21	Requiere proveer la capacidad de actualizaciones sin downtime para software y firmware de la plataforma de hardware sobre la cual se implementa la solución.
C.22	La plataforma debe proveer hardening automático de la misma y configuración de seguridad sin intervención manual.
C.23	La solución debe incluir de forma nativa una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un nodo de la solución, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema no debe incorporar elementos que hagan la función de testigo (witness, quorum o similar).
C.25	La solución debe incluir Servicios de Archivos nativos (CIFS/SMB/NFS) sin necesidad de hardware o software adicional y debe ser gestionada en la misma interfaz que el resto del sistema.
C.26	La solución debe admitir un enfoque de "inicio pequeño" con implementaciones desde 1 TiB, escalando hasta múltiples petabytes.
C.27	La escalabilidad debe admitir incrementos granulares de

	licencias de software en bloques de 1 TiB de capacidad utilizable
C.28	La solución debe permitir ejecutar máquinas virtuales de usuario en el mismo hardware que el servicio de archivos sin necesidad de licencias adicionales o productos de terceros.
C.29	La solución debe incluir Servicios de Almacenamiento de Objetos nativos (estrictamente compatibles con AWS S3) sin necesidad de hardware o software adicional y gestionados en la misma interfaz que el resto del sistema.
C.30	La solución debe incluir servicios de almacenamiento en bloque nativos que expongan recursos de almacenamiento directamente a sistemas operativos invitados virtualizados o hosts físicos (no hipervisores) utilizando el protocolo iSCSI sin necesidad de hardware o software adicional y gestionados en la misma interfaz que el resto del sistema.
C.31.	El proponente deberá entregar el diseño conceptual con la cantidad de servidores

Item	***Especificaciones Técnicas Y Normas***
D	**<u>Equipos de Comunicación para el soporte de las Infraestructuras</u>** **Especificaciones Técnicas** Requerimientos mínimos de hardware para los equipos de

	infraestructura de SIS, SIPE, SAFIRO y TELEMEDICINA.
D.1.	Cada Switch debe entregarse con 48 slot SFP+ 1G/10G, 4 slot para enlaces de 40/100 Gbps de tipo QSFP+/QSFP28.
D.2.	Solo deben ocupar 2 unidades entre los dos swtiches que estarán conectados en alta disponibilidad.
D.3	Soporte de apilamiento de hasta 8 unidades, comportándose como uno solo, administrable con una sola dirección IP y velocidad de stacking mínimo de 160Gbps.
D.4	Switch fabric de Mínimo de 1,92Tbps
D.5	Fordwarding Rate de Mínimo de 1309 Mpps
D.6	Soporte de VLANS 4K
D.7	QoS (Calidad de Servicio) o 8 colas de prioridad por puerto o clasificación de tráfico tipo wirespeed o QoS basado en políticas sobre VLAN, puerto, MAC o capacidad de remarcado extensivo o Taildrop para control de congestión de encolamiento o Marcado DiffServ y IPprecedence sobre capa 2, 3 y 4.
D.8.	ACL basado en cabeceras de capa 3, capa 4 y hardware ACL
D.9	Certificaciones de organismo de seguridad EN55032 class A, EN55024, EN61000-3-levels 2, EN60950-1, EN60825-1, AS/NZS, 60950, FCC class A, VCCI class A, UL60950-1, CAN/CSA-C22.2 No.60950-1-03, UL, cUL, EU RoHS compliant, China RoHS compliant.
D.10	Normas IEEE Standards: el equipo deberá soportar mínimo: o IEEE 802.3ab 1000BASE-T o IEEE 802.3ae 10 Gigabit Ethernet o IEEE 802.3ba 40 Gigabit Ethernet o IEEE 802.3z 1000BASE-X o IEEE 802.3bj 100GBASE-X

	o IEEE 802.3bz 2.5GBASE-T 5GBASE-T o IEEE 802.1ad Provider bridges (VLAN stacking, Q-in-Q) o IEEE 802.1Q Virtual LAN (VLAN) bridges o IEEE 802.1v VLAN classification by protocol and port o IEEE 802.3ac VLAN tagging o IEEE 802.1X authentication protocols (TLS, TTLS, PEAP and MD5) o IEEE 802.1X multi-supplicant authentication o IEEE 802.1X port-based network access control o IEEE 802.1p Priority tagging o IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
D.11	• Normas RFC Standards: el equipo deberá soportar mínimo: o RFC 894 Standard for the transmission of IP data grams over Ethernet networks o RFC 950 Internet standard subnetting procedure o RFC 951 Bootstrap Protocol (BootP) o RFC 1027 Proxy ARP o RFC 1035 DNS client o RFC 1042 Standard for the transmission of IP data grams over IEEE 802 networks o RFC 1071 Computing the Internet checksum o RFC 1122 Internet host requirements o RFC 1191 Path MTU discovery o RFC 1256 ICMP router discovery messages o RFC 1542 Clarifications and extensions for BootP o RFC 1591 Domain Name System (DNS) o RFC 1812 Requirements for IPv4 routers o RFC 1981 Path MTU discovery for IPv6 o RFC 2460 IPv6 specification o RFC 2464 Transmission of IPv6 packets over Ethernet networks

	o RFC 3484 Default address selection for IPv6 o RFC 3596 DNS extensions to support IPv6 o RFC 4007 IPv6 scoped address architecture o RFC 4193 Unique local IPv6 unicast addresses o RFC 4291 IPv6 addressing architecture o RFC 4443 Internet Control Message Protocol (ICMPv6) o RFC 4861 Neighbor discovery for IPv6 o RFC 2863 Interfaces group MIB o RFC 3176 sFlow: a method for monitoring traffic in switched and routed networks o RFC 4862 IPv6 Stateless Address Auto-Configuration (SLAAC) o RFC 5014 IPv6 socket API for source address selection o RFC 5095 Deprecation of type 0 routing headers in IPv6 o RFC 5175 IPv6 Router Advertisement (RA) flags option o RFC 1518 An architecture for IP address allocation with CIDR o RFC 1519 Classless Inter-Domain Routing (CIDR) o RFC 1212 Concise MIB definitions o RFC 1213 MIB for network management of TCP/IP-based Internets: MIB-II o RFC 1215 Convention for defining traps for use with the SNMP o RFC 1227 SNMP MUX protocol and MIB o RFC 1239 Standard MIB o RFC 1724 RIPv2 MIB extension o RFC 2578 Structure of Management Information v2 (SMIv2) o RFC 2579 Textual conventions for SMIv2 o RFC 3810 Multicast Listener Discovery v2 (MLDv2) for IPv6 o RFC 3956 Embedding the Rendezvous Point (RP) address in an IPv6 multicast address o RFC 2580 Conformance statements for SMIv2

	o RFC 2616 Hypertext Transfer Protocol - HTTP/1.1 o RFC 2821 Simple Mail Transfer Protocol (SMTP) o RFC 6105 IPv6 Router Advertisement (RA) guard o RFC 1155 Structure and identification of management information for TCP/IP based internets o RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions o RFC 2741 Agent extensibility (AgentX) protocol o RFC 2787 Definitions of managed objects for VRRP o RFC 2819 RMON MIB (groups 1,2,3 and 9) o RFC 3411 An architecture for describing SNMP management frameworks o RFC 3412 Message processing and dispatching for the SNMP o RFC 3415 View-based Access Control Model (VACM) for SNMP o RFC 2453 RIPv2 o RFC 5246 TLS v1.2 o RFC 854 Telnet protocol specification o RFC 2818 HTTP over TLS (“HTTPS”) o RFC 2865 RADIUS o RFC 2866 RADIUS accounting o RFC 2868 RADIUS attributes for tunnel protocol support o RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) profile o RFC 3546 Transport Layer Security (TLS) extensions o RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP) o RFC 3580 IEEE 802.1x RADIUS usage guidelines o RFC 3748 PPP Extensible Authentication Protocol (EAP) o RFC 3416 Version 2 of the protocol operations for the SNMP o RFC 3417 Transport mappings for the SNMP

	o RFC 3630 Traffic engineering extensions to OSPF o RFC 4552 Authentication/confidentiality for OSPFv3 o RFC 3418 MIB for SNMP o RFC 4022 SNMPv2 MIB for TCP using SMIv2 o RFC 4113 SNMPv2 MIB for UDP using SMIv2 o RFC 1112 Host extensions for IP multicasting (IGMPv1) o RFC 2236 Internet Group Management Protocol v2 (IGMPv2) o RFC 2710 Multicast Listener Discovery (MLD) for IPv6 o RFC 2715 Interoperability rules for multicast routing protocols o RFC 2597 DiffServ Assured Forwarding (AF) o RFC 3246 DiffServ Expedited Forwarding (EF) o RFC 3973 PIM Dense Mode (DM) o RFC 4541 IGMP and MLD snooping switches o RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): protocol specification (revised) o RFC 4604 Using IGMPv3 and MLDv2 for sourcespecific multicast o RFC 1246 Experience with the OSPF protocol o RFC 1370 Applicability statement for OSPF o RFC 1765 OSPF database overflow o RFC 2370 OSPF opaque LSA option o RFC 2740 OSPFv3 for IPv6 o RFC 3101 OSPF Not-So-Stubby Area (NSSA) option o RFC 3509 Alternative implementations of OSPF area border routers o RFC 3623 Graceful OSPF restart o RFC 5329 Traffic engineering extensions to OSPFv3 o RFC 2211 Specification of the controlled-load network

Item	*Especificaciones Técnicas Y Normas*
E.	**Equipos de Comunicación para el soporte de las Infraestructuras** **Especificaciones Técnicas**
E.1	• Normas RFC Standards: el equipo deberá soportar mínimo: o RFC 894 Standard for the transmission of IP data grams over Ethernet networks o RFC 950 Internet standard subnetting procedure o RFC 951 Bootstrap Protocol (BootP) o RFC 1027 Proxy ARP o RFC 1035 DNS client o RFC 1042 Standard for the transmission of IP data grams over IEEE 802 networks o RFC 1071 Computing the Internet checksum o RFC 1122 Internet host requirements o RFC 1191 Path MTU discovery o RFC 1256 ICMP router discovery messages o RFC 1542 Clarifications and extensions for BootP o RFC 1591 Domain Name System (DNS) o RFC 1812 Requirements for IPv4 routers o RFC 1981 Path MTU discovery for IPv6 o RFC 2460 IPv6 specification o RFC 2464 Transmission of IPv6 packets over Ethernet networks o RFC 3484 Default address selection for IPv6 o RFC 3596 DNS extensions to support IPv6 o RFC 4007 IPv6 scoped address architecture o RFC 4193 Unique local IPv6 unicast addresses o RFC 4291 IPv6 addressing architecture

	o RFC 4443 Internet Control Message Protocol (ICMPv6) o RFC 4861 Neighbor discovery for IPv6 o RFC 2863 Interfaces group MIB o RFC 3176 sFlow: a method for monitoring traffic in switched and routed networks o RFC 4862 IPv6 Stateless Address Auto-Configuration (SLAAC) o RFC 5014 IPv6 socket API for source address selection o RFC 5095 Deprecation of type 0 routing headers in IPv6 o RFC 5175 IPv6 Router Advertisement (RA) flags option o RFC 1518 An architecture for IP address allocation with CIDR o RFC 1519 Classless Inter-Domain Routing (CIDR) o RFC 1212 Concise MIB definitions o RFC 1213 MIB for network management of TCP/IP-based Internets: MIB-II o RFC 1215 Convention for defining traps for use with the SNMP o RFC 1227 SNMP MUX protocol and MIB o RFC 1239 Standard MIB o RFC 1724 RIPv2 MIB extension o RFC 2578 Structure of Management Information v2 (SMIv2) o RFC 2579 Textual conventions for SMIv2 o RFC 3810 Multicast Listener Discovery v2 (MLDv2) for IPv6 o RFC 3956 Embedding the Rendezvous Point (RP)

	address in an IPv6 multicast address o RFC 2580 Conformance statements for SMIv2 o RFC 2616 Hypertext Transfer Protocol - HTTP/1.1 o RFC 2821 Simple Mail Transfer Protocol (SMTP) o RFC 6105 IPv6 Router Advertisement (RA) guard o RFC 1155 Structure and identification of management information for TCP/IP based internets o RFC 2674 Definitions of managed objects for bridges with traffic classes, multicast filtering and VLAN extensions o RFC 2741 Agent extensibility (AgentX) protocol o RFC 2787 Definitions of managed objects for VRRP o RFC 2819 RMON MIB (groups 1,2,3 and 9) o RFC 3411 An architecture for describing SNMP management frameworks o RFC 3412 Message processing and dispatching for the SNMP o RFC 3415 View-based Access Control Model (VACM) for SNMP o RFC 2453 RIPv2 o RFC 5246 TLS v1.2 o RFC 854 Telnet protocol specification o RFC 2818 HTTP over TLS (“HTTPS”) o RFC 2865 RADIUS o RFC 2866 RADIUS accounting o RFC 2868 RADIUS attributes for tunnel protocol support o RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) profile o RFC 3546 Transport Layer Security (TLS) extensions o RFC 3579 RADIUS support for Extensible Authentication Protocol (EAP)

	o RFC 3580 IEEE 802.1x RADIUS usage guidelines o RFC 3748 PPP Extensible Authentication Protocol (EAP) o RFC 3416 Version 2 of the protocol operations for the SNMP o RFC 3417 Transport mappings for the SNMP o RFC 3630 Traffic engineering extensions to OSPF o RFC 4552 Authentication/confidentiality for OSPFv3 o RFC 3418 MIB for SNMP o RFC 4022 SNMPv2 MIB for TCP using SMIv2 o RFC 4113 SNMPv2 MIB for UDP using SMIv2 o RFC 1112 Host extensions for IP multicasting (IGMPv1) o RFC 2236 Internet Group Management Protocol v2 (IGMPv2) o RFC 2710 Multicast Listener Discovery (MLD) for IPv6 o RFC 2715 Interoperability rules for multicast routing protocols o RFC 2597 DiffServ Assured Forwarding (AF) o RFC 3246 DiffServ Expedited Forwarding (EF) o RFC 3973 PIM Dense Mode (DM) o RFC 4541 IGMP and MLD snooping switches o RFC 4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): protocol specification (revised) o RFC 4604 Using IGMPv3 and MLDv2 for sourcespecific multicast o RFC 1246 Experience with the OSPF protocol o RFC 1370 Applicability statement for OSPF o RFC 1765 OSPF database overflow o RFC 2370 OSPF opaque LSA option o RFC 2740 OSPFv3 for IPv6

	o RFC 3101 OSPF Not-So-Stubby Area (NSSA) option o RFC 3509 Alternative implementations of OSPF area border routers o RFC 3623 Graceful OSPF restart o RFC 5329 Traffic engineering extensions to OSPFv3 o RFC 2211 Specification of the controlled-load network
E.2.	• Resiliency o RFC 5798 Virtual Router Redundancy Protocol version 3 (VRRPv3) for IPv4 and IPv6 o RFC 1058 Routing Information Protocol (RIP) o RFC 2080 RIPng for IPv6 o RFC 2081 RIPng protocol applicability statement o RFC 2082 RIP-2 MD5 authentication o RFC 4251 Secure Shell (SSHv2) protocol architecture o RFC 4252 Secure Shell (SSHv2) authentication protocol o RFC 4253 Secure Shell (SSHv2) transport layer protocol o RFC 4254 Secure Shell (SSHv2) connection protocol o RFC 855 Telnet option specifications o RFC 857 Telnet echo option o RFC 858 Telnet suppress go ahead option o RFC 1091 Telnet terminal-type option o RFC 2822 Internet message format o RFC 3046 DHCP relay agent information option (DHCP option 82) o RFC 3306 Unicast-prefix-based IPv6 multicast addresses o RFC 3376 IGMPv3 o RFC 2474 DiffServ precedence for eight queues/port o RFC 2697 A single-rate three-color marker

	o RFC 2698 A two-rate three-color marker o RFC 2475 DiffServ architecture o RFC 1350 Trivial File Transfer Protocol (TFTP) o RFC 1985 SMTP service extension o RFC 2049 MIME o RFC 2131 DHCPv4 (server, relay and client) o RFC 2132 DHCP options and BootP vendor extensions o RFC 3315 DHCPv6 (server, relay and client) o RFC 3633 IPv6 prefix options for DHCPv6 o RFC 3646 DNS configuration options for DHCPv6 o RFC 3993 Subscriber-ID suboption for DHCP relay agent option o RFC 4330 Simple Network Time Protocol (SNTP) version 4 o RFC 5905 Network Time Protocol (NTP) version 4
E.3	• Otros: o ITU-T G.8032 Ethernet ring protection switching o Certificación FIPS140-2 y IPv6 Ready o Bootstrap Router (BSR) mechanism for PIM-SM o IGMP/MLD multicast forwarding (IGMP/MLD proxy) o TACACS+ Accounting, Authentication, Authorization (AAA) o Generic VLAN Registration Protocol (GVRP) o VXLAN o MLD snooping (MLDv1 and v2) o PIM-SM and SSM for IPv6 o OSPF link-local signaling o OSPF MD5 authentication o SSH remote login o SSLv2 and SSLv3

	o Out-of-band LSDB resync o IGMP query solicitation o IGMP snooping (IGMPv1, v2 and v3) o IGMP snooping fast-leave o AES (ECB, CBC, CFB and OFB Modes) o 3DES (ECB, CBC, CFB and OFB Modes) o CCM o CMAC o GCM o XTS o DSA o ECDSA o RSA o SHA-1 o SHA-2 (SHA-224, SHA-256, SHA-384. SHA-512) o HMAC (SHA-1, SHA-2(224, 256, 384, 512)
E.4	Potencia de consumo de 267W máximo
E.5	Hasta 96K MAC address
E.6	Mínimo 4 GB DDR SDRAM.
E.7	DDM (Digital Diagnostic Monitoring) para fibra óptica.
E.8	Automáticamente detecte flaps y apague el puerto.
E.9	Ping polling y traceroute para IPV4 e IPV6.
E.10.	SNMPv6, TELNET v6, SSHv6.
E.11	Que pueda limitar el ancho de banda del puerto a 64 kbps.
E.12	QoS basado en Políticas sobre VLAN puerto y/o MAC.
E.13	Clasificación general de paquetes.
E.14	El switch debe soportar a futuro crecimiento de hasta 8 puertos de 40Gbps.
E.15	El switch debe soportar a futuro crecimiento de hasta 5 puertos de 100G.
E.16	El switch debe soportar a futuro crecimiento de hasta 36 slot

	SFP+ 1G/10G
E.17	El switch debe soportar NAC con características esenciales de seguridad para endpoint garantizando la protección contra amenazas de malware interno de la LAN, evitando la propagación.
E.18	El switch core, debe estar en la capacidad de hacerse copias de seguridad automáticamente, sin necesidad de intervención humana, las copias de seguridad deben hacerse al firmware y a la configuración.
E.19	El switch core debe estar en la capacidad de hacerse actualizaciones de software automáticamente, sin necesidad de intervención humana.
E.20	El switch debe estar en la capacidad de administrar vía CLI otros switches de la misma marca de fabricante que estén dentro de la red de datos. De manera virtual incluirlos dentro de su plataforma y poderlos gestionar, administrar y automatizar. Bajo su plataforma poder guardar copias de seguridad de configuraciones y firmware.
E.21	El switch de core debe estar en la capacidad de evitar ataques MITM monitoreando la intensidad del haz de luz del enlace en la fibra óptica. Si se detecta una intrusión, el enlace se puede apagar automáticamente y debe enviar una alerta SNMP
E.22	Al menos dos (2) mecanismos adicionales al STP, RSTP y MSTP para detectar puertos involucrados en loop y poder tomar acciones de forma predeterminada por comandos sobre dichos puertos (mecanismos diferentes a los protocolos basados en Spanning Tree).
E.23	El switch core debe estar en la capacidad de identificar si la misma Mac Address es aprendida por más de un puerto y tomar acciones de forma predeterminada y automática como:

	apagar el puerto, deshabilitar el puerto para que no exista tráfico, deshabilitar la LAN en la que la Mac se está aprendiendo.
E.24	Capacidad de formar anillos y recuperarse ante la falla de un enlace del anillo máximo en 50 milisegundos.
E.25	El switch debe estar en la capacidad de evitar bucles que se presenten en la red de datos, se debe contar con thrash limiting para detectarlos antes que se produzca una tormenta de broadcast e interrumpa los servicios de red.
E.26	Compatibilidad con PVST+.
E27	Soporte Modbus.
E.28	Multicast Source Discovery Protocol (MSDP)
E.29	Capacidad de formar stacking con distancia de al menos 1500 metros utilizando los puertos SFP+ y QSFP+
E.30	UDLD
E.31	Mecanismo que apoye el ahorro de energía sobre fuentes que no se usen al máximo o sobre leds de los puertos mientras no se requieran, aunque tengan enlaces activos.
E.32	Capacidad de realizar scripting en CLI.
E.33	Debe poder operar OSPF, BGP4, BGP4+, PIM-DM, PIM-SM, PIM4-SM/DM, PIM6-SM/SSM, Q-in-Q, RIPng.
E.34	Debe soportar el protocolo G.8032 para anillos.
E.35	Secure copy (SCP)
E.36	Triple-autenticacion: basada en MAC, basada en web y por IEEE 802.1X
E.37	Soporte para TACACS+ commands
E.38	ACL basadas en cabeceras de capa 3 y 4.
E.39	ACL de capa 2 para IPv6.
E.40	Soporte para jumbo frames de mínimo 9KB
E.41	Que posea puerto USB para poder cargar release de

	software, configuraciones o backups.
E.42	Soporte para OpenFLow versión 1.3 o superior
E.43	Buffer de memoria para paquetes de al menos 16MB.
E.44	El equipo debe contar con al menos 2 fuentes de poder, removibles en caliente. Se debe entregar con redundancia en fuente de poder.
E.45	Debe soportar VRF Lite.
E.46	Debe tener administración por CLI y Web.
E.47	La solución se debe entregar configurada, empalmada y en marcha.
E.48	**Garantías:** el equipo debe entregarse con tres años de garantía incluido las piezas.

Item	***Especificaciones Técnicas Y Normas***
F	Prueba de interconexión de los diferentes componentes de la solución
	• Pruebas Funcionales: se deberá probar la funcionalidad de cada componente instalado. • Pruebas de compatibilidad: comprobar la comunicación continua de cada componente contenido en la solución implantada por el proveedor. • Pruebas integrales: comprobar la comunicación entre los componentes para cada Data Center. • Pruebas de velocidad: se deberá medir que las velocidades instaladas son acordes a lo requerido en el presente documento. • Pruebas de latencia: se realizarán pruebas de cargas de trabajo de lectura masiva en las bases de datos y se

	verificará la latencia. • Prueba de alta disponibilidad: se realizará una desconexión controlada de los equipos instalados, las cuales se realizarán en clústeres y entre Data Centers. • Pruebas de interrupción eléctrica masiva. • Simulación de eventos y evaluación de tiempos de respuesta (medición de efectividad del SLA).
	Inspecciones y Pruebas: El Proveedor realizará una prueba de alta disponibilidad con al menos el 10% de los servidores que contenga la nueva infraestructura tecnológica del CSS para verificar la accesibilidad de los sistemas en caso de fallo físico. Este proceso será supervisado por la Dirección de Informática (DNI) del CSS. La DNI realizará adicionalmente, pruebas parciales de funcionalidad de la solución tecnológica implantada por el proveedor, para certificar su correcto funcionamiento. Las pruebas deberán ser realizadas por el proveedor y aceptadas por el CSS. • Sera responsabilidad del proveedor realizar las siguientes actividades: Inspecciones físicas • Se verificará la instalación física de la solución ofertada por el proveedor versus el diseño entregado, para garantizar que al término del proceso de instalación, haya consistencia entre la documentación física y el equipo recibido. • Se verificará que cada equipo y cable utilizado haya sido identificado según nomenclatura provista por el CSS. Es requerido que el proveedor cumpla con la normativa TIA/EIA 606-A y ANSI/UL 969, en referencia al etiquetado de cables.

Item	*Especificaciones Técnicas Y Normas*
G	**Servicios de Soporte de la Plataforma.** La solución ofertada debe tener las siguientes características
G.1	Contar con un software residente en el clúster que permita diagnosticar el estado de salud del mismo y validar configuraciones recomendadas por el fabricante
G.2	Ejecutar de manera continua y proactiva múltiples verificaciones para la detección de problemas
G.3	Tomar acciones correctivas según la naturaleza del problema identificado.
G.4	Generar alertas o, en caso necesario, crear automáticamente casos de soporte con el fabricante.
G.5	Poder ejecutarse mientras los nodos individuales estén en funcionamiento, independientemente del estado del clúster.
G.6	Permitir la configuración de la frecuencia de ejecución de las verificaciones del clúster.
G.7	Contar con la capacidad de enviar por correo electrónico los resultados de dichas verificaciones a los usuarios designados.
G.8	Integrarse con la infraestructura de configuración de alertas, permitiendo el envío automático de información de alertas tanto al soporte técnico del fabricante como a otros destinatarios configurados.
G.9	Obtener información detallada del hardware del clúster o de un nodo individual,
G.10	Debe proveer un servicio de soporte proactivo y diagnóstico predictivo

G.11	Este servicio debe incorporar tecnología que permita la transmisión segura de datos de diagnóstico a una plataforma centralizada para su análisis
G.12	El servicio de soporte proactivo y diagnóstico predictivo debe habilitar flujos de trabajo automatizados de soporte, basados en un enfoque predictivo y contextual.
G.13	El servicio debe ayudar a mejorar la disponibilidad y estabilidad del sistema mediante capacidades avanzadas de monitoreo y análisis.
G.14	El servicio debe garantizar la privacidad y seguridad de los datos, asegurando que no se recopile ni transmita información específica de máquinas virtuales, datos de usuario, metadatos o información personal identificable, como credenciales de administrador.
G.15	El servicio debe implementar flujos de trabajo automatizados que abran casos de soporte cuando se detecten problemas críticos, como fallos de DIMM o discos, y recojan solo los registros relevantes del período correcto.

Item	***Especificaciones Técnicas Y Normas***
H	**Personal Calificado**
H.1.	(1) Jefe de Proyecto con más de 10 años de experiencia demostrables en trabajos similares en entornos críticos corporativos. Certificado PMI
H.2.	(1) Certified Project Management Associate IPMA Level D
	(1) Project Management Professional (PMP)
H.3.	(1) ITIL Foundation Examination
H.4.	(1) Scrum Fundamentals Certified

H.5.	(1) Scrum Master Certified
H.6.	(1) Veeam Certified Engineer v9 (VMCE)
H.7.	(1) Cisco Certified Network Associate
H.8.	

Item	***Especificaciones Técnicas***
I	**<u>Transferencia de Conocimiento</u>** El proveedor deberá suministrar capacitación y/o entrenamientos y/o workshops que faciliten la adopción de las tecnologías y/o productos implementados como parte del proyecto. Estas pueden ser impartidas de forma remota y/o suministrados en formato de cursos en línea. Estas capacitaciones deben cubrir aspectos como los siguientes:
I.1	Capacitación para la gestión y administración de la solución de Hiperconvergencia que incluya los siguientes temas: • Conceptos y arquitectura de la solución • Creación y gestión de máquinas virtuales, redes y almacenamiento. • Implementación de herramientas de monitoreo y diagnóstico para la infraestructura. • Procedimientos para mantener y actualizar la infraestructura, asegurando alta disponibilidad y rendimiento.
I.2	Capacitación en Administración de Kubernetes, que cubra los siguientes temas clave: • Fundamentos de contenedores y orquestación con Kubernetes, incluyendo su arquitectura básica.

	• Estrategias para desplegar y administrar aplicaciones, configuraciones de red y almacenamiento. • Creación, monitoreo y gestión de clústeres, con enfoque en alta disponibilidad y recuperación ante desastres. • Implementación de escalabilidad automática y estrategias de seguridad en los clústeres. • Procedimientos de mantenimiento, gestión de versiones y optimización de rendimiento. • Uso de herramientas para monitoreo, diagnóstico y resolución de problemas en Kubernetes.
I.3	Un Workshop enfocado en el manejo de los servicios de almacenamiento ofrecidos por la solución donde se cubran aspectos como: • Descripción general de la arquitectura de almacenamiento. • Gestión del almacenamiento. • Recuperación / Protección. • Resolución de problemas • Migración

Item	***TÉRMINOS Y CONDICIONES***
J.1	**Solvencia** El proponente deberá aportar una (1) Declaración Juramentada donde se refleje que se cuenta con: o **Al menos Ocho (8) Cifras Bajas**, ya sea en cuentas de ahorros, en cuenta corriente o en líneas de créditos, Certificados de Depósitos a Termino, Fideicomisos o la suma de ellas mismas que demuestren la

	liquides y solvencia de la empresa o persona natural. ○ **Indice de Liquidez, el cual debe ser mayor a 1.0**: Este índice se calcula con los datos mostrados en los estados financieros de la empresa correspondiente de los años 2022 y 2023, debidamente auditados, legalizados y presentados por el proponente de la siguiente manera: I.L. = Activos Corrientes / Pasivos Corrientes ○ **Nivel de Endeudamiento, debe ser menor de 0.82:** Este se calculará con los datos mostrados en los estados financieros de la empresa correspondiente de los años 2022 y 2023, debidamente auditados, legalizados y presentados por el proponente de la siguiente manera: N.E. = Total de Pasivos / Total de Activos ○ El proponente deberá aportar los Estados Financieros completos correspondientes a los años 2022 y 2023, debidamente notariados, los cuales deben haber sido auditados y/o certificados por una firma de auditoria o Contador Público Autorizado en la República de Panamá (CPA). Los estados financieros deberán ser presentados bajo las Normas lnternacionales de Contabilidad (NIC),
J.2	**Experiencia del Proveedor** **El Proponente deberá demostrar su experiencia en la Administración de Plataformas de Infraestructura de servidores. Deberá aportar tres (3) cartas de referencias propias o a través de su subcontratista.**
J.3	**Experiencia del Proveedor** **El Proponente deberá demostrar su experiencia en implementación, manejo y/o soporte de sistemas similares a los que se implementarán en esta solución. Deberá aportar dos (2) cartas de**

	referencias propias o a través de su subcontratista. **Nota: Se podrá utilizar un solo proyecto que evidencie dichas experiencias solicitadas.**
J.5	Experiencia o El proponente deberá demostrar por medio de sus Aviso Operación o Registro Público que cuenta con más de ocho (8) años en el mercado, con el fin de garantizar un óptimo servicio. o El proponente deberá presentar una declaración jurada que indique que cuenta con Diez (10) años o más de experiencia prestando servicios de datacenter, plataformas de virtualización para otras entidades del Estado. o El proponente deberá presentar una declaración jurada que indique que cuenta con Cinco (5) años o más de experiencia prestando servicios de datacenter, plataformas de virtualización para otras entidades del Estado.