BASES
EN VIAS DE REGULARIZACIÓN LA CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
CAUSAL "SITUACION DE EMERGENCIA"
EN MARCO DEL DECRETO SUPREMO N° 199-2023-EF

CONTRATACIÓN
"MEJORAMIENTO DE LA PLATAFORMA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN PARA LA GESTIÓN DEL RIESGO DE DESASTRES (SIGRID) ANTE LA OCURRENCIA DE INUNDACIONES Y MOVIMIENTOS EN MASA COMO CONSECUENCIA DEL PROBABLE FENÓMENO EL NIÑO 2023-2024"

CENEPRED

Firmado digitalmente por:
ALVAREZ RODRIGUEZ ARTURO
ORLANDO FIR 09163639 hard
Motivo: Soy el autor del
documento
Fecha: 02/04/2024 16:29:37-0500

DEBER DE COLABORACIÓN

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista, deben conducir su actuación conforme a los principios previstos en la Ley de Contrataciones del Estado.

En este contexto, se encuentran obligados a prestar su colaboración al OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI, en todo momento según corresponda a sus competencias, a fin de comunicar presuntos casos de fraude, colusión y corrupción por parte de los funcionarios y servidores de la Entidad, así como los proveedores y demás actores que participan en el proceso de contratación.

De igual forma, deben poner en conocimiento del OSCE y a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI los indicios de conductas anticompetitivas que se presenten durante el proceso de contratación, en los términos del Decreto Legislativo N° 1034, "Ley de Represión de Conductas Anticompetitivas", o norma que la sustituya, así como las demás normas de la materia.

La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir al OSCE o a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información referida a las contrataciones del Estado que sea requerida, prestar testimonio o absolución de posiciones que se requieran, entre otras formas de colaboración.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

(EN ESTA SECCIÓN LA ENTIDAD DEBERÁ COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO A LAS INSTRUCCIONES INDICADAS)

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	CENTRO NACIONAL DE ESTIMACIÓN, PREVENCIÓN Y REDUCCIÓN DEL RIESGO DE DESASTRES – CENEPRED
RUC Nº	:	2054389755
Domicilio legal	:	AV. DEL PARQUE NORTE N° 313-319 URB. CORPAC, SAN ISIDRO - LIMA
Teléfono:	:	(511)201-3550
Correo electrónico:	:	azapata@cenepred.gob.pe; aalvarez@cenepred.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la Contratación Directa para el "**Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno el niño 2023-2024**", en vía de regularización por la causal "Situación de emergencia derivada de situaciones que supongan grave peligro de la ocurrencia de acontecimientos catastróficos" en el Marco del Decreto Supremo N° 199-2023-EF, de fecha 11 de setiembre de 2023.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Memorándum N° 00195-2024-CENEPRED/OA de fecha 12 de marzo de 2024, el Formato 02 "Solicitud y Aprobación del Expediente de Contratación".

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios AF-2023

1.5. SISTEMA DE CONTRATACIÓN

El presente procedimiento se rige por el sistema de **A SUMA ALZADA**, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. MODALIDAD DE EJECUCIÓN

MODALIDAD LLAVE EN MANO PREVISTA EN EL EXPEDIENTE DE CONTRATACIÓN.

1.7. DISTRIBUCIÓN DE LA BUENA PRO

NO APLICA.

1.8. ALCANCES DEL REQUERIMIENTO

El alcance de la prestación está definido en el Capítulo III de la presente sección de las bases.

1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán en el plazo de acuerdo a lo señalado en las Especificaciones Técnicas y en concordancia con lo establecido en el expediente de contratación.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/9.70 (Nueve con 70/100 Soles) en Caja de la Entidad, sito Av. Del Parque Norte N° 313-319, Urb. Corpac, San Isidro, Provincia y Departamento de Lima, y recabar las copias en Logística del CENEPRED.

1.11. BASE LEGAL

- Decreto Legislativo N° 1440 – Decreto Legislativo del Sistema Nacional de Presupuesto Público
- Ley Nº 31638 Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley Nº 31639 Ley de Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2023.
- Decreto Supremo N° 082-2019-EF que aprueba el TUO de la Ley N° 30225 – Ley de Contrataciones del Estado.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado, modificado por Decreto Supremo N° 377-2019-EF t Decreto Supremo N° 168-2020-EF.
- Decreto Supremo N° 199-2023-EF, autoriza una transferencia de partidas en el Presupuesto del Sector Público para el Año Fiscal 2023 hasta por la suma de S/17’943,216.00 Soles, a favor del CENEPRED el monto de S/14’469,280 Soles y del Instituto Geográfico Nacional (IGN) el monto de S/3’473,936.00 Soles.
- Decretos Supremos N° 072-2023-PCM, 089-2023-PCM y 110-2023-PCM, mediante los cuales declara y renueva el Estado Emergencia en 18 departamento del país por el peligro inminente ante intensas precipitaciones pluviales (periodo 2023-2024) y posible Fenómeno El Niño.
- Comunicado N° 013-2023-OSCE: Utilización de la Contratación Directa para acciones de prevención.
- Directiva, Pronunciamientos y Opiniones del OSCE.
- Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Ley N° 27806 – Ley de Transparencia y de Acceso a la Información Pública.
- Código Civil.

Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

Según el cronograma de la ficha de selección de la convocatoria publicada en el SEACE.

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos[1], la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. **(Anexo Nº 1)**

b) Documento que acredite la representación de quien suscribe la oferta.

En caso de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto.

En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda.

En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo Nº 2)**

d) Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. **(Anexo Nº 3)**

e) Declaración jurada de plazo de entrega. **(Anexo Nº 4)**[2]

f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. (Anexo Nº 5)

g) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el Anexo Nº 6.

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales. Los precios unitarios pueden ser expresados con más de dos (2) decimales.

2.2.1.2. Documentos para acreditar los requisitos de calificación

Incorporar en la oferta los documentos que acreditan los “Requisitos de Calificación” que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

---

[1] La omisión del índice no determina la no admisión de la oferta.

[2] En caso de considerar como factor de evaluación la mejora del plazo de entrega, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

a) Garantía de pago por Adelanto contra la presentación de Carta Fianza por el 100%. **CARTA FIANZA**
b) Garantía de fiel cumplimiento del contrato. **CARTA FIANZA**
c) Garantía de fiel cumplimiento por prestaciones accesorias, **CARTA FIANZA.**
d) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
e) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
f) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
g) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.
h) Domicilio para efectos de la notificación durante la ejecución del contrato.
i) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [3] (Anexo Nº 11).
j) Detalle de los precios unitarios del precio ofertado[4].

Importante
• *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".* .

Importante
• *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.* • *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[5].*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en forma física en Mesa de Partes del CENEPRED,

[3] En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

[4] Incluir solo en caso de la contratación bajo el sistema a suma alzada.

[5] Según lo previsto en la Opinión N° 009-2016/DTN.

sito en Av. Del Parque Norte N° 313-319, Urb. Corpac, San Isidro o en forma virtual http://cenepred.gob.pe/web/mesa-de-partes-virtual/, https://facilita.gob.pe/t/1265 o correo electrónico mesadepartes@cenepred.gob.pe, en el horario de atención de lunes a viernes: 08:30 a.m. a 5:30 p.m.

2.5. FORMA DE PAGO

PAGO ADELANTADO:

La Entidad realizó el pago de la contraprestación pactada a favor del contratista en **PAGO ÚNICO EN FUNCIÓN AL MONTO DEL CONTRATO ORIGINAL, PREVIO OTORGAMIENTO DE UNA GARANTÍA POR EL MISMO MONTO DEL PAGO**, (numeral 153.1 del artículo 153 del RLCE).

La Oficina de Administración a través de su Especialista en Tesorería o la que haga sus veces, otorgó la conformidad a la GARANTIA presentada por el contratista para tal fin.

La garantía presentada por el contratista tuvo una vigencia de tres (3) meses. Una garantía de Fiel Cumplimiento por el 10% del monto total del contrato, siendo renovado por un plazo idéntico, la misma está comprendida durante la ejecución de la prestación (numeral 153.2 del artículo 153 del RLCE). Asimismo, presenta una garantía de fiel cumplimiento por prestaciones accesorias, renovables anualmente por 36 meses.

La garantía cumple las características y condiciones que la normativa ha contemplado, de modo que la Entidad pueda ejecutarla en caso de incumplimiento del proveedor.

CAPÍTULO III
REQUERIMIENTO

Importante
De conformidad con el numeral 29.8 del artículo 29 del Reglamento, el área usuaria es responsable de la adecuada formulación del requerimiento, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

3.1. ESPECIFICACIONES TÉCNICAS

(SIGUIENTE PAGINA)

MEJORAMIENTO DE LA PLATAFORMA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN PARA LA GESTIÓN DEL RIESGO DE DESASTRES (SIGRID) ANTE LA OCURRENCIA DE INUNDACIONES Y MOVIMIENTOS EN MASA COMO CONSECUENCIA DEL PROBABLE FENÓMENO EL NIÑO 2023-2024.

ESPECIFICACIONES TECNICAS

Unidad Orgánica:	Dirección de Gestión de Procesos – Subdirección de Gestión de Información
Actividad del POI:	Actividad 5005579, Acceso a la información y operatividad del sistema de información en gestión del riesgo de desastres.
Denominación de la Contratación:	Mejoramiento de la plataforma tecnológica del Sistema de Información para la Gestión del Riesgo de Desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable Fenómeno El Niño 2023-2024.

I. FINALIDAD PÚBLICA

Que habiéndose autorizado una transferencia de partidas en el Marco de la Demanda Adicional solicitado al Ministerio de Economía para el Año Fiscal 2023 a favor de CENEPRED, mediante Decreto Supremo N° 199-2023-EF publicado en el diario Oficial El Peruano el 12.09.2023, para financiar acciones del Levantamiento de Información en las Zonas de Alto y Muy Alto Riesgo ante la Ocurrencia del Fenómeno El Niño, resulta necesario el mejoramiento de la plataforma tecnológica del Sistema de Información para la Gestión del Riesgo de Desastres (SIGRID), mediante la implementación de una solución tecnológica integral de Data Center que permita ahorrar energía, espacio de almacenamiento, mejorar los niveles de la tolerancia a fallos, y mejorar la continuidad y protección de los datos críticos del SIGRID; garantizando así la eficiencia de energía, espacio, protección eléctrica y climatización n+1 que garantice la operatividad e integridad del servicio de información SIGRID.

II. OBJETIVO DE LA CONTRATACIÓN

Mejorar la infraestructura a nivel de disponibilidad, eficiencia de energía, espacio, protección eléctrica y climatización n+1 que garantice la operatividad e integridad del servicio de información SIGRID; asimismo, mejorar la seguridad y velocidad de procesamiento, tanto en la red interna como externa.

III. ALCANCES Y DESCRIPCIÓN:

Situación Actual

El Centro de Procesamiento de Datos se encuentra ubicado en el 2do piso del edificio destinada al centro de cómputo, el mismo tiene un diseño convencional con los componentes distribuidos e independientes, asimismo el ambiente no ha sido acondicionado para contener un centro de datos, como por ejemplo no cuenta con una hermetización de la sala adecuada.

En el Centro de Procesamiento de Datos de CENEPRED, el cual alberga el servidor principal donde se encuentra instalado el SIGRID, se encuentra ubicado en un ambiente con un sistema de aire acondicionado de confort que no controla humedad relativa, al no contar con esta característica se vuelve perjudicial para los equipos informáticos, ni tampoco está diseñado para un trabajo 24x7x365, asimismo no cuenta con un diseño y disposición de inyección de aire frio de acuerdo a las buenas prácticas, generando mayor consumo de energía, por ello es necesario realizar una modernización que asegure la continuidad de la prestación de servicios de los principales componentes de TI como los servidores, almacenamiento y equipos de comunicación.

El ambiente actual del centro de datos de la entidad no cuenta con las condiciones técnicas para alojar la infraestructura de tecnología que se requiere, asimismo no cuenta con infraestructura para la proyección de crecimiento que se requiere para consolidar los servicios.

El ambiente actual del centro de datos no cuenta con sensores de temperatura, humedad relativa y aniego.

El ambiente actual del centro de datos no cuenta con un sistema de control de acceso, punto importante para la seguridad perimetral e integridad de la información.

Asimismo, no cuenta con una protección de energía como un grupo electrógeno dimensionado para la nueva infraestructura.

Asimismo, la infraestructura de procesamiento de servidores tiene una antigüedad de más de 8 años los cuales son de generación 1, por otro lado, el almacenamiento actual cuenta con discos rotacionales mecánicos los cuales se encuentran más propensos a fallas.

Por otro lado, el parque de estaciones tiene falencias a nivel de operatividad de componentes y disponibilidad.

a. **CANTIDAD Y UNIDAD DE MEDIDA**

CENEPRED requiere contar con la siguiente infraestructura tecnológica:

Datacenter Principal

04 Gabinetes con sistema autocontenido
02 Sistemas de climatización en alta disponibilidad
02 Sistemas de UPS en alta disponibilidad
01 Sistema de control de acceso de reconocimiento facial
02 Sistema de detección y extinción de incendios rackeable
02 Cámara de video vigilancia
01 Sistema de monitoreo remoto

Datacenter Contingencia

03 Gabinetes con sistema autocontenido
02 Sistemas de climatización en alta disponibilidad
02 Sistemas de UPS en alta disponibilidad
01 Sistema de control de acceso de reconocimiento facial
01 Sistema de detección y extinción de incendios rackeable
01 Cámara de video vigilancia
01 Sistema de monitoreo remoto

Solución de Backup
01 Sistema de Backup
01 Software de Backup
01 Servidor para Backup

Servidores Convergentes
07 Servidores convergentes - 5 servidores para Sede Principal y 02 Sede Contingencia **(Absolución Nº 15)**
02 Storage (01 Sede Principal y 01 Sede Contingencia)

Networking
03 Switchs Core (02 Sede Principal y 01 Sede Contingencia)
04 Switchs SAN - Cantidad 04 (02 Sede Principal -02 Sede Contingencia) **(Absolución Nº 20)**
10 Switchs de Acceso (08 Sede Principal y 02 Sede Contingencia)

Firewall de Protección Perimetral
03 Firewall de Protección Perimetral (02 Sede Principal -01 Sede Contingencia)

Plataforma de Virtualización
Software de Virtualización

El acondicionamiento, montaje, instalación, y puesta en funcionamiento debe estar alineado a los criterios y recomendaciones técnicas específicas para la construcción de centros de datos en el Perú

establecido en la Norma Técnica Peruana para la Construcción de Centros de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral N°030-2019-INACAL/DN; recomendaciones del fabricante; así como las normas de seguridad aplicables a la implementación de datacenters.

IV. CARACTERÍSTICAS TÉCNICAS:

Datacenter Principal

Consideraciones Generales:

- Deberá implementarse en las instalaciones actuales de la entidad, considerando las adecuaciones respectivas para el eficiente funcionamiento de la infraestructura en donde residirán el equipamiento de producción.

A fin de garantizar un entorno óptimo y seguro para los equipos y sistemas, las adecuaciones respectivas deben considerar lo siguiente:

Espacio Físico:

Evaluar el espacio disponible para la instalación del Microdatacenter, teniendo en cuenta los requisitos de dimensiones de los racks, pasillos fríos/calientes y zonas de trabajo.

Electricidad:

Verificar la capacidad eléctrica del lugar y asegurarse de que sea suficiente para alimentar todos los equipos.

Considerar la instalación de sistemas de respaldo de energía como UPS (Sistemas de Alimentación Ininterrumpida) o generadores para evitar interrupciones.

Refrigeración:

Evaluar las necesidades de refrigeración para mantener una temperatura adecuada en el Microdatacenter y prevenir el sobrecalentamiento de los equipos.

Diseñar un sistema de refrigeración eficiente que incluya sistemas de enfriamiento, control de humedad y detección de fugas.

Seguridad:

Implementar medidas de seguridad física como cerraduras biométricas, cámaras de vigilancia y control de acceso para garantizar la protección de los activos de datos.

Considerar la ubicación estratégica del Microdatacenter para reducir riesgos de acceso no autorizado o daños.

Cableado:

Planificar el cableado estructurado de manera ordenada y etiquetada para facilitar la gestión y el mantenimiento de los equipos.

Evaluar la ruta de los cables y las conexiones de red para minimizar interferencias electromagnéticas.

Iluminación y Accesibilidad:

Asegurarse que el lugar cuente con iluminación adecuada para la instalación y mantenimiento de los equipos.

Garantizar la accesibilidad para el personal de mantenimiento y la facilidad de movimiento dentro del Microdatacenter.

Protección Contra Incendios:

Implementar sistemas de detección y extinción de incendios, para proteger los equipos y datos.

Cumplimiento Normativo:

Verificar que todas las adecuaciones cumplan con las normativas y regulaciones locales y nacionales relacionadas con la infraestructura de centros de datos.

Mantenimiento Preventivo:

Diseñar un programa de mantenimiento preventivo para garantizar el buen funcionamiento de la infraestructura a lo largo del tiempo.

Dirección de Gestión de Procesos DEMARCO V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

Escalabilidad:
Diseñar la infraestructura con la capacidad de crecimiento futuro en mente, de modo que pueda adaptarse a las necesidades cambiantes de la organización sin requerir una reconstrucción completa.
Respaldo y Recuperación de Desastres:
Establecer las políticas y procedimientos para el respaldo y la recuperación de datos en caso de fallos o desastres.
Gestión de Cableado:
Implementar soluciones de gestión de cableado efectivas para mantener un entorno organizado y de fácil mantenimiento.

- La entidad estará en la potestad de solicitar dentro de los 03 años al proveedor el traslado de la *infraestructura de Datacenter principal* (*Solución Gabinetes* Autocontenidos) a una nueva ubicación en el ámbito de Lima Metropolitana, la entidad deberá proveer las facilidades técnicas en relación a espacio, energía y acondicionamiento del nuevo local.

- El acondicionamiento, montaje, instalación, y puesta en funcionamiento debe estar alineado a los criterios y recomendaciones técnicas específicas para la construcción de centros de datos en el Perú, establecido en la Norma Técnica Peruana para la Construcción de Centros de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral N°030-2019-INACAL/DN; recomendaciones del fabricante; así como, las normas de seguridad aplicables a la implementación de datacenters.

Item	Descripción
Gabinetes de convergencia	Aplicación: Alberga la infraestructura del centro de datos y el equipamiento para la solución de Datacenter Principal. Cantidad: un (1) sistema convergencia conformado por 04 gabinetes de TI de las siguientes medidas: ▪ Dimensiones máximas. - Altura: 200cm. - Ancho: 60cm. - *Profundidad: 135cm (al menos 25cm dedicados* como pasillo frío contenido). ▪ Perfiles de 19" ajustables. ▪ Fabricado en acero al carbono clase A, recubrimiento zincado y acabado con pintura RAL9005 o similar ▪ Altura 42RU. ▪ Paneles laterales. ▪ Se instalarán 2 rPDU verticales monitoreables de 32A en la parte trasera, con un total de 20 tomas tipo C13 y 4 tomas tipo C19. ▪ Capaz de soportar una carga estática de al menos 1500kg. ▪ Puerta frontal de vidrio y puerta trasera de acero. ▪ Sistema de apertura automática instalada con brazo retráctil. ▪ Se instalará una portacables en el techo para la distribución y comunicación del cableado.

Gabinete IT	▪ Dimensiones máximas. - *Altura:* *200cm.* - Ancho: 60cm. - Profundidad: 135cm (al menos 25cm dedicados como pasillo frío contenido). ▪ Perfiles de 19" ajustables. ▪ Fabricado en acero al carbono clase A, recubrimiento zincado y acabado con pintura RAL9005 o similar ▪ Altura 42RU. ▪ Paneles laterales. ▪ 2 rPDU verticales monitoreables, instalados en la parte trasera, 32A, 20xC13 y 4Xc19. ▪ Capaz de soportar una carga estática de al menos 1500kg. ▪ Puerta frontal de vidrio y puerta trasera de acero. ▪ Sistema de apertura automática instalada con brazo retráctil. ▪ Portacables instalada en el techo para la distribución y comunicación de cableado.
Sistema eléctrico (rackeado)	▪ Alimentación a 380VAC, 3f+neutro + tierra, 60hz. ▪ Interruptor termomagnético principal y llaves ITM independientes para sistema de refrigeración, condensador y UPS instalados en el sistema autocontenido. SPD switch. ▪ Capacidad de ampliación para la alimentación eléctrica de al menos 4 gabinetes desde el gabinete de convergencia. ▪ Se debe considerar sistema ATS rackeado para 125A, alimentación a 380VAC trifásico.
UPS integrado	Se requiere un sistema de UPS con una capacidad de 10KVA/9KW en configuración n+1. Eficiencia de al menos 94.5%. Montaje rackeable. Alimentación 220VAC, 1ph, 60hz. Doble conversión. Factor de potencia de salida de 0.9 THDv <2% (carga lineal). Nivel de ruido <=55dB. Capacidad de sobre carga del inverter: 105% ≤ carga < 125% - transferencia a modo bypass después de 5 minutos. 125% ≤ carga < 150% - transferencia a modo bypass después de 1 minuto.
Baterías rackeables	Bancos de baterías rackeables, 240V, 9Ah.
Sistema monitoreo y gestión centralizada	▪ Sistema de monitoreo rackeable que concentre el monitoreo y gestión del sistema de refrigeración, distribución eléctrica, UPS, seguridad y sensores ambientales. ▪ Unidad de gestión: - Rackeable en 1RU, módulo de potencia y módulo de control extraíbles del chasis para un fácil reemplazo o upgrade. - Temperatura de trabajo -20 a 50°c.

Dirección de Gestión de Procesos GERENCIA V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

- Humedad relativa 5-95%HR.
- Puerto para SIM card para el envío de alertas.
- Antena direccional.
- Alimentación 200-240VAC.
- Suministro de salida para la alimentación de periféricos y equipos conectados. Alimentación de salida 53.5VDC y salida AC.
- Puertos LAN y WAN con autonegociación 10/100/1000Mbits/s.
- Puerto RS485 para expansión.
- Puertos AIDI con conector RJ45 para la conexión de sensores de humo, agua y NTC.
- Puerto USB para la instalación del módulo Wifi para el monitoreo con smartphone o Tablet, que permita revisar el layout de distribución de equipos, alarmas y demás variables.

▪ Detecta y recolecta la estadística de la temperatura y humedad al interior del sistema autocontenido.

▪ Apertura automáticamente las puertas en caso del ingreso de clave o reconocimiento facial.

▪ En caso de emplear sistema de extinción de sala, las puertas traseras se aperturan automáticamente al detectar humo en el sistema autocontenido. En caso de emplear la extinción interior, el sistema se mantiene confinado para permitir la extinción adecuada.

▪ Detecta fuga de agua en la base del autocontenido y provee señales de alarma en tiempo real.

▪ Se interconecta con el UPS de manera nativa para el monitoreo de las variables eléctricas (voltaje, frecuencia, corriente, etc.)

▪ Monitoreo del sistema de refrigeración:
  - Monitoreo del suministro y la temperatura del aire de retorno.
  - Configuración del setpoint de temperatura desde el sistema de monitoreo y gestión centralizada.
  - Monitoreo y presentación de la velocidad de ventilación, % de uso.
  - Monitoreo del estado del compresor.
  - Presentación del estado real del humidificador y resistencia.

▪ Video vigilancia: Conexión con las cámaras del sistema, provee alimentación PoE, acceso real a las imágenes en el gestor web (WebUI).

▪ Vistas:
  - Generación de vistas al menos en 2D que muestren la distribución actual de los gabinetes, indicando la ubicación de tablero eléctrico rackeable, las unidades de refrigeración, los gabinetes IT, gabinetes para networking y los UPS.
  - Muestra el estado actual de alarmas de los sensores de temperatura y humedad.
  - Debe contar con reconocimiento facial a través de la Tablet de monitoreo de al menos 10", instalada en la puerta del gabinete principal.

▪ Alarmas:

Dirección de Gestión de Procesos CENEPRED V°B°

CENEPRED DGP V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

		- El sistema debe monitorear de manera nativa el estado de los equipos de refrigeración, unidades UPS y dispositivos ambientales. En caso de una alerta o error, el sistema deberá generar una alarma en tiempo real. La cual puede ser visualizada en la pantalla de gestión en el gabinete de gestión. La alarma debe ser mostrada, así como la sugerencia de solución. - Alarmas clasificadas en crítico, mayor, menor y warning. Dichas alarmas deberán poder ser filtrada. - La iluminación cambiará de color según el nivel de severidad de la alarma. - Envío de alarmas por email y SMS. Al menos 500 alarmas deben ser soportadas. ▪ Sensores requeridos: temperatura NTC (2 unidades por gabinete), humedad (1 unidad), humo, sonda de inundación tipo cuerda (1 unidad). ▪ 1 cámara domo fijo de 2MP, IR, con accesorio de montaje para el gabinete. ▪ Gestión centralizada.
	Sistema de Climatización de expansión directa (Aire Acondicionado de precisión interno y rackeable)	Cantidad: Un sistema de refrigeración en redundancia N+1 con las siguientes características: **Características Generales:** ▪ Capacidad de. Enfriamiento mínimo de 12.5kW, bajo las siguientes condiciones ▫ Temperatura de bulbo seco 37.8°c y bulbo húmedo de 20.8°C. ▫ Temperatura de bulbo seco (externo) 35°c. ▪ Refrigerante: R410A. ▪ Capacidad de refrigeración regulable a demanda de manera automática de al menos 30-100%. ▪ Monitoreo: Local a través de la pantalla táctil extraíble tipo Tablet instalada en el gabinete de infraestructura y remoto haciendo uso del gestor web que integra la solución de monitoreo ambiental, sistema de refrigeración, tablero y control de acceso. ▪ Condensador y Evaporador de la misma marca ▪ Disponibilidad de operación 24x7 ▪ Capacidad de trabajo en equipo: Deberá permitir la ampliación con unidades de la misma familia para futuros crecimientos o trabajo en redundancia. **Unidad Evaporadora:** ▪ Clase: Rackeable, no mayor a 11RU cada unidad evaporadora. ▪ Flujo de aire: frontal. ▪ Alimentación eléctrica: 208-240VAC / 1 fase / 60 Hz

	▪ Ventiladores: Al menos 4 ventiladores EC. ▪ *Com Flujo promedio: 2600m3/h mínimo.* ▪ Válvula de expansión: Electrónica ▪ Bomba de condensado incorporada. ▪ Se requiere que al menos uno de los 2 evaporadores cuente con humidificador incorporado. **Unidad Condensadora externa:** ▪ Alimentación eléctrica: 208 - 230V / 1 fase / 60 Hz ▪ Ventiladores mínimos 01. ▪ Compresor de capacidad variable: DC de frecuencia variable, capaz de trabajar entre 30-100%, garantizando su operación a demanda de la variación de la carga térmica instalada.
Sistema de detección y extinción de incendios compacto (interno)	Cantidad uno (02): ▪ Dimensiones máximas - Altura: <=6RU, tanque de extinción y sistema de detección cruzada al interior de la unidad. - Ancho: 19" (rackeable) ▪ Agente limpio Perfluorohexanone o NOVEC 1230 >=6.3KG. ▪ Batería para Backup de 24 horas ▪ Capacidad de extinción para el sistema autocontenido. ▪ Extinción al interior del gabinete. ▪ Detección de temperatura y humo. ▪ Alarma, luz de aviso y contacto seco. ▪ Tiempo de vida del sistema de extinción de al menos 10 años.

Datacenter Secundario

Consideraciones Generales:

- Deberá implementarse en las instalaciones actuales de la entidad, considerando las adecuaciones respectivas para el eficiente funcionamiento de la infraestructura en donde residirán el equipamiento de producción

  A fin de garantizar un entorno óptimo y seguro para los equipos y sistemas, las adecuaciones respectivas deben considerar lo siguiente:

  Espacio Físico:
  Evaluar el espacio disponible para la instalación del Microdatacenter, teniendo en cuenta los requisitos de dimensiones de los racks, pasillos fríos/calientes y zonas de trabajo.
  Electricidad:
- Verificar la capacidad eléctrica del lugar y asegurarse de que sea suficiente para alimentar todos los equipos.

Considerar la instalación de sistemas de respaldo de energía como UPS (Sistemas de Alimentación Ininterrumpida) o generadores para evitar interrupciones.

Refrigeración:

Evaluar las necesidades de refrigeración para mantener una temperatura adecuada en el Microdatacenter y prevenir el sobrecalentamiento de los equipos.

Diseñar un sistema de refrigeración eficiente que incluya sistemas de enfriamiento, control de humedad y detección de fugas.

Seguridad:

Implementar medidas de seguridad física como cerraduras biométricas, cámaras de vigilancia y control de acceso para garantizar la protección de los activos de datos.

Considerar la ubicación estratégica del Microdatacenter para reducir riesgos de acceso no autorizado o daños.

Cableado:

Planificar el cableado estructurado de manera ordenada y etiquetada para facilitar la gestión y el mantenimiento de los equipos.

Evaluar la ruta de los cables y las conexiones de red para minimizar interferencias electromagnéticas.

Iluminación y Accesibilidad:

Asegurarse que el lugar cuente con iluminación adecuada para la instalación y mantenimiento de los equipos.

Garantizar la accesibilidad para el personal de mantenimiento y la facilidad de movimiento dentro del Microdatacenter.

Protección Contra Incendios:

Implementar sistemas de detección y extinción de incendios, para proteger los equipos y datos.

Cumplimiento Normativo:

Verificar que todas las adecuaciones cumplan con las normativas y regulaciones locales y nacionales relacionadas con la infraestructura de centros de datos.

Mantenimiento Preventivo:

Diseñar un programa de mantenimiento preventivo para garantizar el buen funcionamiento de la infraestructura a lo largo del tiempo.

Escalabilidad:

Diseñar la infraestructura con la capacidad de crecimiento futuro en mente, de modo que pueda adaptarse a las necesidades cambiantes de la organización sin requerir una reconstrucción completa.

Respaldo y Recuperación de Desastres:

Establecer las políticas y procedimientos para el respaldo y la recuperación de datos en caso de fallos o desastres.

Gestión de Cableado:

Implementar soluciones de gestión de cableado efectivas para mantener un entorno organizado y de fácil mantenimiento.

- La entidad estará en la potestad de solicitar dentro de los 03 años al proveedor el traslado de la infraestructura de Datacenter Contingencia - secundario (Solución Gabinetes Autocontenidos) a una nueva ubicación en el ámbito de Lima Provincias y/o Lima Metropolitana, la entidad deberá proveer las facilidades técnicas en relación a espacio, energía y acondicionamiento del nuevo local.

- El acondicionamiento, montaje, instalación, y puesta en funcionamiento debe estar alineado a los criterios y recomendaciones técnicas específicas para la

construcción de centros de datos en el Perú, establecido en la Norma Técnica Peruana para la Construcción de Centros de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral N°030-2019-INACAL/DN; recomendaciones del fabricante; así como, las normas de seguridad aplicables a la implementación de datacenters.

- La Entidad deberá proporcionar enlace dedicado entre el Datacenter Principal y el Datacenter de contingencia que asegure la sincronización de la información.

Item	Descripción
Gabinetes de convergencia	Aplicación: Alberga la infraestructura del centro de datosy el equipamiento para la solución de Datacenter de contingencia. Cantidad: un (1) sistema convergencia conformado por 03 gabinetes de las siguientes medidas: ▪ Dimensiones máximas. - Altura: 200cm. - Ancho: 60cm. - Profundidad: 135cm (al menos 25cm dedicados como pasillo frío contenido). - Pasillos frío y caliente autocontenidos en el gabinete ▪ Fabricado en acero al carbono clase A, recubrimiento zincado y acabado con pintura RAL9005 o similar. ▪ Altura 42RU. ▪ Fabricante con certificación ISO14001 e ISO9001. ▪ Rieles ajustables de 19" según EIA 310 con marcación de los RU. ▪ Capacidad de carga estática de al menos 1500kg y 1000kg de carga dinámica. ▪ Puerta frontal de vidrio y puerta trasera de acero. ▪ Sistema de apertura automática instalada con brazo retráctil. ▪ Gabinete principal con Iluminación inteligente RGB que indique el estado del sistema. ▪ El sistema debe permitir el montaje de una unidad contra incendios rackeable con capacidad de extinción de hasta 5 gabinetes con una sola unidad.
Gabinete IT	▪ Dimensiones máximas. - Altura: 200cm. - Ancho: 60cm. - Profundidad: 135cm (al menos 25cm dedicados como pasillo frío contenido). ▪ Perfiles de 19" ajustables. ▪ Fabricado en acero al carbono clase A, recubrimiento zincado y acabado con pintura RAL9005 o similar ▪ Altura 42RU. ▪ Paneles laterales. ▪ 2 rPDU verticales monitoreables, instalados en la parte trasera, 32A, 20xC13 y 4Xc19.

	▪ Capaz de soportar una carga estática de al menos 1500kg. ▪ Puerta frontal de vidrio y puerta trasera de acero. ▪ Sistema de apertura automática instalada con brazo retráctil. ▪ Portacables instalada en el techo para la distribución y comunicación de cableado.
Sistema eléctrico (rackeado)	▪ Alimentación a 380VAC, 3f+neutro + tierra, 60hz. ▪ Interruptor termomagnético principal y llaves ITM independientes para sistema de refrigeración, condensador y UPS instalados en el sistema autocontenido. SPD switch. ▪ Capacidad de ampliación para la alimentación eléctrica de al menos 4 gabinetes desde el gabinete de convergencia. ▪ Se debe considerar sistema ATS rackeado para 125A, alimentación a 380VAC trifásico.
UPS integrado	Se requiere un sistema de UPS de 10KVA/9KW en configuración n+1. Eficiencia de al menos 94.5%. Montaje rackeable. Alimentación 220VAC, 1ph, 60hz. Doble conversión. Factor de potencia de salida de 0.9 THDv <2% (carga lineal). Nivel de ruido <=55dB. Capacidad de sobre carga del inverter: 105% ≤ carga < 125% - transferencia a modo bypass después de 5 minutos. 125% ≤ carga < 150% - transferencia a modo bypass después de 1 minuto.
Baterías rackeables	Bancos de baterías rackeables, 240V, 9Ah.
Sistema monitoreo y gestión centralizada	▪ Sistema de monitoreo rackeable que concentre el monitoreo y gestión del sistema de refrigeración, distribución eléctrica, UPS, seguridad y sensores ambientales. ▪ Unidad de gestión: - Rackeable en 1RU, módulo de potencia y módulo de control extraíbles del chasis para un fácil reemplazo o upgrade. - Temperatura de trabajo -20 a 50°c. - Humedad relativa 5-95%HR. - Puerto para SIM card para el envío de alertas. - Antena direccional. - Alimentación 200-240VAC. - Suministro de salida para la alimentación de periféricos y equipos conectados. Alimentación de salida 53.5VDC y salida AC. - Puertos LAN y WAN con autonegociación 10/100/1000Mbits/s. - Puerto RS485 para expansión. - Puertos AIDI con conector RJ45 para la conexión de sensores de humo, agua y NTC. - Puerto USB para la instalación del módulo Wifi para el monitoreo con smartphone o Tablet, que permita revisar el layout de distribución de equipos, alarmas y demás variables.

Dirección de Gestión de Procesos CENPRED V°B°

CENPRED DIDGI

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

- Detecta y recolecta la estadística de la temperatura y humedad al interior del sistema autocontenido.
- Apertura automáticamente las puertas en caso del ingreso de clave o reconocimiento facial.
- En caso de emplear sistema de extinción de sala, las puertas traseras se aperturan automáticamente al detectar humo en el sistema autocontenido. En caso de emplear la extinción interior, el sistema se mantiene confinado para permitir la extinción adecuada.
- Detecta fuga de agua en la base del autocontenido y provee señales de alarma en tiempo real.
- Se interconecta con el UPS de manera nativa para el monitoreo de las variables eléctricas (voltaje, frecuencia, corriente, etc.)
- Monitoreo del sistema de refrigeración:
  - Monitoreo del suministro y la temperatura del aire de retorno.
  - Configuración del setpoint de temperatura desde el sistema de monitoreo y gestión centralizada.
  - Monitoreo y presentación de la velocidad de ventilación, % de uso.
  - Monitoreo del estado del compresor.
  - Presentación del estado real del humidificador y resistencia.
- Video vigilancia: Conexión con las cámaras del sistema, provee alimentación PoE, acceso real a las imágenes en el gestor web (WebUI).
- Vistas:
  - Generación de vistas al menos en 2D que muestren la distribución actual de los gabinetes, indicando la ubicación de tablero eléctrico rackeable, las unidades de refrigeración, los gabinetes IT, gabinetes para networking y los UPS.
  - Muestra el estado actual de alarmas de los sensores de temperatura y humedad.
  - Debe contar con reconocimiento facial a través de la Tablet de monitoreo de al menos 10", instalada en la puerta del gabinete principal.
- Alarmas:
  - El sistema debe monitorear de manera nativa el estado de los equipos de refrigeración, unidades UPS y dispositivos ambientales. En caso de una alerta o error, el sistema deberá generar una alarma en tiempo real. La cual puede ser visualizada en la pantalla de gestión en el gabinete de gestión. La alarma debe ser mostrada, así como la sugerencia de solución.
  - Alarmas clasificadas en crítico, mayor, menor y warning. Dichas alarmas deberán poder ser filtrada.
  - La iluminación cambiará de color según el nivel de severidad de la alarma.
  - Envío de alarmas por email y SMS. Al menos 500 alarmas deben ser soportadas.

		▪ Sensores requeridos: temperatura NTC (2 unidades por gabinete), humedad (1 unidad), humo, sonda de inundación tipo cuerda (1 unidad). ▪ 1 Cámara domo fijo de 2MP, IR, con accesorio de montaje para el gabinete. ▪ Gestión centralizada.
	Sistema de Climatización de expansión directa (Aire Acondicionado de precisión interno y rackeable)	Cantidad: Un sistema de refrigeración en redundancia N+1 con las siguientes características: **Características Generales:** ▪ Capacidad de. Enfriamiento mínimo de 12.5kW, bajo las siguientes condiciones ▫ Temperatura de bulbo seco 37.8°c y bulbo húmedo de 20.8°C. ▫ Temperatura de bulbo seco (externo) 35°c. ▪ Refrigerante: R410A. ▪ Capacidad de refrigeración regulable a demanda de manera automática de al menos 30-100%. ▪ Monitoreo: Local a través de la pantalla táctil extraíble tipo Tablet instalada en el gabinete de infraestructura y remoto haciendo uso del gestor web que integra la solución de monitoreo ambiental, sistema de refrigeración, tablero y control de acceso. ▪ Condensador y Evaporador de la misma marca ▪ Disponibilidad de operación 24x7 ▪ Capacidad de trabajo en equipo: Deberá permitir la ampliación con unidades de la misma familia para futuros crecimientos o trabajo en redundancia. **Unidad Evaporadora:** ▪ Clase: Rackeable, no mayor a 11RU cada unidad evaporadora. ▪ Flujo de aire: frontal. ▪ Alimentación eléctrica: 208-240VAC / 1 fase / 60 Hz ▪ Ventiladores: Al menos 4 ventiladores EC. ▪ Flujo promedio: 2600m3/h mínimo. ▪ Válvula de expansión: Electrónica ▪ Bomba de condensado incorporada. ▪ Se requiere que al menos uno de los 2 evaporadores cuente con humidificador incorporado. ***Unidad Condensadora externa:*** ▪ Alimentación eléctrica: 208 - 230V / 1 fase / 60 Hz ▪ Ventiladores mínimos 01. ▪ Compresor de capacidad variable: DC de frecuencia variable, capaz de trabajar entre 30-100%, garantizando su operación a demanda de la variación de la carga térmica instalada.

Cantidad uno (01):

Sistema de detección y extinción de incendios compacto (interno)	▪ Dimensiones máximas - Altura: <=6RU, tanque de extinción y sistema de detección cruzada al interior de la unidad. - Ancho: 19" (rackeable) ▪ Agente limpio Perfluorohexanone o NOVEC 1230 >=6.3KG. ▪ Batería para Backup de 24 horas ▪ Capacidad de extinción para el sistema autocontenido. ▪ Extinción al interior del gabinete. ▪ *Detección de temperatura y humo.* ▪ Alarma, luz de aviso y contacto seco. ▪ Tiempo de vida del sistema de extinción de al menos 10 años.

Solución de Backup

-01 Sistema de Backup -01Servidor para Backup

-01 Software de Backup

Equipo	Característica	Mínimo requerido
Sistema de almacenamiento de respaldo - SAN	Cantidad de Dispositivo Dedicado a Respaldo a Disco	Uno (01)
	Generalidades	La solución ofertada deberá ser un almacenamiento de propósito específico para datos de Backup, con capacidad para guardar y retener copias de respaldo conforme a las políticas de Backup definidas desde la aplicación de Backup.
		Así, la solución debe estar certificada por el fabricante como solución de almacenamiento para Backup. No se aceptarán soluciones que utilicen almacenamiento de propósito general que a través de controladores externas o software determinado emulen las capacidades de una solución propia para Backup.
	Características de Cómputo	El dispositivo de almacenamiento debe tener al menos dos controladores o nodos y debe tener al menos 64 núcleos con un mínimo de 2,3 GHz.
		La capacidad de cada controladora debe tener un mínimo de 256 GB de memoria Cache, la cual debe ser nativa y no deberá estar basada en discos y/o módulos flash [Excluyendo cualquier módulo de aceleración de rendimiento: PAM FlashCache caché SSD o SCM). (Absolución Consulta N° 1)
	Formato	El dispositivo debe permitir realizar el respaldo y recuperación de información basado en discos duros, mediante un mecanismo de optimización de

			deduplicación; dicha deduplicación deberá de realizarse en línea, durante la ingesta de los datos.
		Deduplicación basada en origen	Se admite la deduplicación de datos basada en origen, lo que puede ahorrar el ancho de banda de la red necesaria para conectar SISTEMA DE ALMACENAMIENTO DE RESPALDO - SAN de medios de Backup y almacenamiento de Backup, y mejorar la velocidad de Backup.
		Compatibilidad	El dispositivo debe ser compatible con los softwares de Backup HPE Data Protector, EMC Networker e IBM Spectrum Protect, Veeam, u otro equivalente.
		Conectividad	La solución ofertada debe soportar conectividad Fibra Channel de 16/32Gb e Ethernet de 10Gb y 25Gb, incluyendo en la oferta como mínimo ocho (08) puertos de 25GbE SFP.
		Disponibilidad	**El dispositivo debe tener componentes como las fuentes de poder y ventiladores redundantes y reemplazables en caliente. debe contar con una arquitectura activo-activo, considerando mínimo 2 controladores por solución.** **(Absolución consultas Nº 2)**
		Tipo de Disco	La solución deberá soportar discos de tecnología *SSD y SAS o NL-SAS. Los discos duros que* conforman esta solución deben ser de tipo SAS. Los discos de Estado Sólido (SSD) deben ser de una capacidad mínima de 3.84TB y los discos duros SAS deben ser de capacidad mínima de 4TB y una velocidad mínima de 7.2 K.
		Rendimiento	El dispositivo deberá de poder llegar a un nivel de rendimiento de escritura de 40 TB/hr
		Protección	**La solución propuesta debe contar con el nivel de protección en RAID 6 en base a la tecnología y *mejores prácticas del fabricante. Deberá soportar* el RAID de triple paridad y configurar en este tipo de arreglo.** **(Absolución consultas Nº 3)**
		Capacidad	El dispositivo deberá suministrarse con al menos 100TiB usables, debidamente licenciados. (antesde la compresión y deduplicación) La ratio de reducción a considerar deberá ser de a lo muchode 2.5 a 1. El dispositivo deberá suministrarse con una capade aceleración basada en SSD con un mínimo de 4 discos SSD de 3.84 TB Se agrega; el ratio de reducción a considerar deberá ser de a lo mucho de 2.5 a 1, de esta forma garantizar los 300TiB efectivos solicitados, considerando 135TiB físicos útiles donde esta capacidad física útil deberá reflejarse en el dashboard. **(Absolución consultas Nº 24)**

			la plataforma deberá tener una escalabilidad máxima de 1.5 PB, considerando que dicha capacidad de escalabilidad es una característica común de equipos de alta gama como el que se viene solicitando. (Absolución consultas N°25)
		Optimización de Datos	La solución propuesta debe incluir la funcionalidad de compresión y deduplicación, el proceso debe correr en la solución y en ninguna circunstancia debe tener agentes o manejadores instalados en los SISTEMA DE ALMACENAMIENTO DE RESPALDO - SAN de respaldo o los clientes del Software de respaldo. La compresión y deduplicación deberá efectuarse en línea, durante la ingesta de datos.
			Debiendo estar licenciado para la capacidad de la solución propuesta/ofertada.
		Administración	El dispositivo debe contar con un software de gestión propio que vía GUI o Web para su administración.
			Debe tener la capacidad de generar y enviar correos electrónicos o alarmas a una consola de gestión y soporte de SNMP Traps.
			Debe Permitir exportar información de monitoreo, log de errores, etc. hacia "fuera" del dispositivo.
			La solución debe ser compatible con la integración a una plataforma tipo SaaS proporcionada por el fabricante, que cuente con capacidades de Machine Learning (ML) para aprovechar el aprendizaje automático en la monitorización y medición proactiva del estado general del almacenamiento ofrecido. Esto se logrará a través de análisis inteligentes, integrales y predictivos.
		Replicación	El dispositivo deberá soportar la funcionalidad de réplica la información a través de redes IP de bajo ancho de banda a otro dispositivo igual, o de la misma familia.
		Seguridad de los datos	Los paquetes NFS y CIFS/SMB admiten la transmisión cifrada en la capa de protocolo.
			Debe incluir una licencia para el cifrado de los datos almacenados para evitar la fuga de información sensible.
			Debe incluir una licencia para WORM a nivel de cumplimiento y permita a los usuarios establecer un período de protección. Durante el período de

		protección, los archivos no se pueden modificar ni eliminar.
	Accesorio	Incluir los cables de poder y todo aquello necesario para el funcionamiento de la solución como cables de red, transceivers y otros.
	Garantía de todo el equipo	La garantía para todas las partes y componentes debe ser por un periodo de tres (03) años on site 7x24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la entidad pueda reportar la incidencia.

Software de Backup

- La solución debe respaldar 70 cargas de trabajo entre máquinas virtuales y servidores físicos.
- El licenciamiento debe ser de modo perpetuo, con soporte del fabricante a 3 años 24x7.
- La solución debe proporcionar una copia de seguridad eficiente 'incremental para siempre' e incluir opciones de copias de seguridad completas y ad-hoc.
- *La solución debe admitir la copia de seguridad de VM directamente desde* SAN.
- La solución debería detectar automáticamente las máquinas virtuales con el uso compartido de bus SCSI y excluirlas de la copia de seguridad.
- La solución debería detectar automáticamente el espacio libre del datastore productivo y evitar la instantánea de copia de seguridad si el espacio está por debajo del umbral definido.
- La solución debería monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido.
- La solución debería detectar automáticamente las instantáneas de respaldo de VMware huérfanas y eliminarlas.
- La solución debería permitir la exclusión de discos de máquinas virtuales y archivos de intercambio (swap) en copias de seguridad basadas en instantáneas.
- La solución debería permitir la exclusión de archivos y carpetas de la copia de seguridad basada en instantáneas.
- La solución no debería requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la recuperación granular.
- No se debe requerir que la solución realice una copia de seguridad separada de los datos de la aplicación en máquinas virtuales para facilitar la recuperación granular de elementos de la aplicación.
- La copia de seguridad sin agente debe truncar los registros de transacciones o archivos de Microsoft SQL, Microsoft Exchange y Oracle Database.
- La copia de seguridad sin agente de máquinas virtuales debe proporcionar copias de seguridad de registros o archivos de transacciones de Microsoft SQL y Oracle Database junto con copias de seguridad basadas en instantáneas.
- La solución debería permitir la recuperación de archivos y elementos de aplicaciones sin instalar Agentes o plugins en Máquinas Virtuales.

- La solución debe integrarse con los sistemas de almacenamiento y utilizar snapshots de almacenamiento para las operaciones de respaldo.
- La solución debería poder leer los datos de la máquina virtual directamente desde un snapshot de almacenamiento a través de una conexión SAN.
- La solución debería proporcionar la capacidad de explorar máquinas virtuales en snapshots de almacenamiento y recuperar instantáneamente la máquina virtual, el archivo del sistema operativo o la carpeta o los elementos de la aplicación directamente desde el snapshot de almacenamiento.
- Esta capacidad también debería aplicarse a los snapshots de almacenamiento creados independientemente de la aplicación de respaldo.
- La solución debería poder utilizar snapshots de almacenamiento para crear una copia de la máquina virtual en un entorno de red aislado para fines de prueba.
- Para eliminar el tiempo de inactividad y minimizar la perdida de datos de VMware vSphere, se debe incorporar una solución de protección continua de datos, logrando RTOs y RPOs mínimos.
- La solución debería replicar máquinas virtuales sin snapshots del ambiente virtual y debe capturar todas las E/S de escritura directamente de la VM.
- La solución no deberá tener dependencia de hardware y deberá proteger cualquier SO y Aplicación que corra en una VM de vSphere, sin importar si se ejecuta en infraestructuras convergentes, hiperconvergentes o discos locales del vSphere ESXi.
  La solución debería ser una replicación asíncrona que se pueda utilizar a cualquier distancia sin un ancho de banda mínimo requerido de operación.
- La funcionalidad deberá estar incluida en el mismo licenciamiento de respaldo, es decir que no debe requerir alguna otra licencia extra.

Operaciones de recuperación

- La solución debe proporcionar una portabilidad completa en cualquier archivo de respaldo propietario y no debe depender de ninguna infraestructura de respaldo en un punto en el tiempo, por ejemplo, el catálogo central, para la recuperación.
- La solución debe proporcionar tecnología de recuperación de la máquina virtual instantánea, correr múltiples Virtual Machine es directamente desde el servidor de copia de seguridad del repositorio.
- La solución debe proporcionar la tecnología de recuperación Changed Block Tracking para máquinas virtuales VMware y Hyper-V.
- La solución debería permitir la recuperación de VMware Virtual Machine a través del canal de fibra SAN.
- La solución debe escanear los datos de la máquina virtual con un software antivirus antes de restaurar la máquina al entorno de producción. La solución debería abortar la operación de recuperación si se detecta malware.
- La solución debería proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script en el sistema operativo invitado que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación.
- La solución debería proporcionar una recuperación completa de la copia de seguridad basada en el Agente con la capacidad de crear un medio de arranque para el servidor específico.
- La solución debe permitir la recuperación instantánea de copias de seguridad basadas en agentes para VMware o máquinas virtuales Hyper-V.
- La solución debe permitir la recuperación instantánea de copias de seguridad de sistemas de archivos tipo NAS (FileShares).
- La solución debería facilitar la recuperación de VMware o una copia de seguridad basada en agentes directamente en Google Platform, Amazon AWS o Microsoft Azure y Microsoft Azure Stack.
- La solución debería convertir automáticamente UEFI a BIOS durante la

operación de recuperación de Amazon AWS.

- La solución debería facilitar las operaciones de recuperación a nivel de archivo sin la necesidad de implementar un agente o plugin en un servidor virtual o físico.
- La solución debería poder recuperar archivos en un sistema operativo invitado de máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual.
- La solución debe proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de buscar un archivo específico en todas las copias de seguridad.
- La solución debe admitir todos los sistemas de archivos dentro del alcance de la entidad.
- La solución debería admitir la recuperación granular de las aplicaciones de Microsoft Active Directory, Exchange, SQL y SharePoint.
- La solución debería admitir la recuperación granular de bases de datos Oracle a partir de copias de seguridad basadas en imágenes u Oracle RMAN.
- La solución no debe usar un producto de terceros para la recuperación granular de elementos de la aplicación.
- La solución debe proporcionar una interfaz de usuario de autoservicio basada en la web y la capacidad de examinar y recuperar elementos de Microsoft Exchange y bases de datos SQL u Oracle.
- La solución debe permitir la recuperación instantánea de base de datos SQL u Oracle desde la copia de seguridad al último estado o a un punto anterior en el tiempo a cualquier servidor de base de datos de producción o clúster (físico o virtual) en minutos, independientemente de su tamaño.

Requisitos de la solución de respaldo

- La solución debe estar definida por software y ser capaz de ejecutarse localmente o en cualquier plataforma en la nube.
- La solución debe ser independiente del almacenamiento y debe contar con tecnología integrada de deduplicación y compresión.
- La solución deberá asegurar las copias de seguridad en repositorios reforzados a prueba de malware y hackers con copias de seguridad inmutables, para prevenir el cifrado o eliminación por ransomware.
- La solución debe poder escalar tanto horizontal como verticalmente (es decir, escalar y escalar).
- La solución debe proporcionar un mecanismo fácil para expandir o contratar el almacenamiento de respaldo de destino.
- La solución debería ofrecer la flexibilidad para ajustar el tamaño del bloque de deduplicación de datos y el nivel de compresión de datos.
- La solución debe integrarse con los dispositivos de deduplicación EMC Data Domain, HPE Store Once, Quantum y ExaGrid.
- La solución debería admitir de forma nativa la copia de seguridad en cinta y no debería requerir software o hardware adicional.
- La solución debe admitir copias de seguridad deduplicadas y comprimidas en medios de cinta.
- La solución debe admitir medios de cinta WORM.
- La solución debería admitir de forma nativa el traslado de archivos de respaldo a Amazon S3 (con inmutabilidad), IBM Cloud Object Storage, Azure Blob Cloud Storage, Google Cloud Storage, y otras plataformas de almacenamiento en la nube compatibles con S3.
- La solución debería admitir de forma nativa el traslado de archivos de respaldo a Amazon S3 Glacier (incluido Deep Archive) con capacidad de inmutabilidad, y Microsoft Azure Blob Storage Archive Tier para archivado a largo plazo de copias de seguridad.
- La solución debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube.
- La solución debería proporcionar 100 o más opciones de proveedor de nube para el almacenamiento de copia de seguridad en la nube

Dirección de Gestión de Procesos CENEPRED V°B°

Dirección de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B° Centro Nacional

- La solución debe proporcionar soporte para el almacenamiento de objetos en las instalaciones.
- La solución debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.
- La solución debería ofrecer inmutabilidad en el almacenamiento de objetos S3 a nivel de depósito.
- La solución debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. Idealmente, ambas opciones se pueden combinar.
- La solución debería encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo.
- La solución debe proporcionar un cifrado AES de 256 bits con tecnología de protección de pérdida de contraseña, por lo que los datos se pueden descifrar si se pierde la contraseña operativa.
- La solución debe integrarse con SAML 2.0 para la autenticación extendida. La solución debería leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debería reconstruir automáticamente el bloque dañado con datos de producción.
- La solución debe proporcionar control de acceso basado en roles a través de una interfaz de usuario web para la mayoría de las operaciones de recuperación y respaldo.
- La solución debería iniciar automáticamente las máquinas virtuales a partir de copias de seguridad y verificar el sistema operativo y la disponibilidad de la aplicación. Esta prueba no debe tener impacto en la red de producción. La solución debe proporcionar un informe de verificación de recuperación.
- La solución debería escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo.

Monitoreo y Reporting de Respaldo

- La solución debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo.
- La solución debe alertar por adelantado si el objetivo de la copia de seguridad se acerca a la capacidad.
- La solución debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento, y el proveedor debe actualizar dinámicamente la detección.
- La solución debe proporcionar un informe de evaluación de Infraestructura VMware para asegurar que el entorno esté preparado para las operaciones de respaldo basadas en instantáneas y detectar máquinas virtuales que requieren implementación de respaldo basada en agente.
- La solución debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas.
- La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas.
- La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo.
- La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría.
- La solución debe proporcionar una infraestructura de respaldo y un informe de cambios de política para fines de auditoría.

Servidor de Backup

Ítem	Características
Cantidad	Uno (01)
Factor Forma	Tipo rack, 1U como máximo
Procesador	Cantidad de procesadores soportados: Mínimo 02. Procesadores instalados**: Mínimo 02.** **Procesadores de última generación.** (Absolución de consulta Nº 18) Número de núcleos instalados por procesador: Mínimo 16. Cantidad de subprocesos por procesador: mínimo 32 hilos Velocidad de reloj de cada procesador: Mínimo 2.3 GHz. Memoria cache por procesador: mínimo 35 MB
Memoria	DDR5 con velocidad mínima de 4800 MHz. Tipo de memoria: RDIMM Capacidad instalada: **Mínima 64 GB**
Almacenamiento	Debe soportar distintos tipos de discos, como mínimo 8 de 2.5" Debe incluir como mínimo 2 discos SSD de 480GB en RAID1 Factor de forma: 2.5" SFF Los discos ofertados deben tener la capacidad de ser intercambiable en caliente (Hot Swap)
Controlador de Almacenamiento	HBA con memoria caché mínima de 4gb y soporte para RAID 0/1/10/5/50/6/60
Red LAN	Se debe incluir 4 puertos de 10/25GbE SFP+ para la LAN con sus respectivos transceivers
Ventilación	Redundantes Hot Swap o Hot Plug. Debe tener instalado el máximo número de ventiladores que soporte el chasis
Fuente de energía	Deberá contar con dos fuentes de poder del tipo AC en redundancia y hot-swap, mínimo de 900W y de categoría TITANIUM
Administración	Software de administración de la misma marca del servidor, acreditada con carta del fabricante, que permita como mínimo: estado de salud del equipo y monitoreo de alertas. Debe contar con la capacidad de monitorear los componentes de hardware y software Debe contar con la capacidad de levantar el inventario de sus componentes Sistema de Alertas Predictivas solicitado requiere de un monitoreo automático y constante, capaz de emitir alertas (a través del software de

Dirección de Gestión de Procesos CENEPRED V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

	gestión, por medio de mail, etc.) ANTES que los componentes alertados fallen. Es decir, con la capacidad de predecir futuras fallas. Acceso remoto con consola gráfica al servidor, vía GUI y/o WEB debidamente licenciada y habilitada.
Sistemas operativos Soportados	Debe soportar como mínimo: Microsoft Windows Server, SUSE Linux Enterprise Server, VMware ESXi, Red Hat Enterprise Linux, openEuler, etc Licencia OEM con Windows Server Estándar y debe incluir las licencias para cubrir la cantidad de cores definido para dicho servidor. **(Absolución de consulta Nº 16)**
Características de seguridad	Debe admitir contraseña de encendido, contraseña de administrador, módulo de plataforma segura (TPM) 2.0, panel de seguridad, inicio seguro y detección de apertura de la cubierta
Temperaturas operativas	Debe soportar los rangos de: 5°C to 45°C (41°F to 113°F)
Soporte del Fabricante	Deberá contar con un soporte 24x7 por parte del fabricante, por un periodo de 36 meses ante cualquier falla.

4.Servidores Convergentes

07 Servidores convergentes -5 servidores para Sede principal y 2 sede contingencia. 02 Storage (01 Sede principal y 01 Sede Contingencia).

Servidor para Infraestructura (Sistema de Procesamiento)

Ítem	Características
Cantidad	**07 (05 Sede principal y 02 Sede de Contingencia)** **(Absolución de consulta Nº 15)**
Factor Forma	Tipo rack, 1U como máximo
Procesador	Cantidad de procesadores soportados: Mínimo 02. **Procesadores de Última generación lanzada por el fabricante de procesadores** **(Absolución de consulta Nº 18)** Número de núcleos instalados por procesador: Mínimo 16. Cantidad de subprocesos por procesador: mínimo 32 hilos Velocidad de reloj de cada procesador: Mínimo 2.3 GHz. Memoria cache por procesador: mínimo 35 MB
Memoria	DDR5 con velocidad mínima de 4800 MHz. Tipo de memoria: RDIMM Capacidad instalada: **Mínima 384 GB** **(Absolución de consulta Nº 15)**
Almacenamiento	Debe soportar distintos tipos de discos, como mínimo 8 de 2.5" Debe incluir como mínimo 2 discos SSD de 240GB en RAID1 Factor de forma: 2.5" SFF

	Los discos ofertados deben tener la capacidad de ser intercambiable en caliente (Hot Swap)
Controlador de Almacenamiento	HBA con memoria caché mínima de 4gb y soporte para RAID 0/1/10/5/50/6/60
Red LAN	Se debe incluir 4 puertos de 10/25GbE SFP+ para la LAN con sus respectivos transceivers
Red SAN	HBA de dos puertos de 16/32Gbps para SAN con sus respectivos transceivers.
Ventilación	Redundantes Hot Swap o Hot Plug. *Debe tener instalado el máximo número de ventiladores que soporte el* chasis
Fuente de energía	Deberá contar con dos fuentes de poder del tipo AC en redundancia y hot-swap, mínimo de 900W y de categoría TITANIUM
Administración	Software de administración de la misma marca del servidor, acreditada con carta del fabricante, que permita como mínimo: estado de salud del equipo y monitoreo de alertas. Debe contar con la capacidad de monitorear los componentes de hardware y software *Debe contar con la capacidad de levantar el inventario de sus* componentes Sistema de Alertas Predictivas solicitado requiere de un monitoreo automático y constante, capaz de emitir alertas (a través del software de gestión, por medio de mail, etc.) ANTES que los componentes alertados fallen. Es decir, con la capacidad de predecir futuras fallas. Acceso remoto con consola gráfica al servidor, vía GUI y/o WEB debidamente licenciada y habilitada.
Sistemas operativos Soportados	Debe soportar como mínimo: Microsoft Windows Server, SUSE Linux Enterprise Server, VMware ESXi, Red Hat Enterprise Linux, openEuler, **Se confirma, el postor podrá trabajar con Windows o un Software devirtualización, el postor deberá entregar las licencias las cuales serán perpetuas (Absolución Nº 16).**
Características de seguridad	Debe admitir contraseña de encendido, contraseña de administrador, módulo de plataforma segura (TPM) 2.0, panel de seguridad, inicio seguro y detección de apertura de la cubierta
Temperaturas operativas	Debe soportar los rangos de: 5°C to 45°C (41°F to 113°F)
Soporte del Fabricante	Deberá contar con un soporte 24x7 por parte del fabricante, por un periodo de 36 meses ante cualquier falla.

Dirección de Gestión de Procesos CENEPRED V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

Almacenamiento STORAGE SEDE PRINCIPAL

ITEM	CARACTERÍSTICAS TÉCNICAS MÍNIMAS
CANTIDAD	▪ **UNO (01)**
SISTEMA DE ALMACENAMIENTO (SAN/NAS)	▪ El sistema de almacenamiento debe ser compatible con la arquitectura activa-activa simétrica, que puede lograr una mayor confiabilidad. No se aceptará una arquitectura ALUA (Asymmetric Logical Unit Access). ▪ **El sistema de almacenamiento debe contar con características SAN/NAS, debiendo considerar como mínimo la característica de SAN, pero el sistema de almacenamiento debe soportar NAS.** (Absolución de Consultas Nº 28) ▪ Los equipos ofertados deberán contar con una arquitectura redundante. (de manera que se pueda tener visibilidad y acceso a cualquier disco/lun desde cualquier controladora/puerto de todo el sistema de almacenamiento). ▪ La solución deberá contar con una arquitectura con características de confiabilidad, disponibilidad y servicio, que permitan realizar cualquier operación de mantenimiento, cambio de ingeniería, actualización de micro-código o tareas de ampliación de cualquier componente de manera que no afecte la continuidad operativa de la solución de almacenamiento ofertada, sin costo adicional para la Entidad.
CONTROLADORAS	▪ Deberá contar con un mínimo, dos (02) controladoras SAN/NAS instaladas y configuradas en activo/activo, con puertos modulares. Debe contemplar alta disponibilidad. La controladora debe tener la capacidad de mover la data dinámicamente entre todos los controladores SAN/NAS, para balanceo de carga y redundancia ▪ El sistema deberá tener integrado el almacenamiento SAN/NAS y volúmenes virtuales (vVol) de Vmware, el cual debe estar licenciado para el total de la capacidad soportada por la solución ofertada ▪ Cada controladora debe tener conexiones redundantes hacia los gabinetes de discos. ▪ **Cada controladora debe contar un mínimo de 64 núcleos de 2.4Ghz como mínimo. Sera permitido colocar la cantidad de controladores necesarios para entregar esta capacidad de procesamiento.** (Absolución de Consultas Nº 9)
FUENTE DE PODER	▪ Redundantes.
VENTILADORES	▪ Redundantes.

DISPONIBILIDAD	▪ El equipo debe poder brindar 99.9999% de nivel de disponibilidad. ▪ Los procesos de upgrade de microcódigo del arreglo de discos debe realizarse sin interrumpir el funcionamiento ▪ Deberá soportar el reemplazo de discos y fuentes de poder en caliente. ▪ La falla de un componente no deberá comprometer la disponibilidad del sistema de almacenamiento. Se deberá garantizar el crecimiento y/o reemplazo de los componentes de manera concurrente, tales como procesamiento, memoria cache, puertos de frontend y back end, fuentes de poder y discos. ▪ Los trabajos de mantenimiento correctivo no deberán detener la operación ni la administración de la solución.
ESCALABILIDAD DE LA SOLUCIÓN DE ALMACENAMIENTO	▪ La solución debe poder escalar como mínimo **2 PiB**, los cuales deberán pertenecer al mismo clúster de controladores (no se aceptará virtualización y/o federación para estos fines). ▪ El sistema de almacenamiento deberá contar con la capacidad de redistribuir los bloques de almacenamiento dentro de un pool de almacenamiento, de tal manera que, si se agregan discos, la información se redistribuya para aprovechar los discos disponibles en el pool de la mejor manera a lo largo de todas las controladoras del sistema. ▪ La solución deberá poder escalar hasta un mínimo de 8 controladoras y/o 500 discos. ▪ La adición de discos duros a la solución dealmacenamiento debe ser sin interrupción de los servicios,el cual podrá ser de uno o varios discos a la vez.
CACHÉ	▪ El sistema de almacenamiento debe tener como mínimo **256 GB de memoria caché por controladora, nativa e instalada**; la cual, debe brindar una buena performance a nivel de IOPS y anchos de banda en el sistema total de almacenamiento de (200 TiB), antes de la compresión y deduplicación de datos (reducción de datos). El postor puede proponer una caché superior que permita la mejora de IOPS en el sistema de almacenamiento, dicha mejora debe ser sustentada con la documentación respectiva. ▪ La capacidad de memoria caché solicitada deberá ser nativa del sistema, no se aceptarán propuestas que ofrezcan capacidad en dispositivos externos virtualizados o federados por el sistema de almacenamiento ofertado. ▪ La memoria caché no debe estar basada en discos de estado sólido o flash.
BATERÍA DE RESPALDO	▪ **Una batería de respaldo en cada controlador u otro mecanismo de protección de la memoria caché, que permita preservar la información en memoria caché, en el mismo sistema de almacenamiento, en caso de falla *no planeada del fluido eléctrico.*** **(Absolución de consulta Nº 13)**
NIVELES DE RAID SOPORTADOS	▪ **Deberá soportar como mínimo RAID 5 y RAID 6. La plataforma deberásoportar el RAID de triple paridad y configurar en este tipo de arreglo.** **(Absolución de consulta Nº 5)**

CONEXIONES	▪ 16 puertos FC 32Gbps, por par de controladoras, las cuales deben ser parte de las placas de las controladoras (mínimo), habilitados y con transceivers, por solución de almacenamiento, además de contemplar el licenciamiento por todos los puertos solicitados. ▪ La totalidad de los puertos del sistema de almacenamiento deberán estar operativos en todo momento, la utilización de alguno de los puertos no debe deshabilitar el uso de otro puerto del sistema.
CONEXIONES BACK-END	▪ La tecnología back-end ofertada deberá ser NVMe PCIe o NVME over RoCE o NVMe over Infiniband o SAS 12Gbps.
ALMACENAMIENTO Y PERFORMANCE	▪ Se deberá considerar, como mínimo, lo siguiente: ○ Los 200 TiB efectivo de almacenamiento antes de la compresión y deduplicación de datos (reducción de datos) y después del RAID 6 (Ratio de reducción máxima 2:1), las cuales deberán sustentarse con carta del fabricante y se deberá visualizar su licencia. ○ **Los 200 TiB de capacidad deben ser entregados considerando un RAID de Triple Paridad con la finalidad de asegurar la disponibilidad del sistema ante la falla en simultáneo de tres discos y que los servicios no sean interrumpidos y proteger la información de la entidad.** (Absolución de consulta Nº 6) ○ La capacidad efectiva solicitada deberá ser nativadel sistema, no se aceptarán propuestas que ofrezcan capacidad en dispositivos externos virtualizado o federados por el sistema dealmacenamiento ofertado. ▪ La plataforma deberá tener una capa de discos SSD con interfaces NVMe. ▪ En caso se requieran discos adicionales para sistema operativo estos deberán considerarse adicionales a los discos solicitados. Adicionalmente, se deberá considerar incluir la cantidad de spares, de acuerdo con las mejores prácticas del fabricante. ▪ Cada sistema de almacenamiento propuesto deberá tener y alcanzar como mínimo el siguiente nivel de rendimiento para la capacidad de almacenamiento ofertada: ○ Capacidad de *240,000 IOPS*; con *70%* read / *30%* write en bloques de 8k en 1ms, en línea calculado después de la compresión y deduplicación (Considerando un Ratio 2:1), sin considerar hit ratio (Read/write). ▪ La capacidad de IOPS solicitado deberá ser sustentado con: carta de fabricante o subsidiaria local, declaración jurada del postor y con un reporte (Pantallazo) de la herramienta oficial del fabricante.
SOPORTE DE DISCOS	La solución debe soportar discos: ▪ **Discos SSD con interfaces NVMe de un tamaño máximo no mayor a 16TB, y no deberán estar basados en módulos flash.** (Absolución de Consulta Nº 7) Debe incluir licenciamiento ilimitado para la administración al total de su capacidad de crecimiento sin necesidad de licenciamiento adicional.
FUNCIONALIDADES ALMACENAMIENTO SAN	▪ Provisionamiento Virtual (ThinProvisioning). ▪ Snapshots continuos montables, escribibles y clones, la frecuencia máxima entre snapshots continuos es de hasta un máximo de 30 segundos y debe incluir el licenciamiento para el total de la capacidad soportada por el modelo del

		sistema de almacenamiento propuesto, la misma que no debe afectar su rendimiento. ▪ Replicación de datos síncrona y asíncrona. ▪ Cifrado de datos en disco físico, basado en algoritmos de encriptación presente en las controladoras del storage o en los mismos discos, para ello el postor podrá incluir los componentes necesarios (hardware y software) para su ejecución. ▪ La solución deberá soporta poder realizar una reducción de datos (compresión y deduplicación) de 02 a 01 como mínimo, y deberá incluir la licencia para el total de la capacidad soportada por el sistema de almacenamiento.
	FUNCIONALIDADES DE NAS	**El sistema de almacenamiento deberá soportar las siguientes características de NAS:** - Deberá soportar e incluir los protocolos SMBv2/v3, NFS v3/v4/v4.1, FTP, HTTP, NDMP. **Protocolos:** - CIFS/SMB: Version 2/3 incluyendo encriptación, /ABE/ABSE/Spare file. - NFS: versión 3/4/4.1. - Kerberos: SMB y NFS los cuales deberán incluir encriptación. - File blocking: SMB y NFS. - NDMP: v4 - IP Protocols: IPv4/IPv6. **Managment:** - HTTPs, SSH v2, TLS v1.2/v1.3 - SNMP (v2c, v3), SFTP, Syslog, SMTP, NTP. ▪ Deberá poder trabajar de forma simultánea con los protocolos SMB y NFS, y acceso simultáneo a un mismo archivo utilizando ambos protocolos desde distintos usuarios. ▪ Deberá incluir autentificación DNS/AD server y LDAP/NIS server. ▪ Deberá incluir realizar mapeo de roles en usuarios y deberá poder trabajar con identificadores como SID/UID/GID. ▪ Deberá incluir trabajar con ACL para clientes SMB y NFS. ▪ Deberá incluir administrar los recursos de almacenamiento para directorios, usuarios y grupos de usuarios, evitando que algunos usuarios ocupen recursos de almacenamiento excesivos, deberá poder trabajar con: - Soft Quota, para espacio utilizado y cantidad de archivos - Hard Quota: para espacio utilizado y cantidad de archivos. - Deberá poder personalizar las alarmas a nivel de porcentajes. - Deberá poder restringir el espacio máximo disponible y la cantidad de archivos permitidos para todos los archivos y subdirectorios bajo un directorio.

- Deberá permitir limitar la cantidad de recursos que puede usar un solo usuario. Las cuotas de usuarios de NAS deberán poder aplicarse a usuarios locales y de dominio (AD, LDAP y NIS). Las cuotas de usuario se pueden configurar en sistemas de archivos o árboles de directorios.
- Deberá poder generar quotas para todos los usuarios que limite la cantidad de recursos que cada usuario puede utilizar.
- Deberá poder generar quotas de grupo de usuarios que limite la cantidad total de recursos que pueden utilizar todos los usuarios de un grupo específico. Este tipo de cuota deberá poder configurar para un grupo de usuarios local o de dominio (LDAP y NIS).

▪ La plataforma deberá poder soportar con Multi-Tenant, la cual debe poder separar un sistema de almacenamiento físico en varios sistemas de almacenamiento virtual, con el fin de servir a diferentes clientes y mejorar la utilización del almacenamiento. Cada almacenamiento virtual está aislado lógicamente con sus propios sistemas de archivos, usuarios/grupos de usuarios, recursos compartidos/exportaciones y LIF (interfaz lógica) para una mejor seguridad, según el siguiente detalle:

- Cada almacenamiento virtual solo puede usar su propia tabla de enrutamiento para comunicarse con redes externas, incluidos clientes, hosts, AD, LDAP, NIS y servicios DNS.
- Los LIF se deberán poder crear a partir de puertos de enlace, puertos VLAN o puertos Ethernet. Los LIF creados a partir de diferentes tipos de puertos podrán tener características diferentes. Por ejemplo, los LIF creados a partir de puertos de enlace presentan un alto ancho de banda y alta confiabilidad, y los LIF creados a partir de puertos VLAN tienen la capacidad de aislamiento de red VLAN.
- Cada almacenamiento virtual tiene instancias de protocolo independiente, incluido SMB, NFS, iSCSI y FC.
- Los sistemas de almacenamiento deberán admitir la gestión de almacenamientos virtuales en la consola de gestión y CLI, incluida la creación, eliminación, modificación y consulta de almacenamientos virtuales.
- Al consultar a un almacenamiento virtual, se podrá obtener el estado de ejecución de almacenamientos virtuales, estadísticas de recursos de bloque (información de cantidad y capacidad de LUN), estadísticas de recursos de archivos (información de cantidad y capacidad del sistema de archivos) e información de servicio de archivos (servicio DNS, zona DNS, dominio LDAP, dominio NIS, dominio AD, servicio NDMP y dominio Kerberos).
- El sistema de almacenamiento permite que el administrador del sistema configure la protección de datos para los sistemas de archivos de almacenamientos virtuales a través de la consola de gestión y CLI, incluida la administración de instantáneas y la replicación remota de los sistemas de archivos de almacenamientos

virtuales. El administrador del sistema podrá utilizar la consola de gestión para administrar de forma centralizada los recursos en los almacenamientos virtuales y usar la CLI para administrar los recursos de forma independiente en los almacenamientos virtuales.

- El sistema de almacenamiento debe permitir a los administradores del sistema configurar servicios compartidos de NAS para almacenamientos virtuales en la consola de gestión y desde CLI, incluida la configuración de usuarios de autenticación de UNIX, usuarios de autenticación de Windows, reglas de mapeo de usuarios, recursos compartidos de NFS, recursos compartidos de CIFS, dominios AD, dominios NIS, dominios *LDAP*, servicios *DNS*, y *LIF*.
- En los escenarios de almacenamientos virtuales, el administrador del sistema tiene derechos excesivos, lo que no satisface la demanda de autogestión de los almacenamientos virtuales. El sistema de almacenamiento deberá admitir la configuración de administradores de los almacenamientos virtuales para gestionar sus propios recursos.
- Los usuarios locales y los usuarios del dominio del servicio pueden acceder a los recursos. Diferentes almacenamientos virtuales pueden tener usuarios con los mismos nombres.
- Para facilitar su uso, los roles de administrador de los almacenamientos virtuales preestablecidos deberán incluir el administrador de almacenamientos virtuales, el administrador de protocolo de almacenamientos virtuales, el administrador de protección de datos de almacenamientos virtuales, el administrador de almacenamientos virtuales WORM y el administrador de respaldo de almacenamientos virtuales NDMP. El superadministrador del sistema puede personalizar las funciones de administrador de los almacenamientos virtuales según sea necesario.

▪ *La lógica de interacción general de la gestión de servicios SAN* es la misma que la de la gestión de servicios NAS. Los almacenamientos virtuales aíslan los recursos lógicos de SAN (LUN, grupos de LUN, hosts, grupos de host, grupos de puertos, asignaciones, instantáneas, grupos de instantáneas, Hyperinstantaneas continuas, replicación remota, activo-activo de tal forma que dos equipos se puedan trabajar como si fueran uno solo y DR).

Protección:

▪ Deberá permitir la función WORM que permite que un archivo entre en el estado de protección después de que se hayan escrito los datos. Un archivo en el estado de protección se puede leer, pero no se puede eliminar, modificar ni renombrar.

▪ Las propiedades de protección se podrán agregar a los sistemas de archivos para controlar el acceso y la modificación de archivos. Cada archivo guarda sus

propias propiedades WORM, que determinan si un archivo está en estado de protección.

- Se podrá implementar las siguientes propiedades en los sistemas de archivos:
  - Período máximo de protección: el período deprotección más largo admitido por los sistemas de archivos.
  - Período de protección mínimo: el período de protección más corto admitido por los sistemas de archivos.
  - Período de protección predeterminado: período de protección predeterminado después de que los archivos ingresen al estado de protección.
  - Bloqueo automático: permite que un archivo ingrese automáticamente al estado de protección contra escritura cuando transcurre el tiempo de espera predeterminado después de un cambio.
  - Tiempo de espera predeterminado: tiempo de espera antes de que un archivo entre automáticamente en el estado de protección.
  - Eliminación automática: permite que un sistema de archivos WORM elimine archivos automáticamente después de que expire el período de protección.
  - Un archivo en estado de retención por investigación no se podrá modificar ni eliminar hasta que se borre el estado. Esta función se puede utilizar para guardar archivos sobre citaciones, litigios, investigaciones reglamentarias y otros casos especiales.

Snapshots:

- Podrá generar rápidamente una imagen coherente, es decir, un duplicado, para un sistema de archivos de origen en un momento determinado sin interrumpir los servicios que se ejecutan en el sistema de archivos de origen. Este duplicado deberá estar disponible inmediatamente después de generarse, y leer o escribir el duplicado que no afectará los datos en el sistema de archivos de origen.
- Podrá funcionar en base a sistemas de archivos ROW. En un sistema de archivos ROW, los datos nuevos o modificados no sobrescriben los datos originales, sino que se escriben en el espacio de almacenamiento recién asignado. Esto garantiza una mayor confiabilidad de los datos y una alta escalabilidad del sistema de archivos. Las imágenes basadas en ROW, podrá ser utilizado para sistemas de archivos, donde se podrá crear instantáneas en segundos. Los datos de la instantánea no ocupan ningún disco adicional espacio a menos que los archivos de origen se eliminen o modifiquen.
- Deberá poder generar snapshots continuos con un lapso de tiempo entre snap y snap de a lo mucho 30 segundos, la cual deberá estar licenciada para el total de la

		capacidad soportada por el sistema de almacenamiento ofertado. **Clonaciones:** • Deberá poder crea un sistema de archivos de clonación, que es una copia, para un sistema de archivos principal en un momento específico. Los sistemas de archivos clonados se pueden compartir con los clientes exclusivamente para cumplir con los requisitos de implementación rápida, pruebas de aplicaciones y simulacros de recuperación ante desastres. **Replicación (síncrona y asíncrona):** • Deberá poder admitir la recuperación de desastres de datos a larga distancia de los sistemas de archivos. Copiar todo el contenido de un sistema de archivos primario al sistema de archivos secundario. • Esto implementa la recuperación remota ante desastres en los centros de datos y minimiza el deterioro del rendimiento causado por la transmisión remota de datos. También se aplicará a los sistemas de archivos dentro de un sistema de almacenamiento para la recuperación de desastres de datos locales, la copia de seguridad de datos y la migración de datos.
	SOPORTE DE SISTEMAS OPERATIVOS	▪ El Sistema de Almacenamiento debe **incluir las licencias perpetuas necesarias** que permitan la conectividad total de servidores operando con sistemas operativos Windows Server, VMware, Linux RedHat, Linux.
	INTEGRACIÓN CON EL SISTEMA DE VIRTUALIZACIÓN	El almacenamiento ofertado deberá estar soportar lo siguiente: ▪ *VASA/ VAAI. VVOL.* ▪ Deberá tener un puente de comunicación entre el sistema de almacenamiento y el SRM de VMWare, el cual debe permitir que el sistema de almacenamiento coopere con SRM para crear, probar y ejecutar un plan de recuperación o una migración planificada. ▪ Al trabajar con entornos Windows, deberá poder trabajar con VSS Provider el cual proporciona interfaces estándar para la capa superior y trabaja con Veeam, Backup Exec para invocar la función de instantánea del sistema de almacenamiento para realizar copias de seguridad.

	SOFTWARE	▪ Se debe incluir el software que permita la funcionalidad de redundancia en formato activo – activo, en conectividad al arreglo de discos, de requerir una licencia esta debe incluir a la totalidad de servidores soportados por el sistema de almacenamiento, dicho software podrá ser distinto a la marca de la solución ofertada, debiendo adjuntar una carta del fabricante del software de tercero en donde asegure su compatibilidad con la solución propuesta. ▪ Se debe incluir la funcionalidad de asignar calidad de servicio (QoS) a los diferentes volúmenes creados en el storage, debe permitir priorizar el rendimiento; para que en forma automática se limite una aplicación por IOPs o ancho de banda, de modo que se reduzca el impacto sobre otras aplicaciones. Ello debe ocurrir sin la intervención de servidores externos. ▪ Deberá contemplar la Replicación Activo – Activo para NAS, según las siguientes características técnicas: a. La plataforma debe permitir a los hosts virtualizar los sistemas de archivos de dos sistemas de almacenamiento como un solo sistema de archivos en un solo sistema de almacenamiento. Además, deberá mantener lacoherencia de los datos en ambos sistemas de archivos. Los datos se leen o escriben en el sistema dealmacenamiento principal y se sincronizan con el sistema de almacenamiento secundario en tiempo real. Si el sistema de *almacenamiento principal falla, la plataforma deberá* cambiar los servicios al sistema de almacenamiento secundario, sin perder ningún dato ni interrumpir ninguna aplicación. b. Deberá brindar los siguientes beneficios: - Alta disponibilidad con protección geográfica - Gestión fácil. - Riesgo mínimo de pérdida de datos, reducción del tiempo de inactividad del sistema y rápida recuperación ante desastres. - Interrupción insignificante para los usuarios y las aplicaciones de los clientes. c. Deberá ser compatible con Fibre Channel (8 Gbit/s, 16 Gbit/s y 32 Gbit/s) y Redes IP (10GE, 25GE, 40GE y 100GE). d. Deberá poder trabajar sin un sistema Gateway. e. Con el diseño sin Gateway, las solicitudes de E/S del host no necesitan ser reenviadas por la puerta de enlace de almacenamiento, lo que evita la latencia de reenvío de E/S correspondiente y las fallas de la puerta de enlace y mejora la confiabilidad. Además, el diseño simplifica la red de alta disponibilidad (HA) entre sitios, lo que facilita el mantenimiento. f. *Esta solución deberá tener una flexibilidad limitada en la* configuración y distribución de recursos. La solución activo-activo deberá poder establecer relaciones de pares entre dos almacenamientos virtuales en diferentes sitios, implementando deduplicación en tiempo real de datos y configuraciones. Cada par de almacenamientos virtuales deberá tener un resultado de arbitraje independiente, lo

	que brinda verdaderas capacidades HA entre sitios a nivel de almacenamientos virtuales. g. La solución activo-activo también debe permitir que las aplicaciones se ejecuten de manera más eficiente en dos sitios, lo que garantiza un mejor equilibrio de carga. Un par de almacenamientos virtuales deberá incluir un almacenamiento virtual principal y un almacenamiento virtual secundario. Si cualquiera de los sistemas de almacenamiento en la solución activo-activo falla o si los enlaces que los conectan se caen, la solución activo-activo implementará el arbitraje por par de almacenamientos virtuales. Los almacenamientos virtuales emparejados deberán ser mutuamente redundantes y deberán mantener la continuidad del servicio en caso de que falle el sistema de almacenamiento.
INTEGRACIÓN	▪ Integración con Software de virtualización (VMware) y debe estar publicado en la tabla de compatibilidad del sistema de almacenamiento. ▪ Debe incluir el soporte de VMware vVols y/o Hyper V ODX y vasa y vaai. ▪ La solución de almacenamiento debe virtualizar o federar sistemas de almacenamiento heterogéneos, debiendo incluir el licenciamiento necesario.
MIGRACIÓN DE DATOS EN CALIENTE	▪ Deberá soportar la migración de datos en caliente (sin disrupción) entre sistemas de almacenamiento fuente - destino, entre distintos tipos de discos, entre distintos pools de discos o diferentes configuraciones de RAID, entre volúmenes Thin o Thick.
REPLICACIÓN LOCAL	▪ Deberá soportar la funcionalidad de replicación local, sin utilizar tiempo de CPU de los servidores. ▪ Se deberá incluir las licencias necesarias para poder generar copias locales de las LUNs que puedan ser usadas inmediatamente. ▪ Las copias locales deberán ofrecer la capacidad de ser generadas usando tecnología Local Point-in-Time (*Snapshots y Thin Clones*). *Es decir, podrán ser usadas* para recuperación a un punto específico en el tiempo, de acuerdo con la política de generación de la copia configurada y el momento al cual se quiera recuperar. ▪ Este licenciamiento deberá soportar la máxima capacidad de almacenamiento que soporte el equipo ofertado.
ALTA DISPONIBILIDAD (SAN)	▪ El sistema de almacenamiento debe tener funcionalidad de replicación asíncrona y síncrona, selectiva a nivel de volumen lógico (LUN), con licencia para todo el almacenamiento. ▪ La arquitectura SAN activo-activo permite que dos sistemas de almacenamiento centrales funcionen en modo activo-activo (los hosts pueden leer o escribir simultáneamente los mismos volúmenes activo-activo). La avería de cualquiera de los sistemas de almacenamiento no afecta a los sistemas de servicio de capa superior, con licencia para todo el almacenamiento.
LICENCIAMIENTO	El sistema debe contemplar el licenciamiento, como mínimo de lo siguiente:

Dirección de Gestión de Procesos CENEPRED V°B°

CENEPRED DGPI V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

		▪ Licenciamiento perpetuo para la conexión del total de servidores soportados operando con sistemas operativos Windows Server, VMware, Linux RedHat, Linux Centos, Linux Ubuntu y todas las versiones de Linux. ▪ Las licencias que deben incluirse son: - Licencias para la administración centralizada (SAN/NAS). - Si el CONTRATISTA precisa licenciamiento para extender la memoria del sistema, deberá contemplar el licenciamiento para un crecimiento de 100% de la memoria base solicitada, para la máxima capacidad ofertada. No se aceptará virtualización o federación para este fin. - Se deberá incluir el licenciamiento ilimitado que permita el aprovisionamiento dinámico de espacio efectivo (thin provisioning). - El postor deberá incluir el licenciamiento para realizar la réplica activo - activo para el total de la capacidad ofertada. De tal modo que, dos sistemas de almacenamiento ubicados en diferentes Data Center funcionen u operen como un solo sistema permitiendo el acceso a los volúmenes de datos (LUNs) independientemente de la ubicación en el Data Center y garantizando la disponibilidad de acceso a los datos. - El sistema de almacenamiento deberá soportar la capacidad de encriptación de los datos. ▪ Deberá soportar la capacidad de ser gestionado por claves externas.	
	HERRAMIENTAS DE ADMINISTRACIÓN	▪ Deberá consolidarse a través de un dashboard las alertas y administración del sistema para la NAS/SAN. ▪ La administración debe realizarse de manera gráfica (Web). Se debe incluir la licencia perpetua de software de administración, de interfaz gráfica. ▪ Debe estar disponible el monitoreo de rendimiento de todos los componentes del Sistema de Almacenamiento, considerando como mínimo, lo siguiente: - Monitoreo en línea del Sistema de Almacenamiento. - Capacity planning (Estimación del crecimiento de los datos SAN del Sistema de Almacenamiento). ▪ El software de administración debe estar licenciado, esta licencia debe tener la cobertura para administrar la capacidad total soportada del sistema de almacenamiento, sin limitar el número de servidores a conectar a este ni la cantidad de discos soportados. ▪ La herramienta de administración podrá ser diferente a la marca de la solución propuesta por el contratista y debe estar disponible durante la totalidad del contrato y de acceso en tiempo real para la entidad.	
	FUNCIONALIDADES DE ADMINISTRACIÓN	▪ Debe permitir definir arreglos RAID sin interrumpir el funcionamiento del sistema de almacenamiento de discos (*hace referencia que se deberá utilizar los discos físicos* entregados en el sistema de almacenamiento ofertado para poder generar el arreglo ya sea en formato distribuido o por discos). ▪ Debe permitir asignar y desasignar discos lógicos (LUNs) entre los servidores de plataforma soportada, sin interrumpir el funcionamiento del servidor de almacenamiento.	

	▪ Debe permitir expandir en línea (sin interrumpir el funcionamiento del sistema de almacenamiento de discos) la capacidad de discos lógicos (LUNs) previamente definidos. ▪ Debe permitir incrementar en línea (sin interrumpir el funcionamiento del sistema de almacenamiento) el número de discos físicos que conformen un arreglo previamente definido. ▪ Contar con una plataforma de análisis predictivo que brinde inteligencia con capacidad de predecir y prevenir problemas de infraestructura antes de que sucedan, a través de herramientas de predicción inteligente y/o inteligencia artificial. - Análisis del equipo conectada globalmente y utilizar estos datos para predecir y evitar problemas. - La plataforma deberá entregar recomendaciones preventivas sobre la administración del equipo. - Contar con capacidad de visualizar de forma remota tendencias detalladas de rendimiento, predicciones de capacidad, controles de estado. - Deberá contar con una aplicación para poder acceder al monitoreo de la solución desde cualquier parte del mundo. - Deberá poder monitorearse desde una aplicación que podrá ser instalada en un teléfono celular. ▪ Deberá contar con una plataforma para la administración, que deberá estar embebida en el sistema de almacenamiento, no deberá estar basada en una plataforma cloud.
SERVICIOS DE NOTIFICACIÓN DE EVENTOS	▪ Debe contar con la funcionalidad de notificación en forma automática (a través de internet utilizando protocolo TCP/IP) los eventos hacia el centro de soporte del fabricante y contratista. ▪ Debe soportar la asistencia proactiva, que permita configurar soporte remoto, chat en línea, apertura de tickets de servicio en forma automática.
	▪ Los componentes de la solución deberán contar con dos fuentes de alimentación de tipo AC (corriente alterna) de 100 a 240 VAC, 50/60 HZ y deben ser hotswap, sin usar transformadores.
GARANTÍA	**Deberá incluir Garantía en modalidad 24x7 con un tiempo de respuesta de 4 horas, por tres (03) años.** **(Absolución de Consulta Nº 8)**

Almacenamiento STORAGE SEDE CONTINGENCIA

ITEM	CARACTERÍSTICAS TÉCNICAS MÍNIMAS
CANTIDAD	▪ **UNO (01)**

SISTEMA DE ALMACENAMIENTO (SAN/NAS)	▪ El sistema de almacenamiento debe ser compatible con la arquitectura activa-activa simétrica, que puede lograr una mayor confiabilidad. No se aceptará una arquitectura ALUA (Asymmetric Logical Unit Access). ▪ **El sistema de almacenamiento debe contar con características SAN/NAS, debiendo considerar como mínimo la característica de SAN, pero el sistema de almacenamiento debe soportar NAS.** (Absolución de Consultas Nº 28) ▪ Los equipos ofertados deberán contar con una arquitectura redundante. (de manera que se pueda tener visibilidad y acceso a cualquier disco/lun desde cualquier controladora/puerto de todo el sistema de almacenamiento). ▪ La solución deberá contar con una arquitectura con características de confiabilidad, disponibilidad y servicio, que permitan realizar cualquier operación de mantenimiento, cambio de ingeniería, actualización de micro-código o tareas de ampliación de cualquier componente de manera que no afecte la continuidad operativa de la solución de almacenamiento ofertada, sin costo adicional para la Entidad.
CONTROLADORAS	▪ Deberá contar con un mínimo, dos (02) controladoras SAN/NAS instaladas y configuradas en activo/activo, con puertos modulares. Debe contemplar alta disponibilidad. La controladora debe tener la capacidad de mover la data dinámicamente entre todos los controladores SAN/NAS, para balanceo de carga y redundancia ▪ El sistema deberá tener integrado el almacenamiento SAN/NAS y volúmenes virtuales (vVol) de Vmware, el cual debe estar licenciado para el total de la capacidad soportada por la solución ofertada ▪ Cada controladora debe tener conexiones redundantes hacia los gabinetes de discos. ▪ **Cada controladora debe contar un mínimo de 64 núcleos de 2.4Ghz como mínimo. Sera permitido colocar la cantidad de controladores necesarios para entregar esta capacidad de procesamiento.** (Absolución de Consultas Nº 9)
FUENTE DE PODER	▪ Redundantes.
VENTILADORES	▪ Redundantes.
DISPONIBILIDAD	▪ El equipo debe poder brindar 99.9999% de nivel de disponibilidad. ▪ Los procesos de upgrade de microcódigo del arreglo de discos debe realizarse sin interrumpir el funcionamiento. ▪ Deberá soportar el reemplazo de discos y fuentes de poder en caliente. ▪ La falla de un componente no deberá comprometer la disponibilidad del sistema de almacenamiento. Se deberá garantizar el crecimiento y/o reemplazo de los componentes de manera concurrente, tales como procesamiento, memoria cache, puertos de frontend y back end, fuentes de poder y discos. ▪ Los trabajos de mantenimiento correctivo no deberán detener la operación ni la administración de la solución.

ESCALABILIDAD DE LA SOLUCIÓN DE ALMACENAMIENTO	▪ La solución debe poder escalar como mínimo **2 PiB**, los cuales deberán pertenecer al mismo clúster decontroladores (no se aceptará virtualización y/o federaciónpara estos fines). ▪ El sistema de almacenamiento deberá contar con la capacidad de redistribuir los bloques de almacenamiento dentro de un pool de almacenamiento, de tal manera que, si se agregan discos, la información se redistribuya para aprovechar los discos disponibles en el pool de la mejor manera a lo largo de todas las controladoras del sistema. ▪ La solución deberá poder escalar hasta un mínimo de 8 controladoras y/o 500 discos. ▪ La adición de discos duros a la solución dealmacenamiento debe ser sin interrupción de los servicios,el cual podrá ser de *uno o varios discos a la vez.*
CACHÉ	▪ El sistema de almacenamiento debe tener como mínimo **256 GB de memoria caché por controladora, nativa e instalada**; la cual, debe brindar una buena performance a nivel de IOPS y anchos de banda en el sistema total de almacenamiento de (200 TiB), antes de la compresión y deduplicación de datos (reducción de datos). El postor puede proponer una caché superior que permita la mejorade IOPS en el sistema de almacenamiento, dicha mejora debe ser sustentada con la documentación respectiva. ▪ La capacidad de memoria caché solicitada deberá sernativa del sistema, no se aceptarán propuestas que ofrezcan capacidad en dispositivos externos virtualizados ofederados por el sistema de almacenamiento ofertado. ▪ La memoria caché no debe estar basada en discos de estado sólido o flash.
BATERÍA DE RESPALDO	▪ **Una batería de respaldo en cada controlador u otro mecanismo de protección de la memoria caché, que permita preservar la información en memoria caché, en el mismo sistema de almacenamiento, en caso de falla no planeada del fluido eléctrico.** **(Absolución de consulta Nº 13)**
NIVELES DE RAID SOPORTADOS	▪ **Deberá soportar como mínimo RAID 5 y RAID 6.** **La plataforma deberásoportar el RAID de triple paridad y configurar en este tipo de arreglo.** **(Absolución de consulta Nº 5)**
CONEXIONES	▪ 16 puertos FC 32Gbps, por par de controladoras, las cuales deben ser parte de las placas de las controladoras (mínimo), habilitados y con transceivers, por solución de almacenamiento, además de contemplar el licenciamiento por todos los puertos solicitados. ▪ La totalidad de los puertos del sistema de almacenamiento deberán estar operativos en todo momento, la utilización de alguno de los puertos no debe deshabilitar el uso de otro puerto del sistema.
CONEXIONES BACK-END	▪ La tecnología back-end ofertada deberá ser NVMe PCIe o NVME over RoCE o NVMe over Infiniband o SAS 12Gbps.
ALMACENAMIENTO Y PERFORMANCE	▪ *Se deberá considerar, como mínimo, lo siguiente:* - 200 TiB efectivo de almacenamiento antes de lacompresión y deduplicación de datos (reducción de datos) y después del RAID 6. (Ratio de reducción máxima 2:1), las cuales deberán sustentarse con carta del fabricante y se deberá visualizar la licencia. - **Los 200TiB de capacidad deben ser entregados considerando un RAID de Triple Paridad con la finalidad de asegurar la disponibilidad del sistema ante la falla en simultáneo de tres discos y que los servicios no sean interrumpidos y proteger la información de la entidad. (Absolución de consulta Nº 6)**

	- La capacidad efectiva solicitada deberá ser nativa del sistema, no se aceptarán propuestas que ofrezcan capacidad en dispositivos externos virtualizados o federados por el sistema de almacenamiento ofertado. - La plataforma deberá tener una capa de discos SSD con interfaces NVMe. - En caso se requieran discos adicionales para sistema operativo estos deberán considerarse adicionales a los discos solicitados. Adicionalmente, se deberá considerar incluir la cantidad de spares, de acuerdo con las mejores prácticas del fabricante. - Cada sistema de almacenamiento propuesto deberá tener y alcanzar como mínimo el siguiente nivel de rendimiento para la capacidad de almacenamiento ofertada: - ***Capacidad de 240,000 IOPS; con 70% read / 30%write* en bloques de 8k en 1ms, en línea calculado después de la compresión y deduplicación (Considerando un Ratio 2:1), sinconsiderar hit ratio (Read/write).** - La capacidad de IOPS solicitado deberá ser sustentado con: carta de fabricante o subsidiaria local, declaración jurada del postor y con un reporte (Pantallazo) de la herramienta oficial del fabricante.
SOPORTE DE DISCOS	La solución debe soportar discos: ▪ **Discos SSD con interfaces NVMe de un tamaño máximo no mayor a 16TB, y no deberán estar basados en módulos flash.** (Absolucion de Consulta Nº 7). ▪ Debe incluir licenciamiento ilimitado para la administración al total de su capacidad de crecimiento sin necesidad de licenciamiento adicional.
FUNCIONALIDADES ALMACENAMIENTO SAN	▪ Provisionamiento Virtual (ThinProvisioning). ▪ Snapshots continuos montables, escribibles y clones, la frecuencia máxima entre snapshots continuos es de hasta un máximo de 30 segundos y debe incluir el licenciamiento para el total de la capacidad soportada por el modelo del sistema de almacenamiento propuesto, la misma que no debe afectar su rendimiento. ▪ Replicación de datos síncrona y asíncrona. ▪ Cifrado de datos en disco físico, basado en algoritmos de encriptación presente en las controladoras del storage o en los mismos discos, para ello el postor podrá incluir los componentes necesarios (hardware y software) para su ejecución. ▪ La solución deberá soporta poder realizar una reducción de datos (compresión y deduplicación) de 02 a 01 como mínimo, y deberá incluir la licencia para el total de la capacidad soportada por el sistema de almacenamiento.
FUNCIONALIDADES DE NAS	**El sistema de almacenamiento deberá soportar las siguientes características de NAS:** - Deberá soportar e incluir los protocolos SMBv2/v3, NFS v3/v4/v4.1, FTP, HTTP, NDMP.

Protocolos:

- CIFS/SMB: Version 2/3 incluyendo encriptación, /ABE/ABSE/Spare file.
- NFS: versión 3/4/4.1.
- Kerberos: SMB y NFS los cuales deberán incluir encriptación.
- File blocking: SMB y NFS.
- NDMP: v4
- IP Protocols: IPv4/IPv6.

Managment:

- HTTPs, SSH v2, TLS v1.2/v1.3
- SNMP (v2c, v3), SFTP, Syslog, SMTP, NTP.

▪ Deberá poder trabajar de forma simultánea con los protocolos SMB y NFS, y acceso simultáneo a un mismo archivo utilizando ambos protocolos desde distintos usuarios.
▪ Deberá incluir autentificación DNS/AD server y LDAP/NIS server.
▪ Deberá incluir realizar mapeo de roles en usuarios y deberá poder trabajar con identificadores como SID/UID/GID.
▪ Deberá incluir trabajar con ACL para clientes SMB y NFS.
▪ Deberá incluir administrar los recursos de almacenamiento para directorios, usuarios y grupos de usuarios, evitando que algunos usuarios ocupen recursos de almacenamiento excesivos, deberá poder trabajar con:
  - Soft Quota, para espacio utilizado y cantidad de archivos
  - Hard Quota: para espacio utilizado y cantidad de archivos.
  - Deberá poder personalizar las alarmas a nivel de porcentajes.
  - Deberá poder restringir el espacio máximo disponible y la cantidad de archivos permitidos para todos los archivos y subdirectorios bajo un directorio.
  - Deberá permitir limitar la cantidad de recursos que puede usar un solo usuario. Las cuotas de usuarios de NAS deberán poder aplicarse a usuarios locales y de dominio (AD, LDAP y NIS). Las cuotas de usuario se pueden configurar en sistemas de archivos o árboles de directorios.
  - Deberá poder generar quotas para todos los usuarios que limite la cantidad de recursos que cada usuario puede utilizar.
  - Deberá poder generar quotas de grupo de usuarios que limite la cantidad total de recursos que pueden utilizar todos los usuarios de un grupo específico. Este tipo de cuota deberá poder configurar para un grupo de usuarios local o de dominio (LDAP y NIS).
▪ La plataforma deberá poder soportar con Multi-Tenant, la cual debe poder separar un sistema de almacenamiento

físico en varios sistemas de almacenamiento virtual, con el fin de servir a diferentes clientes y mejorar la utilización del almacenamiento. Cada almacenamiento virtual está aislado lógicamente con sus propios sistemas de archivos, usuarios/grupos de usuarios, recursos compartidos/exportaciones y LIF (interfaz lógica) para una mejor seguridad, según el siguiente detalle:

- Cada almacenamiento virtual solo puede usar su propia tabla de enrutamiento para comunicarse con redes externas, incluidos clientes, hosts, AD, LDAP, NIS y servicios DNS.
- Los LIF se deberán poder crear a partir de puertos de enlace, puertos VLAN o puertos Ethernet. Los LIF creados a partir de diferentes tipos de puertos podrán tener características diferentes. Por ejemplo, los LIF creados a partir de puertos de enlace presentan un alto ancho de banda y alta confiabilidad, y los LIF creados a partir de puertos VLAN tienen la capacidad de aislamiento de red VLAN.
- Cada almacenamiento virtual tiene instancias de protocolo independiente, incluido SMB, NFS, iSCSI y FC.
- Los sistemas de almacenamiento deberán admitir la gestión de almacenamientos virtuales en la consola de gestión y CLI, incluida la creación, eliminación, modificación y consulta de almacenamientos virtuales.
- Al consultar a un almacenamiento virtual, se podrá obtener el estado de ejecución de almacenamientos virtuales, estadísticas de recursos de bloque (información de cantidad y capacidad de LUN), estadísticas de recursos de archivos (información de cantidad y capacidad del sistema de archivos) e información de servicio de archivos (servicio DNS, zona DNS, dominio LDAP, dominio NIS, dominio AD, servicio NDMP y dominio Kerberos).
- El sistema de almacenamiento permite que el administrador del sistema configure la protección de datos para los sistemas de archivos de almacenamientos virtuales a través de la consola de gestión y CLI, incluida la administración de instantáneas y la replicación remota de los sistemas de archivos de almacenamientos virtuales. El administrador del sistema podrá utilizar la consola de gestión para administrar de forma centralizada los recursos en los almacenamientos virtuales y usar la CLI para administrar los recursos de forma independiente en los almacenamientos virtuales.
- El sistema de almacenamiento debe permitir a los administradores del sistema configurar servicios compartidos de NAS para almacenamientos virtuales en la consola de gestión y desde CLI, incluida la configuración de usuarios de autenticación de UNIX, usuarios de autenticación de Windows, reglas de mapeo de usuarios, recursos compartidos de NFS, recursos compartidos de CIFS, dominios AD, dominios NIS, dominios LDAP, servicios DNS, y LIF.
- En los escenarios de almacenamientos virtuales, el administrador del sistema tiene derechos excesivos, lo

que no satisface la demanda de autogestión de los almacenamientos virtuales. El sistema de almacenamiento deberá admitir la configuración de administradores de los almacenamientos virtuales para gestionar sus propios recursos.

- Los usuarios locales y los usuarios del dominio del servicio pueden acceder a los recursos. Diferentes almacenamientos virtuales pueden tener usuarios con los mismos nombres.
- Para facilitar su uso, los roles de administrador de los almacenamientos virtuales preestablecidos deberán incluir el administrador de almacenamientos virtuales, el administrador de protocolo de almacenamientos virtuales, el administrador de protección de datos de almacenamientos virtuales, el administrador de almacenamientos virtuales WORM y el administrador de respaldo de almacenamientos virtuales NDMP. El superadministrador del sistema puede personalizar las funciones de administrador de los almacenamientos virtuales según sea necesario.

▪ La lógica de interacción general de la gestión de servicios SAN es la misma que la de la gestión de servicios NAS. Los almacenamientos virtuales aíslan los recursos lógicos de SAN (LUN, grupos de LUN, hosts, grupos de host, grupos de puertos, asignaciones, instantáneas, grupos de instantáneas, Hyperinstantaneas continuas, replicación remota, activo-activo de tal forma que dos equipos se puedan trabajar como si fueran uno solo y DR).

Protección:

▪ Deberá permitir la función WORM que permite que un archivo entre en el estado de protección después de que se hayan escrito los datos. Un archivo en el estado de protección se puede leer, pero no se puede eliminar, modificar ni renombrar.

▪ Las propiedades de protección se podrán agregar a los sistemas de archivos para controlar el acceso y la modificación de archivos. Cada archivo guarda sus propias propiedades WORM, que determinan si un archivo está en estado de protección.

▪ Se podrá implementar las siguientes propiedades en los sistemas de archivos:
  - Período máximo de protección: el período de protección más largo admitido por los sistemas de archivos.
  - Período de protección mínimo: el período de protección más corto admitido por los sistemas de archivos.
  - Período de protección predeterminado: período de protección predeterminado después de que los archivos ingresen al estado de protección.
  - Bloqueo automático: permite que un archivo ingrese automáticamente al estado de protección contra

escritura cuando transcurre el tiempo de espera predeterminado después de un cambio.

- Tiempo de espera predeterminado: tiempo de espera antes de que un archivo entre automáticamente en el estado de protección.
- Eliminación automática: permite que un sistema de archivos WORM elimine archivos automáticamente después de que expire el período de protección.
- Un archivo en estado de retención por investigación no se podrá modificar ni eliminar hasta que se borre el estado. Esta función se puede utilizar para guardar archivos sobre citaciones, litigios, investigaciones reglamentarias y otros casos especiales.

Snapshots:

- Podrá generar rápidamente una imagen coherente, es decir, un duplicado, para un sistema de archivos de origen en un momento determinado sin interrumpir los servicios que se ejecutan en el sistema de archivos de origen. Este duplicado deberá estar disponible inmediatamente después de generarse, y leer o escribir el duplicado que no afectará los datos en el sistema de archivos de origen.
- Podrá funcionar en base a sistemas de archivos ROW. En un sistema de archivos ROW, los datos nuevos o *modificados no sobrescriben los datos originales, sino que* se escriben en el espacio de almacenamiento recién asignado. Esto garantiza una mayor confiabilidad de los datos y una alta escalabilidad del sistema de archivos. Las imágenes basadas en ROW, podrá ser utilizado para sistemas de archivos, donde se podrá crear instantáneas en segundos. Los datos de la instantánea no ocupan ningún disco adicional espacio a menos que los archivos de origen se eliminen o modifiquen.
- Deberá poder generar snapshots continuos con un lapso de tiempo entre snap y snap de a lo mucho 30 segundos, la cual deberá estar licenciada para el total de la capacidad soportada por el sistema de almacenamiento ofertado.

Clonaciones:

- Deberá poder crea un sistema de archivos de clonación, que es una copia, para un sistema de archivos principal en un momento específico. Los sistemas de archivos clonados se pueden compartir con los clientes exclusivamente para cumplir con los requisitos de implementación rápida, pruebas de aplicaciones y simulacros de recuperación ante desastres.

Replicación (síncrona y asíncrona):

- Deberá poder admitir la recuperación de desastres de datos a larga distancia de los sistemas de archivos. Copiar todo el contenido de un sistema de archivos primario al sistema de archivos secundario.

	• Esto implementa la recuperación remota ante desastres en los centros de datos y minimiza el deterioro del rendimiento causado por la transmisión remota de datos. También se aplicará a los sistemas de archivos dentro de un sistema de almacenamiento para la recuperación de desastresde datos locales, la copia de seguridad de datos y la migraciónde datos.
SOPORTE DE SISTEMAS OPERATIVOS	▪ El Sistema de Almacenamiento debe **incluir las licencias perpetuas necesarias** que permitan la conectividad total de servidores operando con sistemas operativos Windows Server, VMware, Linux RedHat, Linux.
INTEGRACIÓN CON EL SISTEMA DE VIRTUALIZACIÓN	El almacenamiento ofertado deberá estar soportar lo siguiente: ▪ VASA/ VAAI. VVOL. ▪ Deberá tener un puente de comunicación entre el sistema de almacenamiento y el SRM de VMware, el cual debe permitir que el sistema de almacenamiento coopere con SRM para crear, probar y ejecutar un plan de recuperación o una migración planificada. ▪ Al trabajar con entornos Windows, deberá poder trabajar con VSS Provider el cual proporciona interfaces estándar para la capa superior y trabaja con Veeam, Backup Exec para invocar la función de instantánea del sistema de almacenamiento para realizar copias de seguridad.
SOFTWARE	▪ Se debe incluir el software que permita la funcionalidad de redundancia en formato activo – activo, en conectividad al arreglo de discos, de requerir una licencia esta debe incluir a la totalidad de servidores soportados por el sistema de almacenamiento, dicho software podrá ser distinto a la marca de la solución ofertada, debiendo adjuntar una carta del fabricante del software de tercero en donde asegure su compatibilidad con la solución propuesta. ▪ Se debe incluir la funcionalidad de asignar calidad de servicio (QoS) a los diferentes volúmenes creados en el storage, debe permitir priorizar el rendimiento; para que en forma automática se limite una aplicación por IOPs o ancho de banda, de modo que se reduzca el impacto sobre otras aplicaciones. Ello debe ocurrir sin la intervención de servidores externos. ▪ Deberá contemplar la Replicacion Activo – Activo para NAS, según las siguientes características técnicas: a) La plataforma debe permitir a los hosts virtualizar los sistemas de archivos de dos sistemas de almacenamientocomo un solo sistema de archivos en un solo sistema de almacenamiento. Además, deberá mantener la coherencia de los datos en ambos sistemas de archivos. Los datos se leen o escriben en el sistema de almacenamiento principal y se sincronizan con el sistema de almacenamiento secundario en tiempo real. Si el sistema de almacenamiento principal falla, la plataforma

		deberá cambiar los servicios al sistema de almacenamiento secundario, sin perder ningún dato ni interrumpir ninguna aplicación. b) Deberá brindar los siguientes beneficios: - Alta disponibilidad con protección geográfica - Gestión fácil. - Riesgo mínimo de pérdida de datos, reducción del tiempo de inactividad del sistema y rápida recuperación ante desastres. - Interrupción insignificante para los usuarios y las aplicaciones de los clientes. c) Deberá ser compatible con Fibre Channel (8 Gbit/s, 16 Gbit/s y 32 Gbit/s) y Redes IP (10GE, 25GE, 40GE y 100GE). d) Deberá poder trabajar sin un sistema Gateway. e) Con el diseño sin gateway, las solicitudes de E/S del host no necesitan ser reenviadas por la puerta de enlace de almacenamiento, lo que evita la latencia de reenvío de E/Scorrespondiente y las fallas de la puerta de enlace y mejora la confiabilidad. Además, el diseño simplifica la redde alta disponibilidad (HA) entre sitios, lo que facilita el mantenimiento. f) Esta solución deberá tener una flexibilidad limitada en la configuración y distribución de recursos. La solución activo-activo deberá poder establecer relaciones de pares entre dos almacenamientos virtuales en diferentes sitios, implementando deduplicación en tiempo real de datos y configuraciones. Cada par de almacenamientos virtuales deberá tener un resultado de arbitraje independiente, lo que brinda verdaderas capacidades HA entre sitios a nivelde almacenamientos virtuales. g) La solución activo-activo también debe permitir que las aplicaciones se ejecuten de manera más eficiente en dossitios, lo que garantiza un mejor equilibrio de carga. Un par de almacenamientos virtuales deberá incluir un almacenamiento virtual principal y un almacenamiento virtual secundario. Si cualquiera de los sistemas de almacenamiento en la solución activo-activo falla o si los enlaces que los conectan se caen, la solución activo- activo implementará el arbitraje por par de almacenamientos virtuales. Los almacenamientos virtuales emparejados deberán ser mutuamente redundantes y deberán mantener la continuidad del servicio en caso de que falle el sistema de almacenamiento.
	INTEGRACIÓN	▪ Integración con Software de virtualización (VMware) y debe estar publicado en la tabla de compatibilidad del sistema de almacenamiento. ▪ Debe incluir el soporte de VMware vVols y/o Hyper V ODX y vasa y vaai. ▪ La solución de almacenamiento debe virtualizar o federar sistemas de almacenamiento heterogéneos, debiendo incluir el licenciamiento necesario.

MIGRACIÓN DE DATOS EN CALIENTE	▪ Deberá soportar la migración de datos en caliente (sin disrupción) entre sistemas de almacenamiento fuente - destino, entre distintos tipos de discos, entre distintos pools de discos o diferentes configuraciones de RAID, entre volúmenes Thin o Thick.
REPLICACIÓN LOCAL	▪ Deberá soportar la funcionalidad de replicación local, sin utilizar tiempo de CPU de los servidores. ▪ Se deberá incluir las licencias necesarias para poder generar copias locales de las LUNs que puedan ser usadas inmediatamente. ▪ Las copias locales deberán ofrecer la capacidad de ser generadas usando tecnología Local Point-in-Time (Snapshots y Thin Clones). Es decir, podrán ser usadas para recuperación a un punto específico en el tiempo, de acuerdo con la política de generación de la copia configurada y el momento al cual se quiera recuperar. ▪ Este licenciamiento deberá soportar la máxima capacidad de almacenamiento que soporte el equipo ofertado.
ALTA DISPONIBILIDAD (SAN)	▪ El sistema de almacenamiento debe tener funcionalidad de replicación asíncrona y síncrona, selectiva a nivel de volumen lógico (LUN), con licencia para todo el almacenamiento. ▪ La arquitectura SAN activo-activo permite que dos sistemas de almacenamiento centrales funcionen en modo activo-activo (los hosts pueden leer o escribir simultáneamente los mismos volúmenes activo-activo). La avería de cualquiera de los sistemas de almacenamiento no afecta a los sistemas de servicio de capa superior, con licencia para todo el almacenamiento.
LICENCIAMIENTO	El sistema debe contemplar el licenciamiento, como mínimo de lo siguiente: ▪ Licenciamiento perpetuo para la conexión del total de servidores soportados operando con sistemas operativos Windows Server, VMware, Linux RedHat, Linux Centos, Linux Ubuntu y todas las versiones de Linux. ▪ Las licencias que deben incluirse son: - Licencias para la administración centralizada (SAN/NAS). - Si el CONTRATISTA precisa licenciamiento para extender la memoria del sistema, deberá contemplar el licenciamiento para un crecimiento de 100% de la memoria base solicitada, para la máxima capacidad ofertada. No se aceptará virtualización o federación para este fin. - Se deberá incluir el licenciamiento ilimitado que permita el aprovisionamiento dinámico de espacio efectivo (thin provisioning). - El postor deberá incluir el licenciamiento para realizar la réplica activo - activo para el total de la capacidad ofertada. De tal modo que, dos sistemas de almacenamiento ubicados en diferentes Data Center funcionen u operen como un solo sistema permitiendo el acceso a los volúmenes de datos (LUNs) independientemente de la ubicación en el Data Center y garantizando la disponibilidad de acceso a los datos. - El sistema de almacenamiento deberá soportar la capacidad de encriptación de los datos.

		▪ Deberá soportar la capacidad de ser gestionado por claves externas.
	HERRAMIENTAS DE ADMINISTRACIÓN	▪ Deberá consolidarse a través de un dashboard las alertas y administración del sistema para la NAS/SAN. ▪ La administración debe realizarse de manera gráfica (Web). Se debe incluir la licencia perpetua de software de administración, de interfaz gráfica. ▪ Debe estar disponible el monitoreo de rendimiento de todos los componentes del Sistema de Almacenamiento, considerando como mínimo, lo siguiente: - Monitoreo en línea del Sistema de Almacenamiento. - Capacity planning (Estimación del crecimiento de los datos SAN del Sistema de Almacenamiento). ▪ El software de administración debe estar licenciado, esta licencia debe tener la cobertura para administrar la capacidad total soportada del sistema de almacenamiento, sin limitar el número de servidores a conectar a este ni la cantidad de discos soportados. ▪ La herramienta de administración podrá ser diferente a la marca de la solución propuesta por el contratista y debe estar disponible durante la totalidad del contrato y de acceso en tiempo real para la entidad.
	FUNCIONALIDADES DE ADMINISTRACIÓN	▪ Debe permitir definir arreglos RAID sin interrumpir el funcionamiento del sistema de almacenamiento de discos (hace referencia que se deberá utilizar los discos físicos entregados en el sistema de almacenamiento ofertado para poder generar el arreglo ya sea en formato distribuido o por discos). ▪ Debe permitir asignar y desasignar discos lógicos (LUNs) entre los servidores de plataforma soportada, sin interrumpir el funcionamiento del servidor de almacenamiento. ▪ Debe permitir expandir en línea (sin interrumpir el funcionamiento del sistema de almacenamiento de discos) la capacidad de discos lógicos (LUNs) previamente definidos. ▪ Debe permitir incrementar en línea (sin interrumpir el funcionamiento del sistema de almacenamiento) el número de discos físicos que conformen un arreglo previamente definido. ▪ Contar con una plataforma de análisis predictivo que brinde inteligencia con capacidad de predecir y prevenir problemas de infraestructura antes de que sucedan, a través de herramientas de predicción inteligente y/o inteligencia artificial. - Análisis del equipo conectada globalmente y utilizar estos datos para predecir y evitar problemas. - La plataforma deberá entregar recomendaciones preventivas sobre la administración del equipo. - Contar con capacidad de visualizar de forma remota tendencias detalladas de rendimiento, predicciones de capacidad, controles de estado. - Deberá contar con una aplicación para poder acceder al monitoreo de la solución desde cualquier parte del mundo. - Deberá poder monitorearse desde una aplicación que podrá ser instalada en un teléfono celular.

	▪ Deberá contar con una plataforma para la administración, que deberá estar embebida en el sistema de almacenamiento, no deberá estar basada en una plataforma cloud.
SERVICIOS DE NOTIFICACIÓN DE EVENTOS	▪ Debe contar con la funcionalidad de notificación en forma automática (a través de internet utilizando protocolo TCP/IP) los eventos hacia el centro de soporte del fabricante y contratista. ▪ Debe soportar la asistencia proactiva, que permita configurar soporte remoto, chat en línea, apertura de tickets de servicio en forma automática. ▪ Los componentes de la solución deberán contar con dos fuentes de *alimentación* de tipo AC (*corriente alterna*) de 100 a 240 VAC, 50/60 HZ y deben ser hotswap, sin usar transformadores.
GARANTÍA	**Deberá incluir Garantía en modalidad 24x7 con un tiempode respuesta de 4 horas, por tres (03) años.**

5. SOFTWARE DE VIRTUALIZACION

El software de virtualización debe licenciar para todos los cores de los procesadores instalados en la solución ofertada.

El software de virtualización deberá contar con derecho a actualizaciones y soporte por tres (03) año (7x24) brindado por el fabricante del software de virtualización, una vez culminado el periodo de soporte de tres años, el software deberá mantener la capacidad operativa con todas sus funcionalidades originales habilitadas incluso sin haber renovado el soporte.

Las características mínimas que se debe considerar para proveer y configurar el Software de Virtualización para servidores o nodos, entre otras son las siguiente:

DESCRIPCION	CARACTERISTICAS
Características Técnicas mínimas del Software de Virtualización de servidores o nodos	El software de virtualización se ejecuta directamente sobre los niveles más bajos de hardware de los equipos en modo "BARE METAL" comosistema *operativo dedicado al manejo y administración de máquinas virtuales.*
	El licenciamiento perpetuo del software de virtualización debe ser para todos los servidores o nodos ofertados, contando con derecho a actualizaciones y soporte por tres (03) años (7x24) directamente con el fabricante del software de virtualización.
	Se acepta licenciamiento OEM y el soporte será brindado en todos sus niveles (Nivel 1-3) directamente por el fabricante del software virtualización.
	Debe permitir configurar máquinas virtuales en Alta Disponibilidad.
	Debe incluir el soporte para la migración de máquinas virtuales apagadas (Power off) de un servidor físico a otro tan solo indicando la acción de la máquina virtual seleccionada en la consola de administración.

	Debe incluir el soporte para la migración de máquinas virtuales en ejecución o encendidas (Power On) desde un servidor físico a otro similar, sin interrupciones para los usuarios ni pérdidas de servicio, eliminando la necesidad de planificar tiempo fuera de servicio de aplicaciones para realizar el mantenimiento planificado de los servidores.
	Debe incluir el soporte para la migración de máquinas. Permite agregar recursos de vCPU, memoria, NICS y discos a las máquinas virtuales cuando sea necesario, sin alterar la disponibilidad del servicio.
	Debe brindar disponibilidad constante de cualquier aplicación, en caso de fallas, sin pérdida de datos. Se debe entregar un sistema de HA de las VMs a nivel de Hypervisor, en caso de falla inesperada de uno de los nodos, el sistema reinicie automáticamente la máquina virtual usando la capacidad de los nodos restantes del cluster. Esta funcionalidad de HA funciona de manera automática. Debe contar con funcionalidad de tolerancia a fallas de máquinasvirtuales con hasta 8 Vcpus.
	El software de virtualización debe permitir gestionar el consumo eficiente de la energía en cada clúster o conjunto de servidores.
	El software de virtualización debe permitir la creación rápida de nuevas máquinas virtuales usando plantillas de máquinas virtuales.
	El software de virtualización debe permitir la configuración de memoria persistente para las máquinas virtuales.
	Debe permitir habilitar el control de acceso basado en funciones y/o roles.
	El software de virtualización debe permitir como mínimo los sistemas operativos: Windows Server 2016 R2 o superior; RHEL 7.x o superior.
Gestión Centralizada	Debe incluir el software de gestión centralizada que permite gestionar desde una única consola los servidores de virtualización.

Networking

SWITCH DE CORE– Cantidad 03 (02 Sede Principal y 01 Sede Contingencia) ; 04 Switchs SAN (02 sede principal y 02 sede contingencia) y 10 Switchs de acceso (08 sede principal y 02 sede contingencia).

ITEM	DESCRIPCION
CANTIDAD	3 Unidades
HARDWARE	▪ El switch debe tener un tamaño no mayor a las 10 RU. **(Absolución de consulta Nº 19)** ▪ El switch deberá ser modular. **(Absolución de consulta Nº 19)** ▪ El switchs propuesto debe proveer como mínimo 48 puertos de 10GbpsSFP+, con todos los transceivers requeridos en la presente solución.
	▪ Debe proveer puertos de uplink con capacidad de 40/100 Gbps QSFP28, con un mínimo de 4 puertos 40/100 Gbps

	▪ Debe proveer cables para Stacking de 40Gbps, mínimo de 1m
	▪ El switchs debe contar con redundancia a nivel de módulo de energía, de tipo hotswap. ▪ El Switchs debe tener al menos procesador redundante, fuentes y fan redundantes (Absolución de consulta Nº 19) ▪ El Switchs debe contar con 4 slots de servicio (Absolución de consulta Nº 19)
	▪ El switch deber contar con una capacidad de conmutación no menor a 2.16 Tbps. El switch debe tener un rendimiento de reenvió de al menos 14 Mpps (Absolución de consulta Nº 19)
	▪ Debe soportar la capacidad mínima de entradas de MAC address de 380K.
	▪ El equipo debe soportar un número total de 250K rutas en IPv4 de 80K rutas en IPv6.
	▪ Cada equipo debe poder trabajar con alimentación 100 V AC a 240 V, 50/60Hz y bajo consumo de energía.
	▪ Cada equipo debe poder operar a una temperatura de funcionamiento entre 0 °C y 45 °C.
VLAN	▪ El switchs debe soportar 4K VLANs.
	▪ El switchs debe soportar Private VLAN o similares.
	▪ El switchs debe permitir la asignación de VLAN en base a dirección MAC.
	▪ El switchs debe soportar QinQ y QinQ selectivo.
MULTICAST	▪ El equipo debe proveer soporte a escenarios de red con transporte de tráfico multicast, y soportar, como mínimo, los siguientes protocolos: PIM-DM, PIM-SM, IGMP v1/v2/v3 e IGMP snooping.
	▪ El equipo debe soportar MLD Snooping.
	▪ El equipo debe soportar la supresión de paquetes de protocolo de multidifusión
	▪ El equipo debe soportar el control de tráfico de multidifusión
ENRUTAMIENTO	▪ Debe soportar los siguientes protocolos de enrutamiento de capa 3: enrutamiento estático, RIP, RIPng, OSPF, OSPFv3, IS-IS, IS-ISv6, BGP, BGP4+, VRRP y Policy-based routing.
Proteccion Ethernet	▪ El equipo debe soportar los protocolos IEEE 802.1d STP, IEEE 802.1w RSTP y IEEE 802.1s MSTP.
	▪ El equipo debe soportar la funcionalidad para protección BPDU en puertos de acceso.
	▪ El equipo debe soportar la funcionalidad para protección de root y protección contra loops.
QoS	▪ Soporte de modificación de la prioridad de los paquetes.

	▪ Manejo de ocho colas en cada puerto.
	▪ El switch debe soportar, como mínimo, los siguientes algoritmos de programación de colas: Priority Queuing (PQ), Weighted Deficit Round Robin (WDRR) y PQ + WDRR.
	▪ Debe soportar WRED.
	▪ Soporte de remarcado de la prioridad 802.1p.
	▪ Soporte de clasificaciones trafico basado en encabezados desde la capa 2 hasta la capa 4.
	▪ Soporte de listas de control de acceso en IPv4 y en IPv6.
	▪ Soporte de listas de control de acceso en capa 2.
	▪ Soporte de traffic shaping.
FUNCIONALIDADES COMPLEMENTARIAS	▪ El equipo debe soportar la defensa contra ataques DoS, ataques de inundación SYN del protocolo de control de transmisión (TCP), ataques de inundación del protocolo de datagramas de usuario (UDP), tormentas de transmisión.
	▪ El equipo debe soportar protocolo de autenticación vía IEEE 802.1x, RADIUS y TACACS o similares.
	▪ Debe soportar aprendizaje automático de MAC address y envejecimiento de MAC address.
	▪ Debe soportar entradas de MAC address estática, dinámica y blackhole.
	▪ Debe soportar limitación de aprendizaje de MAC address por interfaz.
	▪ El switch debe soportar protocolos de tipo IP flow como sFlow, Netflow o similares.
	▪ El equipo debe soportar BFD para BGP, BFD para IS-IS, BFD para OSFP y BFD para rutas estáticas.
	▪ El equipo debe soportar el protocolo G.8032.
	▪ El equipo debe soportar funciones VXLAN, gateways VXLAN, así como BGP EVPN.
	▪ El equipo debe soportar configuraciones VXLANusando NETCONF/YANG.
	▪ El equipo debe soportar la asociación entre los protocolos IEEE 802.1ag
	▪ El equipo debe soportar protocolos de gestión SNMP v1/v2c/v3.
	▪ El equipo debe soportar gestión basada en web.
	▪ El equipo debe soportar gestión y configuración remota a través de Telnet.
	▪ El equipo debe soportar protocolo SSHv2 para administración remota.
	▪ El equipo debe soportar RMON.

SWITCHS SAN – Cantidad 04 (02 Sede Principal HA- 02 Sede Contingencia HA) (Absolución de consulta Nº 19)

DETALLE	ESPECIFICACIÓN
CANTIDAD	• 04 unidades (Absolución de consulta Nº 20)
MONTAJE	• Debe contar con todos los accesorios para montaje y operación en rack estándar de 19".
VENTILADORES	• Redundantes
FUENTE Y ALIMENTACIÓN.	• Debe operar entre 200-240 VAC y a una frecuencia entre 50-60 Hz.
	• **Se debe incluir mínimo una fuente de poder.** (Absolución de consulta Nº 21)
	• Se deben suministrar todos los cables de conexionado eléctrico.
	• En caso de que el tipo de conexionado no sea compatible con el existente en los gabinetes disponibles, será de cargo del oferente le cambio de los cables de conexionado eléctrico o el suministro de las PDU requeridas.
LICENCIAMIENTO	• El licenciamiento provisto debe ser perpetuo.
	• Debe incluir 24 puertos licenciados y habilitados
TRANSCEIVERS y PUERTOS	• 24 puertos de 32Gb que soporte velocidades de 8, 16 y 32Gbps con conector LC, multimodo.
	• *01 puerto de gestión Ethernet - RJ-45 10/100/1000Mbps.*
	• 01 puerto serial
	• 01 puerto USB.
	• Todos los puertos solicitados deben estar habilitados y disponibles para su uso inmediato sin costo adicional para la entidad. • Asimismo, debe incluir el licenciamiento, accesorios y transceivers para los puertos solicitados.
SERVICIOS DEL SWITCH	• Funcionalidad completa de switch fibra canal o full fabric.
	• **La plataforma deberá poder trabajar en: modo Full Fabric y/o Funcionalidad de crear y/o unirse a unfabric.** (Absolución de Consulta Nº 22)
	• Access Gateway.
ANCHO DE BANDA AGREGADO	• **Deberá contar con un mínimo de 768Gbps.** (Absolución de Consulta N°23)
TIPOS DE PUERTOS SOPORTADOS	• F_Port, E_Port, D_Port en los 24 ports o equivalentes.
	• Modo Access Gateway: F_Port enabled N_Port
ADMINISTRACIÓN	• HTTP, SNMP v1 / v3 (FE MIB, FC Management MIB), SSH; Auditoría, Syslog; Herramientas web avanzadas; Interfaz de línea de comandos (CLI); Compatible con SMI-S.

SWITCHS DE ACCESO PoE : Cantidad 10 (8 sede principal, 2 sede contingencia)

ATRIBUTO	CARACTERÍSTICAS TÉCNICAS MINIMAS
HARDWARE	Unidades de rack: 01 RU

	Cantidad de puertos (interfaces) instaladas y operativas fijas o a través de módulos 24 Ethernet 100/1000 PoE, + 4x10G SFP+
	Debe contar con puertos físicos para Administración, Gestión y configuración del equipo: Conexión serial, RJ45 y/o puerto USB.
	Memoria mínima de 512 MB de CPU o RAM o DRAM o SDRAM
	VLAN's: 4,000
	Direcciones MAC: 32,000
	Tasa de reenvío: 96 Mbps
	Capacidad del Switch: 128 Gbps
	Fuente de alimentación: 220 VAC
	Capaz de operar en capa 2 y capa 3
FUNCIONALIDADES DE RED	Soporta IPv4 e IPv6 SNMP v3
	Soporta IEEE 802.1s, IEE 802.1w, IEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3ad
	Soporta OSPF, RMON (Remote Network Monitoring), QoS
IPv6	Soporte de IPv6
MECANISMOS DE SEGURIDAD	Protección con usuarios y contraseñas de acceso
	Soporta ARP
	Soporta Multicast
	Soporta ACL
SOFTWARE	Toda funcionalidad de software, establecida para el funcionamiento del switch de red deberá contar con el respectivo licenciamiento y la capacidad de actualizarse sin incurrir en costos adicionales para el Proyecto
	Deberá tener un sistema operativo dedicado y desarrollado por el fabricante para tal equipamiento, no se aceptarán versiones de software como GNU/Linux, BSD, SUN, Solaris, Microsoft Windows, Apple OSX, etc., adaptadas
CONSIDERACIONES ADICIONALES	El contratista deberá considerar, de ser el caso, todos los componentes, accesorios, licenciamiento para la configuración del equipo. Todos los puertos de fibra deberán estar licenciados para su utilización
	El equipo deberá quedar preparado para la habilitación del protocolo IPv6

Dirección de Gestión de Procesos CENEPRED V°B°

CENEPRED/DGP

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

	Cada equipo deberá ser nuevo y de primer uso
	Deberán ser equipos vigentes en el mercado, no ser remanufacturados, ni estar en la lista de End of Life del fabricante
SERVICIO	Montaje, instalación y configuración de VLANs del switch de borde será realizado por el contratista en coordinación con el encargado de Tecnología. Incluye la realización de las configuraciones de seguridad y aquellas recomendadas por buenas prácticas del fabricante

FIREWALL DE SEGURIDAD PERIMETRAL

Cantidad 03 (2 en HA Sede Principal y 1 en Sede Contingencia)

- Integra firewall, VPN, prevención de intrusiones, antivirus, administración de ancho de banda, Anti-DDoS, filtrado de URL; proporciona una vista de configuración global; administra políticas de manera unificada.
- Identifica más de 6000 aplicaciones y admite la granularidad del control de acceso hasta las funciones de la aplicación; combina la identificación de aplicaciones con detección de intrusos, antivirus y filtrado de datos, lo que mejora el rendimiento y la precisión de la detección.
- Controla las aplicaciones empresariales en la nube de una manera refinada y diferenciada para cumplir con los requisitos de las empresas para la gestión de aplicaciones en la nube.
- Obtiene la información más reciente sobre amenazas de manera oportuna para una detección precisa y defensa contra ataques basados en vulnerabilidades. Soporta cobertura de decenas de miles de vulnerabilidades y exposiciones comunes (CVE).Detecta tráfico malicioso, como tráfico de ataques de vulnerabilidad, tráfico de ataques web(como inyección SQL y ataques de scripting entre sitios), botnets, control remoto, y troyanos, y es compatible con la detección de ataques de fuerza bruta. Soporta firmas definidas por el usuario. Admite la detección de agrietamiento por fuerza bruta basada en el comportamiento del usuario y en períodos estadísticos definidos por el usuario.
- El soporte detecta el tráfico de Botnet mediante el uso de la función de protección de prevención de intrusiones.
- Soporta un motor antivirus inteligente que puede detectar cientos de millones de variantes de virus.
- El soporte utiliza el motor antivirus para detectar software espía.
- Gestiona el ancho de banda por usuario y por IP basado en la identificación de aplicaciones de servicio, asegurando la experiencia de red de los servicios y usuarios clave. La gestión y el control pueden implementarse limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y cambiando la prioridad de reenvío de la aplicación.
- Proporciona una base de datos de categorías de URL con más de 140 millones de URLs y acelera el acceso a categorías específicas de sitios web, mejorando la experiencia de acceso de sitios web de alta prioridad. Admite el filtrado DNS, en el que las páginas web a las que se accede se filtran en función de los nombres de dominio.
- Admite el filtro de URL antiphishing.
- Soporta la función SafeSearch para filtrar recursos de motores de búsqueda, como Google, para garantizar el acceso solo a recursos de red saludables.

- Soporta PBR específico de servicio y selección de enlace ascendente inteligente basada en múltiples algoritmos de equilibrio de carga en escenarios de múltiples salidas.
- Soporta múltiples funciones VPN de alta disponibilidad, como IPsec VPN, SSL VPN y GRE.
- Soporta la virtualización de múltiples tipos de servicios de seguridad, incluyendo firewall,
- Prevención de intrusiones, antivirus y VPN. Los usuarios pueden realizar por separado la gestión personal en el mismo dispositivo físico.
- Gestiona y controla el tráfico basado en ID de VLAN, quintuples, zonas de seguridad, regiones, aplicaciones, categorías de URL y rangos de tiempo, e implementa la detección de seguridad de contenido integrada.
- Proporciona plantillas de defensa de escenario común predefinidas para facilitar la implementación de políticas de seguridad.
- Proporciona soluciones de gestión de políticas de seguridad en asociación con FireMon y AlgoSec para reducir los costos de operación y mantenimiento y posibles fallos.
- Soporta múltiples tipos de protocolos y características de enrutamiento, como RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+ e IPv6 IS-IS.
- Admite modos de trabajo transparentes, de enrutamiento e híbridos y alta disponibilidad (HA), incluidos los modos Activo/Activo y Activo/En espera.
- Rendimiento del firewall1 (1518/512/64 bytes, UDP) de 100/100/60 Gbit/s
- Latencia del firewall (64 bytes, UDP) de 35 µs
- Sesiones Concurrentes de 30,000,000
- Nuevas sesiones/Segunda de 1,000,000
- FW + SA* Rendimiento de 45 Gbps
- Rendimiento NGFW de 30 Gbps
- Rendimiento de protección contra amenazas de 14 Gbps
- Rendimiento IPsec VPN de 40 Gbps
- Rendimiento VPN SSL de 10 Gbps
- Usuarios VPN SSL simultáneos de 10000, máximo
- Políticas de seguridad de 60000
- Firewalls virtuales de 1000
- Filtrado de URL: al menos 130 Categorías
- Retroalimentación automatizada de amenazas y actualizaciones de firmas IPS
- 4094 VLAN
- VLAN de interfaz 1024
- Interfaces fijas: 2 × 100GE (QSFP28) + 2 × 40G (QSFP+) + 8 × 25 (ZSFP+) + 20 × 10GE (SFP+)
- Factor de forma: 1 RU
- Fuentes de alimentación de CA dual
- Fuente redundantes
- Debe incluir una memoria interna SSD mínimo de 240GB.
- La configuración centralizada, el registro, el monitoreo y la generación de informes son obligatorios

Instalación y Configuración:

La entidad brindara la ubicación donde se instalarán las soluciones solicitadas.

- Los datos y especificaciones de red necesarias para la configuración de la solución.
- Las facilidades e información pertinente para el ingreso, traslado y ubicación del equipamiento ofertado.

- El proveedor será responsable de la instalación, configuración y puesta en marcha del equipamiento ofertado, interconectar los componentes, configurar todos los componentes necesarios para dicho fin.
- El proveedor será responsable de la puesta en marcha y pruebas de la operatividad de la solución.
- El proveedor será responsable de la implementación y del rackeado y conexionado de la solución, para ello la entidad deberá garantizar el ambiente y condiciones eléctricas y de comunicación de red de la solución.
- CENEPRED será responsable de la comunicación de los componentes que requieran conectividad de la solución ofertada con la red LAN y acceso a Internet.
- El Proveedor efectuará la configuración y parametrización de los dispositivos y sistemas adquiridos, de acuerdo a:
- Las políticas de seguridad establecidas por CENEPRED.
- Las mejores prácticas establecidas para estos casos.
- El Proveedor documentará de manera exhaustiva los procesos de instalación de cada uno de los elementos de la solución ofertada, incluyendo los parámetros, descripciones y esquemas de configuración dispuestos para su normal operación.
- El Proveedor establecerá y documentará adecuadamente los procedimientos de gestión técnica necesarios para la efectiva administración de cada uno de los componentes de la solución ofertada.

Mantenimiento y Soporte:

A continuación, se detallan las condiciones y característica del mantenimiento y soporte:

- El proveedor deberá interconectar la solución multimedia mediante una VPN (Virtual Private Network o Conexión segura) a su local central de atenciones, para ello coordinará con CENEPRED para que le brinden las facilidades técnicas e infraestructura necesaria para lograr dicho objetivo.
- El proveedor deberá ofrecer soporte y mantenimiento 24x7 durante la duración del contrato.
- El proveedor será responsable del soporte y mantenimiento de la infraestructura adquirida, así como de la operatividad de los componentes de la solución.
- La entidad podrá generar un ticket de atención vía telefónica y/o correo electrónico, la cual tendrá que ser atendido de acuerdo a como se indica a continuación:
- **Falla Menor:** Entiéndase por falla menor a la indisponibilidad de algún componente que no afecte ningún servicio crítico en las soluciones proveídas
- Solución del problema de falla menor: 48 horas como máximo, contabilizado desde que se crea el reporte de avería o se active la alarma del software de monitoreo (lo primero que ocurra). De excederse el tiempo indicado para solucionar un problema, el tiempo de exceso será considerado para el cálculo de penalidades.
- **Falla mayor**: Entiéndase por falla mayor a la indisponibilidad de algún componente que afecte a uno o más componentes básicos.
    - Solución del problema de falla mayor: 08 horas como máximo, contabilizado desde que se crea el reporte de avería o se active la alarma por el software de monitoreo (lo primero que ocurra). De excederse el tiempo indicado para solucionar un problema.

V. REQUISITOS DEL POSTOR

DOCUMENTACIÓN DEL POSTOR

- **El postor deberá presentar en su propuesta técnica una carta del fabricante y/o subsidiaria en el país en la cual indique que puede comercializar equipamiento y servicios en el territorio peruano en el equipamiento de Datacenter y/o switchs core y/o acceso y/o almacenamiento.** Absolución de Consulta Nº 32).

- El postor deberá contar con un sistema de generación de tickets y central telefónica 0800 disponible para las atenciones de las incidencias 24x7, para ello deberá presentar en su propuesta técnica imágenes de la plataforma de generación de tickets así como link de acceso, copia del recibo de servicio de 0800 e indicar número del servicio, la entidad se encuentra en la potestad de realizar las pruebas inopinadas de lo presentado

- El postor deberá contar con un sistema de reportes de incidencias que se pueda visualizar en los sistemas operativos Android y iOS y deberá ser instalada en los teléfonos celulares que el cliente disponga, para ello el postor deberá presentar en su propuesta técnica imágenes del sistema de reportes de incidencias en los sistemas operativos Android y iOS indicando el nombre de la aplicación, la entidad se encuentra en la potestad de realizar las pruebas inopinadas de lo presentado

- El postor deberá contar con un local central de atenciones propio, en donde se visualice el estado y alertas de los equipos de la solución en un Video Wall mínimo de 3x2, para ello el postor deberá presentar en su propuesta técnica copia de recibo de servicios del local, copia de certificado de licencia municipal de funcionamiento, fotos del videowall, la entidad se encuentra en la potestad de realizar las pruebas y visita inopinadas de lo presentado.

- El postor deberá contar con una software de mantenimiento de activos en Cloud, dicho software de mantenimiento podrá generar ordenes de trabajo, También deberá tener la Capacidad de generar historial por cada activo de la solución, la herramienta permitirá subir documentos adjuntos como fotos e instructivos, la entidad podrá tener acceso al control y seguimiento de las ordenes de trabajo y para la conformidad de cada orden de trabajo deberá permitir la revisión y conformidad digitalmente mediante firma en línea, la herramienta deberá tener la capacidad de leer QR y NFC, la herramienta deberá tener la Capacidad de accesar vía celular (android y IOs), tablet, y estaciones de trabajo, deberá contar con la capacidad de integrarse mediante API`s a otros sistemas externos o ERPs, para ello deberá presentar como sustento en su propuesta técnica, copia de la licencia a nombre del postor y/o carta del fabricante y/o carta del parthner y/o la subsidiaria en el país en donde consigne que el postor tiene utiliza el software para la gestión de activos en donde también se avalen las características indicadas

VI. REQUISITOS DE CALIFICACIÓN

A) CAPACIDAD LEGAL:

Representación:

- Documento que acredite fehacientemente la representación de quien suscribe la oferta. En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda.

- El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades.

Acreditación:

- Tratándose de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto, expedido por registros públicos con una antigüedad no mayor de treinta (30) días calendario a la presentación de ofertas, computada desde la fecha de emisión.
- En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda, expedido por registros públicos con una antigüedad no mayor de treinta (30) días calendario a la presentación de ofertas, computada desde la fecha de emisión.

B) EXPERIENCIA DEL POSTOR

El postor deberá demostrar un histórico de facturación acumulada equivalente a S/. 14,000,000.00 (CATORCE MILLONES CON 00/100) por la comercialización de bienes idénticos o similares al objeto de esta convocatoria. Este historial se calculará retrospectivamente durante un período de ocho (8) años anteriores a la fecha de presentación de las ofertas, tomando en consideración la fecha de emisión de conformidades o comprobantes de pago, según corresponda.

Se consideran bienes similares a los siguientes: **Suministro y/o Implementación de centros de Datos y/o Microdatacenter y/o Gabinetes Autocontenidos y/o UPS y/o Aires Acondicionados de Precisión y/o Servidores y/o Sistemas de Almacenamiento.**

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuyacancelación 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[35] 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 solo se considerará, para la evaluación, las veinte (20) primeras contrataciones referidas a la Experiencia del Postor en la Especialidad.

En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes depago 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.

C) CAPACIDAD TÉCNICA Y PROFESIONAL

Un (01) Especialista en Soluciones de Datacenter

Formación Académica

- Ingeniero electrónico o sistemas, titulado, habilitado por el Colegio de Ingenieros del Perú

Certificaciones

- Certificado de Consultor de Diseñador por TIA 942.
- Certificación de diseñador de Centro de Datos, ATD de UPTIME INSTITUTE
- Certificación de especialista de Centro de Datos, DCS de Diseño de DCPRO/ DATACENTER DYNAMICS.
- Certificación de diseñador de Centro de Datos, CCRD de ICREA.
- Certificado de profesional en Centro de Datos o Data Center o Centro de Cómputo.

Experiencia

- Contar con experiencia mínima de cuatro (04) años, como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador en actividades relacionadas a la consultoría, diseño, supervisor de Centro de Datos (Data Center) y las Soluciones de Tecnología de Información y comunicaciones. Se deberá adjuntar las constancias de la experiencia.

Dirección de Gestión de Procesos CENAGRED V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMATICA V°B°

- Experiencia en haber participado como mínimo en tres (03) Servicios de Ingeniería o Diagnostico Situacional o Supervisiones o Acondicionamiento o Instalaciones de Centro de Datos o Data Center o Centro de Computo, en los últimos años. Se deberá adjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad.

Un (01) Especialista en UPS y AAP

Formación Académica

- Formación: Ing. Electrónico o electricista, titulado, habilitado por el Colegio de Ingenieros del Perú.

Certificaciones

- Certificación en Implementación de Datacenter Oficial técnica vigente (no venta, no preventa) emitido por el fabricante de Datacenter ofertado.

Experiencia

- Experiencia no menor de 5 años como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador de instalaciones de UPS y AAP. Se deberá adjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad.

Un (1) Especialista en Infraestructura

Formación Académica:

- Profesional Bachiller o Titulado en Ingeniería: Electrónica y/o Informática y/o Sistemas y/o Computación e Informática y/o Redes y Comunicación de Datos y/o Industrial y/o Sistemas e informática y/o Redes y Comunicaciones y/o Empresarial y de sistemas y/o Ciencias de la Computación y/o Electrónica de Sistemas Computarizado y/o Ingeniería de Telecomunicaciones.

Certificación:

- Certificación Oficial técnica (no venta, no preventa) nivel Asociado y/o profesional de servidores emitida por el fabricante de la marca de servidores
- Certificación Oficial técnica (no venta, no preventa) de implementación y/o instalación y/o administración y/o profesional de almacenamiento emitida por el fabricante en la marca de almacenamiento ofertados
- Certificación Oficial Técnica (no venta, no preventa) de implementación y/o instalación y/o administración y/o Profesional en Switches SAN emitida por elfabricante en la marca del equipamiento ofertado y/o Brocade o similar.

Experiencia:

- Tres (3) años mínimo como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador en implementación y/o soporte y/o administración de Infraestructura TI. Se deberá adjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad.

Un (1) Especialista en Networking

Formación Académica:

- Profesional Bachiller o Titulado en Ingeniería: Electrónica y/o informática y/o Sistemas y/o Computación e Informática y/o Redes y Comunicación de Datos y/o Industrial y/o Sistemas e Informática y/o Redes y Comunicaciones y/o Empresarial y de sistemas y/o Ciencias de la Computación y/o Electrónica de Sistemas Computarizado y/o Ingeniería de Telecomunicaciones.

Certificación:

- Certificación Oficial técnica (no venta, no prevente) en Networking y/o Datacom y/o Switching emitida por el fabricante del equipamiento de comunicaciones ofertado.

Experiencia:

- Dos (2) años mínimo como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador en administración y/o implementación y/o soporte de soluciones de Networking. Se deberá adjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad.

Dos (2) Especialista en Virtualización

Formación Académica

- Titulado o Bachiller en Ingeniería: Electrónica y/o Informática y/o Sistemas y/o Computación e Informática y/o Redes y Comunicación de Datos y/o Industrial y/o Sistemas e Informática y/o Redes y Comunicaciones y/o Empresarial y de sistemas y/o Ciencias de la Computación y/o Electrónica de Sistemas Computarizado y/o Ingeniería de Telecomunicaciones.

Capacitación

- Certificación Oficial técnica (no venta, no preventa) no mayor a 03 años de instalación y/o implementación y/o profesional de virtualización de Centro de Datos emitida por el fabricante del Software de Virtualización ofertado.
- Certificación Oficial técnica (no venta, no preventa) no mayor a 03 años de instalación y/o implementación y/o profesional de virtualización de redes emitida por el fabricante del software de virtualización.
- Certificación Oficial técnica en HCI emitida por el fabricante del software de virtualización ofertado. *

*Se aceptará Badge oficial siempre y cuando se adjunte en la propuesta el transcript con Link público emitido por el fabricante evidenciando la especialización del profesional en HCI.

Experiencia

- Cinco (5) años como mínimo como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador y/o administración de soluciones Virtualización.

VII. SISTEMA Y MODALIDAD DE CONTRATACIÓN

- Sistema de contratación SUMA ALZADA
- Modalidades de contratación LLAVE EN MANO

VIII. LUGAR Y PLAZO DE EJECUCIÓN

Prestación Principal

Dirección de Gestión de Procesos CENEPRED V°B°

CENEPRED V°B°

Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

Lugar de entrega: Los bienes y el servicio serán entregados y ejecutados respectivamente en la sede del CENEPRED, sito en avenida parque norte 313-319, San Isidro. El lugar de entrega podrá ser modificado previa comunicación oportuna de la entidad

Plazos:
La entrega del Equipamiento tendrá un plazo máximo hasta noventa y cinco (95) días calendario a partir del día siguiente de suscrito el contrato.

Prestación accesoria:

Mantenimiento:
Mantenimiento anual y soporte técnico durante 36 meses a partir de la conformidad brindada por CENEPRED de la instalación, configuración y puesta en marcha.

Capacitación:
Infraestructura de la solución, 8 horas, para 5 personas certificado.
Solución de almacenamiento Storage, 8 horas, para 5 personas certificado.
Solución de Backup, 8 horas, para 5 personas certificado.

Migración de la data
Se efectuará la migración de toda la data relacionada al SIGRID y aplicaciones geoespaciales del(los) servidores actuales al nuevo Data Center.

IX. ENTREGABLES

Primer entregable: El cual consiste en el Plan de Trabajo en formato digital, deberá ser presentado en un plazo máximo de cinco (5) días calendario a partir de la firma del contrato.

Segundo Entregable: La entrega de los bienes de infraestructura de los gabinetes Autocontenidos para el Datacenter principal y el Datacenter de Contingencia deberá realizarse en un plazo máximo de quince (15) días calendario a partir de la firma del contrato.

Tercer Entregable: La entrega de los bienes correspondientes a la Solución de Backup, Servidores Convergentes, Networking, Firewall de Protección Perimetral y Plataforma de Virtualización deberá efectuarse en un **plazo máximo de sesenta (60) días calendario a partir de la firma del contrato.** Absolución de Consulta Nº 27).

Cuarto Entregable: La instalación, configuración, puesta en marcha y capacitación del equipamiento deberán completarse en un plazo máximo de ochenta y cinco (85) días calendario a partir de la firma del contrato.

Entregable final: La documentación técnica en formato digital, que debe incluir el inventario del equipamiento, los procedimientos de instalación y configuración de los equipos y los diagramas de conectividad, deberá entregarse en un plazo máximo de noventa y cinco (95) días calendario a partir de la firma del contrato.

X. CONFORMIDAD

La conformidad, por cada entregable, será otorgada por la Dirección de Gestión de Procesos previo informe del Especialista en Informática de la Oficina de Administración del CENEPRED, el cual contendrá el inventario de todos los bienes entregados por el proveedor (incluido licencias), características técnicas de cada bien y licencias, claves de acceso a los servidores, códigos de activación de licencias.

La conformidad final contendrá las pruebas de funcionamiento y confirmación de la operatividad del Datacenter principal y secundario.

Asimismo, previo al informe y/o acta de recepción conforme de los bienes entregados, tanto del Datacenter principal como secundario y componentes respectivos, elaborado por el Especialista en Control Patrimonial de la Oficina de Administración.

XI. FORMA Y CONDICIONES DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGO ÚNICO EN FUNCIÓN AL MONTO DEL CONTRATO ORIGINAL, previo otorgamiento de una garantía por el mismo monto del pago; para lo cual la Oficina de Administración, a través de su especialista en tesorería o la que haga sus veces, otorgan la conformidad a la GARANTIA presentada por el contratista para tal fin.
La garantía presentada por el contratista tendrá una vigencia comprendida durante la ejecución del servicio hasta la conformidad del mismo.
La garantía debe cumplir las características y condiciones que la normativa ya ha contemplado, de modo que la Entidad pueda ejecutarla en caso de incumplimiento del proveedor

XII. CONFIDENCIALIDAD

Como parte del servicio, el proveedor pudiera tomar conocimiento de la plataforma tecnológica y de los sistemas de información del CENEPRED, si este fuera el caso, esta información es reservada, por lo tanto, el proveedor y todo su personal deberá mantener la confidencialidad de la misma.

El compromiso de confidencialidad se prolonga indefinidamente aun después de terminado el proyecto y se hace extensivo al personal del proveedor aun cuando ellos hayan dejado de tener vínculo laboral con este.

XIII. RESPONSABILIDAD DEL PROVEEDOR

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada por la Entidad.

XIV. RESPONSABILIDAD POR LA ASIGNACIÓN DE BIENES

En virtud de lo dispuesto en los artículos 11 y 18 de la Ley Nro. 29151 –Ley General del Sistema Nacional de Bienes Estatales, en aquellos casos en los cuales, para el cumplimiento de la prestación, la Entidad asigne al Proveedor algún bien mueble o inmueble, éste será responsable del buen uso y conservación de los mismos; de lo contrario, responderá por su deterioro o pérdida, debiendo proceder a su reposición dentro del plazo máximo de cinco (5) días hábiles.

XV. PENALIDADES

Penalidad por Mora en la ejecución de la prestación:
En caso de retraso injustificado del proveedor en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso. 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 tiene 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 y consultorías: F = 0.25.
   b.2) Para obras: F = 0.15

Tanto el monto como el plazo se refieren, según corresponda, a la ejecución total del servicio o a la obligación parcial, de ser el caso, que fuera materia de retraso.

Se considera justificado el retraso, cuando el proveedor acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.

Esta calificación del retraso como justificado no da lugar al pago de gastos generales de ningún tipo.

Dirección de Gestión de Procesos CENEPRED V°B°

CENEPRED I DGP V°B°

Centro Nacional de Estimación Prevención y Reducción del Riesgo de Desastres INFORMÁTICA V°B°

3.2. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	<u>Requisitos</u>: Documento que acredite fehacientemente la representación de quien suscribe la oferta. En el caso de consorcios, este documento debe ser presentado por cada uno de los integrantes del consorcio que suscriba la promesa de consorcio, según corresponda. En representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades. <u>Acreditación</u>: Tratándose de persona jurídica, copia del certificado de vigencia de poder del representante legal, apoderado o mandatario designado para tal efecto, expedido por registros públicos con una antigüedad no mayor de treinta (30) días calendario a la presentación de ofertas computada desde la fecha de emisión. En caso de persona natural, copia del documento nacional de identidad o documento análogo, o del certificado de vigencia de poder otorgado por persona natural, del apoderado o mandatario, según corresponda, expedido por registros públicos con una antigüedad no mayor de treinta (30) días calendario a la presentación de ofertas, computada desde la fecha de emisión.

B	EXPERIENCIA DEL POSTOR
	<u>Requisitos</u>: El postor debe acreditar un monto facturado acumulado equivalente a S/14’000,000.00 (Catorce millones con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) 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 bienes similares a los siguientes Suministro y/o Implementación de centros de Datos y/o Microdatacenter y/o Gabinetes Autocontenidos y/o UPS y/o Aires Acondicionados de Precisión y/o Servidores y/o Sistemas de Almacenamiento. <u>Acreditación</u>: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, 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[6], 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 solo 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.

[6] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

> *“… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado”*
> *(…)*
> *“Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término “cancelado” o “pagado”] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia”.*

	En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores 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 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 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 que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9. Cuando en los contratos, órdenes de compra 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 compra o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo Nº 8 referido a la Experiencia del Postor en la Especialidad. Importante *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".*

Importante para la Entidad

En caso que el objeto de la convocatoria sea la adquisición de bienes bajo la modalidad de ejecución llave en mano, cuando se requiera personal para la instalación y puesta en funcionamiento, y se haya considerado que éste es personal clave, se puede incluir el siguiente requisito de calificación:

C	CAPACIDAD TÉCNICA Y PROFESIONAL
	Un (01) Especialista en Soluciones de Datacenter <u>Formación Académica</u> - Ingeniero electrónico o sistemas, titulado, habilitado por el Colegio de Ingenieros del Perú. <u>Certificaciones</u> - Certificado de Consultor de Diseñador por TIA 942. - Certificación de diseñador de Centro de Datos, ATD de UPTIME INSTITUTE - Certificación de especialista de Centro de Datos, DCS de Diseño de DCPRO/ DATACENTER DYNAMICS. - Certificación de diseñador de Centro de Datos, CCRD de ICREA. - Certificado de profesional en Centro de Datos o Data Center o Centro de Cómputo

Experiencia

- Contar con experiencia mínima de cuatro (04) años, como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador en actividades relacionadas a la consultoría, diseño, supervisor de Centro de Datos (Data Center) ylas Soluciones de Tecnología de Información y comunicaciones. Se deberá adjuntarlas constancias de la experiencia.

- Experiencia en haber participado como mínimo en tres (03) Servicios de Ingeniería o Diagnostico Situacional o Supervisiones o Acondicionamiento o Instalaciones de Centro de Datos o Data Center o Centro de Computo, en los últimos años. Se deberáadjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad.

Un (01) Especialista en UPS y AAP

Formación Académica

- Formación: Ing. Electrónico o electricista, titulado, habilitado por el Colegio de Ingenieros del Perú.

Certificaciones

- Certificación en Implementación de Datacenter Oficial técnica vigente (no venta, no preventa) emitido por el fabricante de Datacenter ofertado.

Experiencia

- Experiencia no menor de 5 años como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador de instalaciones de UPS y AAP. Se deberá adjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad.

Un (1) Especialista en Infraestructura

Formación Académica:

- Profesional Bachiller o Titulado en Ingeniería: Electrónica y/o Informática y/o Sistemas y/o Computación e Informática y/o Redes y Comunicación de Datos y/o Industrial y/o Sistemas e informática y/o Redes y Comunicaciones y/o Empresarial yde sistemas y/o Ciencias de la Computación y/o Electrónica de Sistemas Computarizado y/o Ingeniería de Telecomunicaciones.

Certificación

- Certificación Oficial técnica (no venta, no preventa) nivel Asociado y/o profesional de servidores emitida por el fabricante de la marca de servidores
- Certificación Oficial técnica (no venta, no preventa) de implementación y/o instalacióny/o administración y/o profesional de almacenamiento emitida por el fabricante en la marca de almacenamiento ofertados
- Certificación Oficial Técnica (no venta, no preventa) de implementación y/o instalación y/o administración y/o Profesional en Switches SAN emitida por elfabricante en la marca del equipamiento ofertado y/o Brocade o similar.

Experiencia

Tres (3) años mínimo como especialista y/o consultor y/o perito y/o supervisor y/o jefede proyecto y/o coordinador en implementación y/o soporte y/o administración de Infraestructura TI. Se deberá adjuntar las constancias de los servicios realizados y/u ordenes de servicio con su respectiva conformidad.

Un (1) Especialista en Networking

Formación Académica:

- Profesional Bachiller o Titulado en Ingeniería: Electrónica y/o informática y/o Sistemasy/o Computación e Informática y/o Redes y Comunicación de Datos y/o Industrial y/o Sistemas e Informática y/o Redes y Comunicaciones y/o Empresarial y de sistemas y/oCiencias de la Computación y/o Electrónica de Sistemas Computarizado y/o Ingeniería de

	Telecomunicaciones. Certificación - Certificación Oficial técnica (no venta, no prevente) en Networking y/o Datacom y/o Switching emitida por el fabricante del equipamiento de comunicaciones ofertado. Experiencia - Dos (2) años mínimo como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador en administración y/o implementación y/o soporte de soluciones de Networking. Se deberá adjuntar las constancias de los servicios realizados y/o ordenes de servicio con su respectiva conformidad. **Dos (2) Especialista en Virtualización** Formación Académica - Titulado o Bachiller en Ingeniería: Electrónica y/o Informática y/o Sistemas y/o Computación e Informática y/o Redes y Comunicación de Datos y/o Industrial y/o Sistemas e Informática y/o Redes y Comunicaciones y/o Empresarial y de sistemas y/oCiencias de la Computación y/o Electrónica de Sistemas Computarizado y/o Ingeniería de Telecomunicaciones. Capacitación - Certificación Oficial técnica (no venta, no preventa) no mayor a 03 años de instalaciónyy/o implementación y/o profesional de virtualización de Centro de Datos emitida por el fabricante del Software de Virtualización ofertado. - Certificación Oficial técnica (no venta, no preventa) no mayor a 03 años de instalaciónyy/o implementación y/o profesional de virtualización de redes emitida por el fabricante del software de virtualización. - Certificación Oficial técnica en HCI emitida por el fabricante del software de virtualización ofertado. ***** *****Se aceptará Badge oficial siempre y cuando se adjunte en la propuesta el transcript con Link público emitido por el fabricante evidenciando la especialización del profesional en HCI. Experiencia - Cinco (5) años como mínimo como especialista y/o consultor y/o perito y/o supervisor y/o jefe de proyecto y/o coordinador y/o administración de soluciones Virtualización.

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*

- *El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

CAPÍTULO IV
FACTORES DE EVALUACIÓN

La evaluación se realiza sobre la base de cien (100) puntos.

Para determinar la oferta con el mejor puntaje y el orden de prelación de las ofertas, se considera lo siguiente:

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<u>Evaluación</u>: Se evaluará considerando el precio ofertado por el postor. <u>Acreditación</u>: Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ i = Oferta Pi = Puntaje de la oferta a evaluar Oi = Precio i Om = Precio de la oferta más baja PMP = Puntaje máximo del precio 100 puntos

CAPÍTULO V
PROFORMA DEL CONTRATO

CONTRATACIÓN DIRECTA N° 002-2024-CENEPRED
POR LA CAUSAL "SITUACIÓN DE EMERGENCIA"
EN EL MARCO DEL DECRETO SUPREMO N° 199-2023-EF

MEJORAMIENTO DE LA PLATAFORMA TECNOLÓGICA DEL SISTEMA DE INFORMACIÓN PARA LA GESTIÓN DEL RIESGO DE DESASTRES (SIGRID) ANTE LA OCURRENCIA DE INUNDACIONES Y MOVIMIENTOS EN MASA COMO CONSECUENCIA DEL PROBABLE FENÓMENO EL NIÑO 2023-2024

Conste por el presente documento, la contratación para el **"Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno el niño 2023-2024"**, para el Centro Nacional de Estimación, Prevención y Reducción del Riesgo de Desastres – CENEPRED, que celebra de una parte el CENEPRED, en adelante LA ENTIDAD, con RUC Nº 20543891755, con domicilio legal en Av. Del Parque Norte N° 313-319, Urb. Corpac, Distrito de San Isidro de la Provincia y Departamento de Lima, representado por el señor OSWALDO ALEJANDRO ULLOA TAMAYO, identificado con DNI Nº 09455775, facultado para suscribir contratos del CENEPRED mediante Resolución Jefatural N° 00001-2023-CENEPRED/J, de fecha 04 de enero del 2023; y de otra parte EL CONSORCIO, conformado por VALTOM INGENIEROS S.A.C., con RUC 20507745629 con domicilio legal en CA. LOS NOGALES MZ L, LT-12, URB SHANGRI-LA, DISTRITO DE PUENTE PIEDRA – PROVINCIA Y DEPARTAMENTO DE LIMA, inscrita en la partida electrónica N° 11626848 Asiento A00001 de Registro de Personas Jurídica de Lima, debidamente representado por la señora MARIA ELENA PAVLICH ORDOÑEZ, con DNI N° 08268004; y OLC INGENIEROS E.I.R.L., con RUC Nº 20254356051, con domicilio legal en CA. LOS NOGALES, MZ M, LT 12, URB. SHANGRI-LA, DISTRITO DE PUENTE PIEDRA, PROVINCIA Y DEPARTAMENTO DE LIMA, inscrita en la partida electrónica N° 01525409, Asiento N° C00003 del Registro de Personas Jurídicas de la ciudad de Lima, debidamente representado por su Representante Legal el señor OSCAR LUIS CHION LUY, con DNI N° 07987649, debidamente representados por su REPRESENTANTE LEGAL COMÚN OSCAR LUIS CHION LUY con DNI N° 07987649, con domicilio legal en CA. LOS NOGALES, MZ M, LT 12 URB. SHANGRI-LA, DISTRITO DE PUENTE PIEDRA, PROVINCIA Y DEPARTAMENTO DE LIMA, según poder en el Contrato de Consorcio de fecha 14 de noviembre de 2023, a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha 13 de noviembre de 2023 (Carta N° 168-2024-CENEPRED/OA), el Órgano Encargado de las Contrataciones adjudicó la Buena Pro de la CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED para la contratación de "Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno el niño 2023-2024", derivada de situaciones que supongan grave peligro de la ocurrencia de acontecimientos catastróficos al CONSORCIO VALTON INGENIEROS S.A.C. - OLC INGENIEROS E.I.R.L., por el monto de S/9'598,603.34 (NUEVE MILLONES QUINIENTOS NOVENTA Y OCHO MIL SEISCIENTOS TRES CON 34/100 SOLES), cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la Contratación Directa por la causal "Situación de Emergencia" para "Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno el niño 2023-2024", derivada de situaciones que supongan grave peligro de la ocurrencia de acontecimientos catastróficos.

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a S/9'598,603.34 (NUEVE MILLONES QUINIENTOS NOVENTA Y OCHO MIL SEISCIENTOS TRES CON 34/100 SOLES), que incluye todos los impuestos de Ley.

Este monto comprende el costo del bien y el servicio, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución de la prestación materia del presente contrato.

Prestación a ejecutarse por parte de EL CONTRATISTA	Adquisición de Bienes	Prestación de Servicios	Monto Total de la Contratación
"Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno El Niño 2023-2024"	S/9'568,603.34 (Nueve millones quinientos sesenta y ocho mil seiscientos tres con 34/100 Soles)	S/30,000.00 (Treinta mil con 00/100 Soles)	S/9'598,603.34 (Nueve millones quinientos noventa y ocho mil seiscientos tres con 34/100 Soles)

CLÁUSULA CUARTA: DEL PAGO

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES, en PAGO ÚNICO, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

Los pagos se efectuarán de acuerdo al siguiente detalle:

Prestación a ejecutarse por parte de EL CONTRATISTA	Plazo máximo para la ejecución de la prestación	Pago por Adelanto contra la presentación de Carta Fianza al 100%
"Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno El Niño 2023-2024"	Noventa (90) días de la notificación de la Orden de Compra y Orden de Servicio	S/9'598,603.34 (Nueve millones quinientos noventa y ocho mil seiscientos tres con 34/100 Soles)

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de noventa (90) días calendario, el mismo que se computa desde el día siguiente de la notificación de la Orden de Compra N° 0025 y Orden de Servicio N° 0308 de fecha 04.12.2023, en la modalidad de Llave en Mano siendo el plazo de entrega de noventa (90) días calendario, su instalación y puesta en funcionamiento.

La Entidad estará en la potestad de solicitar dentro de los 03 años al proveedor el traslado de la infraestructura de DATA CENTER PRINCIPAL (Solución Gabinetes Autocontenidos) a una nueva ubicación en el ámbito de Lima Metropolitana, la entidad deberá proveer las facilidades técnicas en relación a espacio, energía y acondicionamiento del nuevo local.

El acondicionamiento, montaje, instalación, y puesta en funcionamiento debe estar alineado a los criterios y recomendaciones técnicas específicas para la construcción de centros de datos en el Perú, establecido en la Norma Técnica Peruana para la Construcción de Centros de Datos ISO/IEC TS 22237, aprobado mediante Resolución Directoral N° 030-2019-INACAL/DN; recomendaciones del fabricante; así como, las normas de seguridad aplicables a la implementación de DATACENTERS.

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS

Prestación accesoria:

Mantenimiento:
Mantenimiento anual y soporte técnico durante 36 meses a partir de la conformidad brindada por CENEPRED de la instalación, configuración y puesta en marcha.

Capacitación:
Infraestructura de la solución, 8 horas, para 5 personas certificado.
Solución de almacenamiento Storage, 8 horas, para 5 personas certificado.
Solución de Backup, 8 horas, para 5 personas certificado.

Migración de la data
Se efectuará la migración de toda la data relacionada al SIGRID y aplicaciones geoespaciales del(los) servidores actuales al nuevo Data Center.

El monto de las prestaciones accesorias asciende a TREINTA MIL CON 00/100 SOLES (S/30,000.00), que incluye todos los impuestos de Ley, tal como se detalla:

Prestación a ejecutarse por parte de EL CONTRATISTA	Garantía por todo el Equipamiento y Servicio	Garantía de Fiel Cumplimiento por Prestaciones Accesorias
"Mejoramiento de la plataforma tecnológica del sistema de información para la gestión del riesgo de desastres (SIGRID) ante la ocurrencia de inundaciones y movimientos en masa como consecuencia del probable fenómeno El Niño 2023-2024"	La garantía para todas las partes y componentes debe ser por un periodo por tres (3) años ON SITE 7X24, con un tiempo de respuesta no mayor a las 4 horas y las incidencias podrán ser ingresadas o por una llamada telefónica, correo electrónico y/o un portal web del fabricante, de tal forma que en cualquier momento la Entidad pueda reportar la incidencia	S/30,000.00 (Treinta mil con 00/100 Soles)

La prestación es garantizada a través de una Garantía de Fiel Cumplimiento por Prestaciones Accesorias, de acuerdo a lo siguiente:

GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS:

- Carta Fianza N° **10652068-000**
- Emitida por: SCOTIABANK
- Monto: **S/30,000.00** (Treinta mil con 00/100 Soles)
- Fecha de Emisión: 06.03.2024
- Vigencia: **06.03.2025**

El plazo de ejecución de las prestaciones accesorias es de Treinta y Seis (36) meses, el mismo que se computa desde LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO.

La garantía de fiel cumplimiento por prestaciones accesorias debe ser renovada a los diez (10) calendario, antes de la fecha de vigencia, por el Representante Común del Consorcio VALTOM INGENIEROS S.A.C. – OLC INGENIEROS E.I.R.L.

CLÁUSULA SÉTIMA: PARTES INTEGRANTES DEL CONTRATO
El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA OCTAVA: GARANTÍAS
EL CONTRATISTA entregó al perfeccionamiento del contrato en la Ordene de Compra N° 025 y Orden de Servicio N° 380 de fechas, 04 de diciembre de 2023, la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por concepto, importe y vigencia siguiente:

1) **PAGO POR ADELANTO CONTRA LA PRESENTACION DE CARTA FIANZA POR EL 100%**:
Carta Fianza N° 10650034-000

Emitida por: SCOTIABANK
Monto: S/9'598,603.34 (Nueve millones quinientos noventa y ocho mil seiscientos tres con 34/100 Soles)
Fecha de Emisión: 06.12.2023
Vigencia: 05.03.2024 (DEVUELTA contra la presentación del Acta de Conformidad).

2) <u>PRESENTACIÓN DE GARANTÍA POR FIEL CUMPLIMIENTO</u>:
Carta Fianza N° 10650032-000; Renovada: 10650032-001
Emitida por: SCOTIABANK
Monto: S/959,860.33 (Novecientos cincuenta y nueve mil ochocientos sesenta con 33/100 Soles)
Fecha de Emisión: 06.12.2023; Renovada: 07.03.2024
Vigencia: 05.03.2024; Renovada: 03.06.2024

Esta garantía es emitida por una empresa bajo el ámbito de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones. Esta garantía deberá encontrarse vigentes hasta la conformidad de la recepción de la prestación a cargo de EL CONTRATISTA.

<u>CLÁUSULA NOVENA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN</u>
LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

<u>CLÁUSULA DÉCIMA: ADELANTO CONTRA PRESENTACIÓN DE CARTA FIANZA POR EL 100%</u>

LA ENTIDAD otorgará adelanto de pago por el 100% del monto del contrato original previo otorgamiento de una garantía por adelantos mediante CARTA FIANZA por el mismo monto del pago.

Por el pago de la contraprestación pactada a favor del contratista en PAGO ÚNICO EN FUNCIÓN AL MONTO DEL CONTRATO ORIGINAL, previo otorgamiento de una garantía por el mismo monto del pago, por concepto, importe y vigencia siguiente:

<u>PAGO POR ADELANTO</u>:
Carta Fianza N° 10650034-000
Emitida por: SCOTIABANK
Monto: S/9'598,603.34 (Nueve millones quinientos noventa y ocho mil seiscientos tres con 34/100 Soles)
Fecha de Emisión: 06.12.2023
Vigencia: 05.03.2024 (DEVUELTA contra la presentación del Acta de Conformidad)

<u>CLÁUSULA DÉCIMA PRIMERA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN</u>
La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por EL ESPECIALISTA EN ALMACÉN Y CONTROL PATRIMONIAL y la conformidad será otorgada por LA SUBDIRECCIÓN DE GESTION DE PROCESOS de la DIRECCIÓN DE GESTIÓN DE PROCESOS previo informe del ESPECIALISTA EN INFORMÁTICA de la OFICINA DE ADMINISTRACIÓN del CENEPRED, el cual contendrá el inventario de todos los bienes entregados por el CONTRATISTA (Incluido Licencias), características técnicas de cada bien y licencias, claves de acceso a los servidores, códigos de activación de licencias.

De conformidad final contendrá las pruebas de funcionamiento y confirmación de la operatividad del DATA CENTER PRINCIPAL y SECUNDARIO.

Asimismo, previo al informe y/o acta de recepción conforme de los bienes entregados, tanto del DATA CETER PRINCIPAL como SECUNDARIO y componentes respectivos, elaborado por el Especialista en Almacén y Control Patrimonial de la Oficina de Administración.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede otorgar al

CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

CLÁUSULA DÉCIMA SEGUNDA: DECLARACIÓN JURADA DEL CONTRATISTA

EL CONTRATISTA declara bajo juramento que se compromete a cumplir las obligaciones derivadas del presente contrato, bajo sanción de quedar inhabilitado para contratar con el Estado en caso de incumplimiento.

CLÁUSULA DÉCIMA TERCERA: RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 40 de la Ley de Contrataciones del Estado y 173 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de TRES (3) AÑOS contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA CUARTA: PENALIDADES

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo a la siguiente fórmula:

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de LA ENTIDAD no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme el numeral 162.5 del artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA QUINTA: RESOLUCIÓN DEL CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 32.3 del artículo 32 y artículo 36 de la Ley de Contrataciones del Estado, y el artículo 164 de su Reglamento. De darse el caso, LA ENTIDAD procederá de acuerdo a lo establecido en el artículo 165 del Reglamento de la Ley de Contrataciones del Estado.

CLÁUSULA DÉCIMA SEXTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.
Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SÉTIMA: ANTICORRUPCIÓN

EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, el CONTRATISTA 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, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA OCTAVA: MARCO LEGAL DEL CONTRATO
Sólo en lo no previsto en este contrato, en la Ley de Contrataciones del Estado y su Reglamento, en las directivas que emita el OSCE y demás normativa especial que resulte aplicable, serán de aplicación supletoria las disposiciones pertinentes del Código Civil vigente, cuando corresponda, y demás normas de derecho privado.

CLÁUSULA DÉCIMA NOVENA: SOLUCIÓN DE CONTROVERSIAS

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación o arbitraje, según el acuerdo de las partes.

Cualquiera de las partes tiene derecho a iniciar el arbitraje a fin de resolver dichas controversias dentro del plazo de caducidad previsto en la Ley de Contrataciones del Estado y su Reglamento.

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 45.21 del artículo 45 de la Ley de Contrataciones del Estado.

CLÁUSULA VIGÉSIMA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA
Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA PRIMERA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL
Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: AV DEL PARQUE NORTE N° 313-319 URB. CORPAC, DISTRITO DE SAN ISIDRO, PROVINCIA Y DEPARTAMENTO DE LIMA.

DOMICILIO DEL CONTRATISTA: CA. LOS NOGALES, MZ M, LT 12 URB. SHANGRI-LA, DISTRITO DE PUENTE PIEDRA, PROVINCIA Y DEPARTAMENTO DE LIMA.

La variación del domicilio aquí declarado de alguna de las partes debe ser comunicada a la otra parte, formalmente y por escrito, con una anticipación no menor de quince (15) días calendario.

De acuerdo con las bases, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de **LIMA al 03 DE ABRIL DE 2024**.

"LA ENTIDAD"	"EL CONTRATISTA"

Importante
Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[7].

[7] Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

El que se suscribe, [……..], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], DECLARO BAJO JURAMENTO que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra[8]

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda

Importante
La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

[8] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

Importante
Cuando se trate de consorcios, la declaración jurada es la siguiente:

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

El que se suscribe, [……..], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], DECLARO BAJO JURAMENTO que la siguiente información se sujeta a la verdad:

Datos del consorciado 1			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Datos del consorciado …			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra[9]

Asimismo, me comprometo a remitir la confirmación de recepción, en el plazo máximo de dos (2) días hábiles de recibida la comunicación.
[CONSIGNAR CIUDAD Y FECHA]

[9] Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

…….....
Firma, Nombres y Apellidos del representante
común del consorcio

Importante
La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.

ANEXO Nº 2

DECLARACIÓN JURADA
(ART. 52 DEL REGLAMENTO DE LA LEY DE CONTRATACIONES DEL ESTADO)

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento:

i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.

ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.

iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.

iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo Nº 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.

v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.

vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.

vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda

Importante
En el caso de consorcios, cada integrante debe presentar esta declaración jurada, salvo que sea presentada por el representante común del consorcio.

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el [CONSIGNAR EL OBJETO DE LA CONVOCATORIA], de conformidad con las Especificaciones Técnicas que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante
Adicionalmente, puede requerirse la presentación de documentación que acredite el cumplimiento de las especificaciones técnicas, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO. EN CASO DE LA MODALIDAD DE LLAVE EN MANO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO Nº 5

PROMESA DE CONSORCIO
(Sólo para el caso en que un consorcio se presente como postor)

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la LICITACIÓN PÚBLICA Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO].

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por el artículo 140 del Reglamento de la Ley de Contrataciones del Estado, bajo las siguientes condiciones:

a) Integrantes del consorcio
   1. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1].
   2. [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2].

b) Designamos a [CONSIGNAR NOMBRES Y APELLIDOS DEL REPRESENTANTE COMÚN], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], como representante común del consorcio para efectos de participar en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato correspondiente con [CONSIGNAR NOMBRE DE LA ENTIDAD].

   Asimismo, declaramos que el representante común del consorcio no se encuentra impedido, inhabilitado ni suspendido para contratar con el Estado.

c) Fijamos nuestro domicilio legal común en [.....].
   |
d) Las obligaciones que corresponden a cada uno de los integrantes del consorcio son las siguientes:

1.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1]	[%] [10]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%] [11]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[12]

[CONSIGNAR CIUDAD Y FECHA]

[10] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

[11] Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

[12] Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

……	……..
Consorciado 1	Consorciado 2
Nombres, apellidos y firma del Consorciado 1 o de su Representante Legal	Nombres, apellidos y firma del Consorciado 2 o de su Representante Legal
Tipo y N° de Documento de Identidad	Tipo y N° de Documento de Identidad

Importante
De conformidad con el artículo 52 del Reglamento, las firmas de los integrantes del consorcio deben ser legalizadas.

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que, de acuerdo con las bases, mi oferta es la siguiente:

CONCEPTO	PRECIO TOTAL
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante

- *El postor debe consignar el precio total de la oferta, sin perjuicio, que de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- *El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

  "Mi oferta no incluye [CONSIGNAR EL TRIBUTO MATERIA DE LA EXONERACIÓN]".

Importante para la Entidad

- *En caso de procedimientos según relación de ítems, consignar lo siguiente:*
  "El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente".
- *En caso de contrataciones que conllevan la ejecución de prestaciones accesorias, consignar lo siguiente:*
  "El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias".

ANEXO Nº 7

DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA EXONERACIÓN DEL IGV

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

1.- Que el domicilio fiscal de la empresa[13] se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);

2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);

3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y

4.- Que la empresa no tiene producción fuera de la Amazonía.[14]

[CONSIGNAR CIUDAD Y FECHA]

……..
Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda

Importante
Cuando se trate de consorcios, esta declaración jurada será presentada por cada uno de los integrantes del consorcio, salvo que se trate de consorcios con contabilidad independiente, en cuyo caso debe ser suscrita por el representante común, debiendo indicar su condición de consorcio con contabilidad independiente y el número de RUC del consorcio.

[13] En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquéllas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

[14] En caso de empresas de comercialización, no consignar esta condición.

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Mediante el presente, el suscrito detalla la siguiente EXPERIENCIA EN LA ESPECIALIDAD*:*

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [15]	FECHA DE LA CONFORMIDAD DE SER EL CASO[16]	EXPERIENCIA PROVENIENTE[17] DE:	MONEDA	IMPORTE[18]	TIPO DE CAMBIO VENTA[19]	MONTO FACTURADO ACUMULADO[20]
1										
2										
3										

[15] Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

[16] **Únicamente**, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

[17] Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN *"Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz"*. Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, *"… en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe"*.

[18] Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

[19] El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

[20] Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [15]	FECHA DE LA CONFORMIDAD DE SER EL CASO[16]	EXPERIENCIA PROVENIENTE[17] DE:	MONEDA	IMPORTE[18]	TIPO DE CAMBIO VENTA[19]	MONTO FACTURADO ACUMULADO[20]
4										
5										
6										
7										
8										
9										
10										
…										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

…….....
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro que la experiencia que acredito de la empresa [CONSIGNAR LA DENOMINACIÓN DE LA PERSONA JURÍDICA] como consecuencia de una reorganización societaria, no se encuentra en el supuesto establecido en el numeral 49.4 del artículo 49 del Reglamento.

[CONSIGNAR CIUDAD Y FECHA]

……..……..
Firma, Nombres y Apellidos del postor o
Representante legal, según corresponda

Importante
A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados. *También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.*

ANEXO Nº 10

SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA
ITEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO CORRESPONDE A UNA AS])

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

Mediante el presente el suscrito, postor y/o Representante legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

……..……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante
• *Para asignar la bonificación, el comité de selección, según corresponda, verifica la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2/.* • *Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.*

ANEXO Nº 11

AUTORIZACIÓN DE NOTIFICACIÓN DE LA DECISIÓN DE LA ENTIDAD SOBRE LA SOLICITUD DE AMPLIACIÓN DE PLAZO MEDIANTE MEDIOS ELECTRÓNICOS DE COMUNICACIÓN

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
ORGANO ENCARGADO DE LAS CONTRATACIONES
CONTRATACIÓN DIRECTA Nº 002-2024-CENEPRED
Presente.-

El que se suscribe, [……..], postor adjudicado y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], autorizo que durante la ejecución del contrato se me notifique al correo electrónico [INDICAR EL CORREO ELECTRÓNICO] lo siguiente:

- ✓ Notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo.

[CONSIGNAR CIUDAD Y FECHA]

……..……..
Firma, Nombres y Apellidos del postor o
Representante legal o común, según corresponda

Importante
La notificación de la decisión de la Entidad respecto a la solicitud de ampliación de plazo se efectúa por medios electrónicos de comunicación, siempre que se cuente con la autorización correspondiente y sea posible obtener un acuse de recibo a través del mecanismo utilizado.