

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

Aprobado mediante Directiva N° 001-2019-OSCE/CD



SUB DIRECCIÓN DE NORMATIVIDAD – DIRECCIÓN TÉCNICO NORMATIVA
ORGANISMO SUPERVISOR DE LAS CONTRATACIONES DEL ESTADO - OSCE

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

Las bases estándar deben ser elaboradas en formato WORD, y deben tener las siguientes características:

N°	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Inferior: 2.5 cm Izquierda: 2.5 cm Derecha: 2.5 cm
2	Fuente	Arial
3	Estilo de Fuente	Normal: Para el contenido en general Cursiva: Para el encabezado y pie de página Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
4	Color de Fuente	Automático: Para el contenido en general Azul : Para las Consideraciones importantes (Ítem 3 del cuadro anterior)
5	Tamaño de Letra	16 : Para las dos primeras hojas de las Secciones General y Específica 11 : Para el nombre de los Capítulos. 10 : Para el cuerpo del documento en general 9 : Para el encabezado y pie de página Para el contenido de los cuadros, pudiendo variar, según la necesidad 8 : Para las Notas al pie
6	Alineación	Justificada: Para el contenido en general y notas al pie. Centrada : Para la primera página, los títulos de las Secciones y nombres de los Capítulos)
7	Interlineado	Sencillo
8	Espaciado	Anterior : 0 Posterior : 0
9	Subrayado	Para los nombres de las Secciones y para resaltar o hacer hincapié en algún concepto

INSTRUCCIONES DE USO:

- Una vez registrada la información solicitada dentro de los corchetes sombreados en gris, el texto deberá quedar en letra tamaño 10, con estilo normal, sin formato de negrita y sin sombrear.
- La nota **IMPORTANTE** no puede ser modificada ni eliminada en la Sección General. En el caso de la Sección Específica debe seguirse la instrucción que se indica en dicha nota.

Elaboradas en enero de 2019

Modificadas en junio 2019, diciembre 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022



HOSPITAL NACIONAL
DANIEL ALCIDES CARRIÓN

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

LICITACIÓN PÚBLICA N°03-2023-HNDAC-CS-1
PRIMERA CONVOCATORIA

CONTRATACIÓN DE BIENES

ADQUISICION DE SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE), SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE) Y ; EN EL(LA) EESS NAC. DANIEL A. CARRION - BELLAVISTA EN LA LOCALIDAD BELLAVISTA, DISTRITO DE BELLAVISTA, PROVINCIA CONSTITUCIONAL DEL CALLAO, DEPARTAMENTO CALLAO CON EL CUI N° 2554512

JUNIO 2023 - CALLAO

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 GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

(ESTA SECCIÓN NO DEBE SER MODIFICADA EN NINGÚN EXTREMO, BAJO SANCIÓN DE NULIDAD)

CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

Cuando en el presente documento se mencione la palabra Ley, se entiende que se está haciendo referencia a la Ley N° 30225, Ley de Contrataciones del Estado, y cuando se mencione la palabra Reglamento, se entiende que se está haciendo referencia al Reglamento de la Ley de Contrataciones del Estado aprobado por Decreto Supremo N° 344-2018-EF.

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

1.2. CONVOCATORIA

Se realiza a través de su publicación en el SEACE de conformidad con lo señalado en el artículo 54 del Reglamento, en la fecha señalada en el calendario del procedimiento de selección, debiendo adjuntar las bases y resumen ejecutivo.

1.3. REGISTRO DE PARTICIPANTES

El registro de participantes se realiza conforme al artículo 55 del Reglamento. En el caso de un consorcio, basta que se registre uno (1) de sus integrantes.

Importante

- *Para registrarse como participante en un procedimiento de selección convocado por las Entidades del Estado Peruano, es necesario que los proveedores cuenten con inscripción vigente y estar habilitados ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Supervisor de las Contrataciones del Estado (OSCE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.rnp.gob.pe.*
- *Los proveedores que deseen registrar su participación deben ingresar al SEACE utilizando su Certificado SEACE (usuario y contraseña). Asimismo, deben observar las instrucciones señaladas en el documento de orientación "Guía para el registro de participantes electrónico" publicado en <https://www2.seace.gob.pe/>.*
- *En caso los proveedores no cuenten con inscripción vigente en el RNP y/o se encuentren inhabilitados o suspendidos para ser participantes, postores y/o contratistas, el SEACE restringirá su registro, quedando a potestad de estos intentar nuevamente registrar su participación en el procedimiento de selección en cualquier otro momento, dentro del plazo establecido para dicha etapa, siempre que haya obtenido la vigencia de su inscripción o quedado sin efecto la sanción que le impuso el Tribunal de Contrataciones del Estado.*

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada, aun cuando el requerimiento haya sido homologado parcialmente respecto a las características técnicas y/o requisitos de calificación y/o condiciones de ejecución. Las consultas y observaciones que se formulen sobre el particular, se tienen como no presentadas.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en los numerales 72.4 y 72.5 del artículo 72 del Reglamento.

Importante

- *No se absolverán consultas y observaciones a las bases que se presenten en forma física.*
- *Cuando exista divergencia entre lo indicado en el pliego de absolución de consultas y observaciones y la integración de bases, prevalece lo absuelto en el referido pliego; sin perjuicio, del deslinde de responsabilidades correspondiente.*

1.6. ELEVACIÓN AL OSCE DEL PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES E INTEGRACIÓN DE BASES

Los cuestionamientos al pliego de absolución de consultas y observaciones así como a las bases integradas por supuestas vulneraciones a la normativa de contrataciones, a los principios que rigen la contratación pública u otra normativa que tenga relación con el objeto de la contratación, pueden ser elevados al OSCE de acuerdo a lo indicado en los numerales del 72.8 al 72.11 del artículo 72 del Reglamento.

La solicitud de elevación para emisión de Pronunciamiento se presenta ante la Entidad, la cual debe remitir al OSCE el expediente completo, de acuerdo a lo señalado en el artículo 124 del TUO de la Ley 27444, aprobado por Decreto Supremo N° 004-2019-JUS, al día hábil siguiente de recibida dicha solicitud.

Advertencia

La solicitud de elevación al OSCE de los cuestionamientos al pliego de absolución de consultas y observaciones, así como a las Bases integradas, se realiza de manera electrónica a través del SEACE, a partir de la oportunidad en que establezca el OSCE mediante comunicado.

Importante

Constituye infracción pasible de sanción según lo previsto en el literal n) del numeral 50.1 del artículo 50 de la Ley, presentar cuestionamientos maliciosos o manifiestamente infundados al pliego de absolución de consultas y/u observaciones.

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 del Reglamento.

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

¹ 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>

- *Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.*
- *En caso la información contenida en los documentos escaneados que conforman la oferta no coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.*
- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

El participante presentará su oferta de manera electrónica a través del SEACE, desde las 00:01 horas hasta las 23:59 horas del día establecido para el efecto en el cronograma del procedimiento; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo a lo requerido en las bases.

El participante debe verificar antes de su envío, bajo su responsabilidad, que el archivo pueda ser descargado y su contenido sea legible.

Importante

Los integrantes de un consorcio no pueden presentar ofertas individuales ni conformar más de un consorcio en un procedimiento de selección, o en un determinado ítem cuando se trate de procedimientos de selección según relación de ítems.

En la apertura electrónica de la oferta, el comité de selección, verifica la presentación de lo exigido en la sección específica de las bases, de conformidad con el numeral 73.2 del artículo 73 del Reglamento y determina si las ofertas responden a las características y/o requisitos funcionales y condiciones de las Especificaciones Técnicas, detalladas en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.9. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el artículo 74 del Reglamento.

El desempate mediante sorteo se realiza de manera electrónica a través del SEACE.

1.10. CALIFICACIÓN DE OFERTAS

La calificación de las ofertas se realiza conforme a lo establecido en los numerales 75.1 y 75.2 del artículo 75 del Reglamento.

1.11. SUBSANACIÓN DE LAS OFERTAS

La subsanación de las ofertas se sujeta a lo establecido en el artículo 60 del Reglamento. El plazo que se otorgue para la subsanación no puede ser inferior a un (1) día hábil.

La solicitud de subsanación se realiza de manera electrónica a través del SEACE y será remitida al correo electrónico consignado por el postor al momento de realizar su inscripción en el RNP, siendo su responsabilidad el permanente seguimiento de las notificaciones a dicho correo. La notificación de la solicitud se entiende efectuada el día de su envío al correo electrónico.

La presentación de las subsanaciones se realiza a través del SEACE. No se tomará en cuenta la subsanación que se presente en físico a la Entidad.

1.12. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

De rechazarse alguna de las ofertas calificadas, el comité de selección revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.13. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE, incluyendo el cuadro comparativo y las actas debidamente motivadas de los resultados de la admisión, no admisión, evaluación, calificación, descalificación, rechazo y el otorgamiento de la buena pro.

1.14. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los ocho (8) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

En caso que se haya presentado una sola oferta, el consentimiento de la buena pro se produce el mismo día de la notificación de su otorgamiento.

El consentimiento del otorgamiento de la buena pro se publica en el SEACE al día hábil siguiente de producido.

Importante

Una vez consentido el otorgamiento de la buena pro, el órgano encargado de las contrataciones o el órgano de la Entidad al que se haya asignado tal función realiza la verificación de la oferta presentada por el postor ganador de la buena pro conforme lo establecido en el numeral 64.6 del artículo 64 del Reglamento.

CAPÍTULO II SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

A través del recurso de apelación se pueden impugnar los actos dictados durante el desarrollo del procedimiento de selección hasta antes del perfeccionamiento del contrato.

El recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

Los actos que declaren la nulidad de oficio, la cancelación del procedimiento de selección y otros actos emitidos por el Titular de la Entidad que afecten la continuidad de este, se impugnan ante el Tribunal de Contrataciones del Estado.

Importante

- *Una vez otorgada la buena pro, el comité de selección, está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, salvo la información calificada como secreta, confidencial o reservada por la normativa de la materia, a más tardar dentro del día siguiente de haberse solicitado por escrito.*

Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el comité de selección.

- *A efectos de recoger la información de su interés, los postores pueden valerse de distintos medios, tales como: (i) la lectura y/o toma de apuntes, (ii) la captura y almacenamiento de imágenes, e incluso (iii) pueden solicitar copia de la documentación obrante en el expediente, siendo que, en este último caso, la Entidad deberá entregar dicha documentación en el menor tiempo posible, previo pago por tal concepto.*
- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone dentro de los ocho (8) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro.

La apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento, se interpone dentro de los ocho (8) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

Los plazos y el procedimiento para perfeccionar el contrato se realiza conforme a lo indicado en el artículo 141 del Reglamento.

Para perfeccionar el contrato, el postor ganador de la buena pro debe presentar los documentos señalados en el artículo 139 del Reglamento y los previstos en la sección específica de las bases.

3.2. GARANTÍAS

Las garantías que deben otorgar los postores y/o contratistas, según corresponda, son las de fiel cumplimiento del contrato y por los adelantos.

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

Como requisito indispensable para perfeccionar el contrato, el postor ganador debe entregar a la Entidad la garantía de fiel cumplimiento del mismo por una suma equivalente al diez por ciento (10%) del monto del contrato original. Esta se mantiene vigente hasta la conformidad de la recepción de la prestación a cargo del contratista.

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación accesorio, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

En caso se haya previsto en la sección específica de las bases la entrega de adelantos, el contratista debe presentar una garantía emitida por idéntico monto conforme a lo estipulado en el artículo 153 del Reglamento.

3.3. REQUISITOS DE LAS GARANTÍAS

Las garantías que se presenten deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la Entidad. Asimismo, deben ser emitidas por empresas que se encuentren bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones y que cuenten con clasificación de riesgo B o superior. Asimismo, deben estar autorizadas para emitir garantías; o estar consideradas en la última lista de bancos extranjeros de primera categoría que periódicamente publica el Banco Central de Reserva del Perú.

Importante

Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro y/o contratista cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.

Advertencia

Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente:

1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).

2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.

3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.

4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.

En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.

De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza>).

Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.

3.4. EJECUCIÓN DE GARANTÍAS

La Entidad puede solicitar la ejecución de las garantías conforme a los supuestos contemplados en el artículo 155 del Reglamento.

3.5. ADELANTOS

La Entidad puede entregar adelantos directos al contratista, los que en ningún caso exceden en conjunto del treinta por ciento (30%) del monto del contrato original, siempre que ello haya sido previsto en la sección específica de las bases.

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

3.6.2. OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la mencionada en el numeral precedente, según lo previsto en el artículo 163 del Reglamento y lo indicado en la sección específica de las bases.

Estos dos tipos de penalidades se calculan en forma independiente y pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

3.7. INCUMPLIMIENTO DEL CONTRATO

Las causales para la resolución del contrato, serán aplicadas de conformidad con el artículo 36 de la Ley y 164 del Reglamento.

3.8. PAGOS

El pago se realiza después de ejecutada la respectiva prestación, pudiendo contemplarse pagos a cuenta, según la forma establecida en la sección específica de las bases o en el contrato.

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

La conformidad se emite en un plazo máximo de siete (7) días de producida la recepción salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad del funcionario que debe emitir la conformidad.

En el caso que se haya suscrito contrato con un consorcio, el pago se realizará de acuerdo a lo que se indique en el contrato de consorcio.

Advertencia

En caso de retraso en los pagos a cuenta o pago final por parte de la Entidad, salvo que se deba a caso fortuito o fuerza mayor, esta reconoce al contratista los intereses legales correspondientes, de conformidad con el artículo 39 de la Ley y 171 del Reglamento, debiendo repetir contra los responsables de la demora injustificada.

3.9. DISPOSICIONES FINALES

Todos los demás aspectos del presente procedimiento no contemplados en las bases se regirán supletoriamente por la Ley y su Reglamento, así como por las disposiciones legales vigentes.

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 : HOSPITAL NACIONAL DANIEL ALCIDES CARRIÓN DE CALLAO
RUC N° : 20174943924
Domicilio legal : Av. Guardia Chalaca N° 2176 Bellavista Callao
Teléfono: : 01 - 614-7474 anexo 3251
Correo electrónico: : servicios@hndac.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de ADQUISICION DE SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE), SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE) Y ; EN EL(LA) EESS NAC. DANIEL A. CARRION - BELLAVISTA EN LA LOCALIDAD BELLAVISTA, DISTRITO DE BELLAVISTA, PROVINCIA CONSTITUCIONAL DEL CALLAO, DEPARTAMENTO CALLAO CON EL CUI N° 2554512

Ítem	Prestación	Sub Ítem	Descripción	Unidad de Medida	Cantidad Total
Paquete	Principal	1.1	Solución Hiperconvergente	Unidad	1
		1.2	Solución de Backup en Disco	Unidad	1
		1.3	Solución de Backup en Cinta	Unidad	1
		1.4	Solución de Seguridad - Ciberseguridad	Unidad	1
		1.5	Capacitación	Servicio Global	1
		1.6	Solución llave en mano (Instalación, configuración y migración)	Servicio Global	1

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante FORMATO N° 02 SOLICITUD Y APROBACIÓN DE EXPEDIENTE DE CONTRATACIÓN 16-2023-OL-HNDAC el 29 de mayo de 2023

1.4. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS

Importante

La fuente de financiamiento debe corresponder a aquella prevista en la Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal en el cual se convoca el procedimiento de selección.

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

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 máximo de noventa (90) días calendarios contando partir del día siguiente de suscrito el contrato 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/ 5.00 soles] en CAJA DE LA ENTIDAD DEL HOSPITAL NACIONAL DANIEL ALCIDES CARRIÓN.

Importante

El costo de entrega de un ejemplar de las bases no puede exceder el costo de su reproducción.

1.11. BASE LEGAL

Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N°30225, Ley de Contrataciones del Estado y sus modificatorias vigentes.

- Decreto Supremo N°344-2018-EF que modifica el Reglamento de la Ley de Contrataciones y sus modificatorias vigentes.
- Ley N° 31365 Ley de Presupuesto del Sector Público para el Año Fiscal 2022.
- Ley N° 31366 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2022.
- D.S N° 106-2019-EF y "Directiva N° 001-2019-EF/63.01 "Directiva General Del Sistema Nacional De Programación Multianual Y Gestión De Inversiones"
- Decreto Supremo N° 014-2011 –SA
- Decreto Supremo N° 016-2011-SA
- Ley N° 29783 Ley de Seguridad y Salud en el Trabajo y su Reglamento
- 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.

Importante

De conformidad con la vigesimosegunda Disposición Complementaria Final del Reglamento, en caso la Entidad (Ministerios y sus organismos públicos, programas o proyectos adscritos) haya difundido el requerimiento a través del SEACE siguiendo el procedimiento establecido en dicha disposición, no procede formular consultas u observaciones al requerimiento.

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos², 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 N° 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.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE³ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- d) Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

² La omisión del índice no determina la no admisión de la oferta.

³ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

Incorporar a las bases o eliminar, según corresponda

- e) Declaración jurada de plazo de entrega. **(Anexo N° 4)**⁴
- 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 N° 5)**
- g) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el **Anexo N° 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.

Importante

El comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.

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.

2.2.2. Documentación de presentación facultativa

Advertencia

El comité de selección no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites “Documentos para la admisión de la oferta”, “Requisitos de calificación” y “Factores de evaluación”.

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 fiel cumplimiento del contrato.
- b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- d) 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.
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

Advertencia

⁴ 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.

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁶ (**Anexo N° 11**).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) Detalle del precio de la oferta de cada uno de los bienes que conforman el paquete⁸.

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”.*
- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

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 Haya⁹.*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

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,

⁵ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gobiernodigital.gob.pe/interoperabilidad/>

⁶ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁷ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

⁸ Incluir solo en caso de contrataciones por paquete.

⁹ Según lo previsto en la Opinión N° 009-2016/DTN.

debe presentar la documentación requerida en MESA DE PARTES DEL HOSPITAL NACIONAL DANIEL ALCIDES CARRIÓN DE 08:00 AM A 13:00 HORAS ubicada en Av. Guardia Chalaca N° 2176 Bellavista Callao

Importante

En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de compra, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200,000.00).

Importante para la Entidad

2.5. ADELANTOS¹⁰

“La Entidad otorgará el 30% DEL MONTO DEL CONTRATO ORIGINAL

El contratista debe solicitar los adelantos dentro de LOS 08 (OCHO) DÍAS SIGUIENTES DE LA SUSCRIPCIÓN DE CONTRATO], adjuntando a su solicitud la garantía por adelantos¹¹ mediante carta fianza o póliza de caución acompañada del comprobante de pago correspondiente. Vencido dicho plazo no procede la solicitud.

La Entidad debe entregar el monto solicitado dentro de 07 (SIETE) DÍAS siguientes a la presentación de la solicitud del contratista”.

Incorporar a las bases o eliminar, según corresponda

2.6. FORMA DE PAGO

7.3. Forma de pago:

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en Único Pago.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Recepción de los bienes en el área de almacén.
- Informe del funcionario responsable del Oficina de Estadística y Sistemas Informáticos (OESI) emitiendo la conformidad de la prestación efectuada y la puesta en funcionamiento.
- Constancia de Capacitación al personal establecido en las EE.TT.
- Comprobante de pago.

Dicha documentación se debe presentar en MESA DE PARTES DE LA ENTIDAD HOSPITAL NACIONAL DANIEL ALCIDES CARRIÓN, sito en Av. Guardia Chalaca N° 2176 Bellavista Callao].

¹⁰ Si la Entidad ha previsto la entrega de adelantos, debe prever el plazo en el cual el contratista debe solicitar el adelanto, así como el plazo de entrega del mismo, conforme a lo previsto en el artículo 156 del Reglamento.

¹¹ De conformidad con el artículo 153 del Reglamento, esta garantía debe ser emitida por idéntico monto y un plazo mínimo de vigencia de tres (3) meses, renovable por un plazo idéntico hasta la amortización total del adelanto otorgado. Cuando el plazo de ejecución contractual sea menor a tres (3) meses, las garantías pueden ser emitidas con una vigencia menor, siempre que cubra la fecha prevista para la amortización total del adelanto otorgado.

CAPÍTULO III REQUERIMIENTO

ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICION DE SERVIDORES HIPERCONVERGENTES PARA EL HOSPITAL NACIONAL DANIEL ALCIDES CARRION

1. DENOMINACION DE LA ADQUISICION:

Adquisición de servidores Hiperconvergentes para el Hospital Nacional Daniel Alcides Carrión.

2. FINALIDAD PUBLICA:

El presente proceso busca implementar una infraestructura Hiperconvergente de alta especialización, donde dicha solución deberá encontrarse dentro del último cuadrante mágico de Gartner, y debería estar en el segmento de líderes, con el fin de garantizar que la solución cumpla todas las especificaciones solicitadas, esta solución deberá permitir el adquirir y/o renovar la tecnología de los servidores preexistentes, y a su vez salvaguardar la información y los sistemas del Hospital Daniel Alcides Carrión.

3. ANTECEDENTES:

Actualmente la entidad cuenta con nueve (09) servidores, cuyas capacidades ya han alcanzado su límite, por tal motivo la entidad requiere adquirir una Solución Integral de Última Generación para los Sistemas Informáticos, cuya capacidad técnica esté acorde a los requerimientos informáticos actuales y que cubran sus necesidades y demandas.

Item	Prestación	Sub Item	Descripción	Unidad de Medida	Cantidad Total
Paquete	Principal	1.1	Solución Hiperconvergente	Unidad	1
		1.2	Solución de Backup en Disco	Unidad	1
		1.3	Solución de Backup en Cinta	Unidad	1
		1.4	Solución de Seguridad - Ciberseguridad	Unidad	1
		1.5	Capacitación	Servicio Global	1
		1.6	Solución llave en mano (Instalación, configuración y migración)	Servicio Global	1

4. OBJETIVOS DE LA ADQUISICION:

4.1. Objetivo General:

El presente proceso tiene por objetivo aumentar la capacidad de procesamiento en la plataforma de servidores que se encuentran alojado en el Centro de Datos de la entidad; lo cual permitirá cubrir la demanda de procesamiento requerida para la ejecución de los proyectos informáticos actuales y en desarrollo.

4.2. Objetivo Especifico:

Garantizar la infraestructura adecuada para la implementación de los proyectos informáticos mediante la provisión del equipamiento para el desarrollo de dichas soluciones.



524

5. CARACTERÍSTICAS Y CONDICIONES DE LOS BIENES A CONTRATAR:

5.1. Descripción y cantidad de los bienes:

Todos los equipos deben ser nuevos de fábrica y estar en perfectas condiciones de uso, además de incluir los accesorios necesarios para su instalación.

5.2. Características técnicas mínimas para el Centro de Datos principal:

- El equipo deberá tener las configuraciones necesarias para poder trabajar en forma conjunta con la consola de administración y deberá ser del mismo fabricante.
- El proveedor deberá brindar todos los accesorios necesarios para poder poner en funcionamiento la solución solicitada.
- De ser necesario el proveedor deberá brindar las licencias que el hardware pueda necesitar para interactuar con la consola de administración; siendo estas licencias perpetuas.
- Deberá tener una configuración redundante.
- El equipo debe soportar hot swap para el crecimiento del mismo.
- Cada nodo deberá trabajar independientemente y de manera autónoma.
- Estar compuesta solamente por servidores (Nodos) basados en procesadores de propósito general. Cada nodo deberá tener almacenamiento Local en Discos Magnéticos (SAS Y/O SATA) y de estado sólido (tipo Flash / SSD).
- La solución deberá permitir integrar nodos/servidores con diferentes características en un solo gran clúster haciendo crecer la solución en demanda, que le permitan adaptarse a los requerimientos de cada una de las aplicaciones y formando un clúster mixto.
- Los tipos de nodos esperados son:
 - Intensivos en CPU/Memoria
 - Intensivos en Almacenamiento
 - Nodos solamente con discos SSD
- Deberá tener la opción de proveer una alta densidad de procesamiento permitiendo la integración de hasta 4 nodos/servidores por cada 2 unidades de rack, también se aceptarán nodos en formato de servidor de 1u o 2u de rack. Dichos nodos deben ser independientes cada uno, contando cada uno de ellos con su CPU/Memoria y discos, así como conexiones Ethernet propias para el armado del clúster.
- La solución deberá tener habilitada en todo el cluster la funcionalidad de automatizar la creación y upgrades de cluster Kubernetes, de manera que se puedan crear cluster Kubernetes con los volúmenes persistentes provistos por la solución, esta funcionalidad debe estar licenciada para todo el cluster.
- La alimentación Eléctrica de los nodos deberá ser de tipo Redundante (1+1), pudiendo ser compartida por los 3 nodos, siempre que se mantenga la redundancia.
- El detalle del equipo a proveer, será un equipo web scale Hiperconvergente para virtualización de máquinas de propósito general, que como mínimo deberá contener la siguiente capacidad Bruta (raw-capacity), previas a la compresión, de duplicación, RF2, RF3 o erasure-coding.



523

SERVIDORES (NODOS) HIPERCONVERGENTE:

Descripción	Características técnicas mínimas
Generalidades	<p>El equipamiento debe considerar los servicios de administración de la solución, los que deberán considerar redundancia para la misma.</p> <p>El postor debe considerar todo lo necesario para asegurar que la capa de administración de la solución cuente con Alta Disponibilidad.</p> <p>El equipo debe soportar hot swap para el crecimiento de este. Cada nodo deberá trabajar independientemente y de manera autónoma.</p> <p>La Solución estará compuesta solamente por servidores (Nodos) basados en procesadores de propósito general. Cada nodo deberá tener almacenamiento Local en Discos y deberá estar basado en discos SAS ó SATA o SSD.</p> <p>Los procesadores deberán ser basados en Arquitectura actual x86.</p> <p>La solución deberá permitir integrar nodos/servidores de diferentes generaciones y con diferentes características en un solo gran clúster haciendo crecer la solución en demanda, que le permitan adaptarse a los requerimientos de cada una de las aplicaciones y formando un clúster mixto.</p> <p>La solución deberá estar listada en el cuadrante mágico de Gartner, en el cuadrante de líderes.</p>
Cantidad mínima	La Solución deberá tener como mínimo 6 nodos.
Solución Hiperconvergente	La solución de hiperconvergencia por definición es cómputo, virtualización y storage totalmente definido por software.
Procesadores por nodo como mínimo:	Procesadores para Servidores de última generación Cantidad de núcleos mínimo de 28 Core y subprocesos mínimo 56, Cache mínimo de 52Mb y que soporte como mínimo 6 Tb de memoria y tipo de velocidad de memoria 3200 MHz.
Memoria RAM por nodo como mínimo:	Mínimo 512 GB por nodo.
Conexiones LAN por nodo como mínimo:	Dos (02) puertos 10/25Gbps (Integradas o con tarjeta controladora) Se Conectará al Switch existente, los accesorios para la conectividad al switch actual serán cubierto en la propuesta del CONTRATISTA.



Almacenamiento	<p>El almacenamiento definido por Software utilizando los recursos de los nodos debe ser unificado y disponible para todos los nodos del Cluster. Deberá entregar como mínimo la siguiente capacidad total descrita. Las capacidades solicitadas son netas utilizables reales (para datos y/o VMs del usuario), luego de descontar cualquier Overhead que pueda ser consumido por la infraestructura Hyperconvergente en sí misma.</p> <p>Se deberá garantizar la capacidad mínima solicitada luego de aplicar un esquema de protección por doble copia (FFT1, RF2 o RAID1), y considerando la salida de servicio de uno de los nodos (Redundancia de Nodo N+1) con capacidad de recuperar el esquema de protección por doble copia (FFT1, RF2 o RAID1) utilizando la capacidad de los N-1 nodos restantes:</p> <p>Espacio total UTILIZABLE para escritura en el Clúster: 240TIB mínimo efectivo. De esta capacidad total, como mínimo deberá entregarse 120 TB RAW sobre discos de estado sólido (SSD), mientras que la capacidad restante puede ser sobre discos magnéticos/mecánicos tradicionales (HDD)</p> <p>Si bien se solicita que la solución provista pueda aplicar y tenga licenciada la funcionalidad de compresión y deduplicación a los datos almacenados, la capacidad solicitada deberá ser entregada sin considerar ahorro alguno por compresión ni deduplicación de los datos de usuario. De esta forma si al aplicar estos algoritmos se lograra un ahorro de los datos almacenados, eso redundará en un aumento de la capacidad disponible por sobre los valores indicados, el cual será aprovechado por el usuario como una capacidad extra.</p>
Administración de la solución	<p>Permitir analizar de manera predictiva, el uso de los recursos del clúster (memoria, discos y procesamiento).</p> <p>Permitir el análisis del comportamiento de una máquina virtual, Permitir su optimización automatizada en caso no esté usando los recursos de manera eficiente.</p> <p>Permitir analizar de manera gráfica, la estadística de las cargas de trabajo, permitir proyectar crecimientos, para luego recomendar un upgrade de recursos (memoria, disco y procesamiento) que soporte ese crecimiento futuro (Capacity Planing).</p>
Gestión de Datos almacenados como mínimo:	La solución debe realizar réplicas de datos almacenados a través de los nodos del clúster.
Alta Disponibilidad como mínimo:	La solución de Hiperconvergencia debe permitir alta disponibilidad ante la caída de uno de los nodos.
Soporte de replicación	<p>La plataforma de Hiperconvergencia deberá de soportar replicación a una o más locaciones remotas, ante un desastre de manera Síncrona y/o Asíncrona, e integrado a la solución de administración de la solución.</p> <p>La funcionalidad de réplica deberá tener la capacidad de replicar entre distintas ciudades a nivel nacional.</p>
Crecimiento de clúster	Proveer un crecimiento lineal, estable y predecible en su rendimiento a medida que se agreguen servidores/nodos. Soportar un crecimiento mínimo de 64 nodos por clúster, que incrementen la capacidad de procesamiento, memoria y almacenamiento. El clúster una vez establecido debe ser capaz de crecer de aun nodo por vez.



Alta disponibilidad	La solución de hiperconvergencia debe considerar ante la caída de un nodo, levantar la máquina virtual en otro nodo automáticamente realizando la funcionalidad de alta disponibilidad.
Compatibilidad con hardware	La plataforma de la solución Hiperconvergente, al ser software, podrá encontrar compatibilidad con varios fabricantes de hardware, con el fin de poder escoger la mejor plataforma de hardware disponible.
Integración de la solución por el fabricante	La plataforma de software Hiperconvergente deberá ser de tipo OPEN de manera que no esté asociado al servidor físico, con el fin de poder mantener el licenciamiento y poder reemplazar el hardware de forma independiente, cuando este llegue a cumplir su vigencia tecnológica, de ser necesario contando además con derecho a actualizaciones y soporte del fabricante directo de software en la modalidad de 3 años x 24 x 7 x 4 horas
Gestión Automatizada	La solución debe permitir actualización de Firmware, drivers y software de la solución Hiperconvergente en forma no disruptiva, es decir sin para ni reinicio de la plataforma.
Hypervisor	La plataforma de Software Hyperconvergente deberá de soportar los hypervisores más conocidos del mercado, como por ejemplo VmWare, Hyper-V, KVM, etc.
Copia de seguridad	La plataforma de Software Hyperconvergente debe contar con soporte para suministrar copias en línea consistentes para las máquinas virtuales entre todos los nodos. Este punto no está considerado como replicación.
Seguridad	La solución deberá tener habilitada la funcionalidad de Microsegmentación de redes, definida por software, habilitada desde el principio la que deberá asignar políticas de acceso a red a grupos específicos de VMs, permitiendo tráfico entre ellos en base a políticas configurables en la solución de administración de la solución Hiperconvergente. La política deberá contar con capacidades de actualizarse automáticamente según el ciclo de vida de las VM involucradas. El licenciamiento debe ser parte de la oferta del postor.
Consideraciones	La solución debe de administrarse desde una consola de gestión centralizada. La solución debe soportar una administración centralizada para la administración global de los futuros sitios remotos. La solución debe permitir la gestión en el mismo cluster de nodos híbridos de almacenamiento, es decir soportar unidades de estado sólido (SSD) y discos magnéticos o mecánicos. Asimismo, deberá de soportar soluciones de sólo discos de estado sólido (SSD) a fin de brindar una solución de almacenamiento de alto rendimiento
Automatización	La solución deberá incluir una funcionalidad que permita el despliegue asistido de Clusters Kubernetes multi-master, manejando tanto el deployment automatizado del Cluster, Scale-Out de Cluster Kubernetes, Upgrade de imágenes, Storage Persistente, Monitoreo Logging, y alertas. Esta funcionalidad deberá estar incluida y licenciada para todos los nodos de los clusters Hyperconvergentes ofertados, sin límite de capacidad.



520

Almacenamiento	Almacenamiento FileSharing (NAS): Capacidad de ofrecer nativamente y de manera distribuida un File Sharing corporativo para los usuarios, con soporte para protocolos SMB / NFS integrado con Active-Directory (incluyendo permisos, cuotas, etc.). Este Sistema deberá distribuir y proteger los datos en el Cluster Hyperconvergente, garantizando escalabilidad en cantidad de usuarios e integración con Snapshots del Sistema. La gestión de esta solución de FileSharing deberá estar integrada en la misma consola de Gestión del Cluster Hyperconvergente. Se debe incluir licencia para capacidad de hasta 20 TB de almacenamiento para este propósito (permitiendo al cliente expandir esta capacidad a futuro mediante licenciamiento adicional)
	Capacidad de ofrecer nativamente y de manera distribuida almacenamiento por Objetos. El acceso al almacenamiento por Objetos deberá ser compatible con el API S3 mediante HTTPS, y permitir políticas de tipo Write Once Read Many (WORM). La capacidad de ofrecer Storage por objetos debe poder escalar en capacidad agregando nodos de la misma forma que el Cluster Hyperconvergente. La gestión de esta solución de Object Storage deberá estar integrada en la misma consola de Gestión del Cluster Hyperconvergente. Se debe incluir licencia para capacidad de hasta 5 TiB de almacenamiento para este propósito (permitiendo al cliente expandir esta capacidad a futuro mediante licenciamiento adicional) La solución deberá ser compatible con soluciones de Escritorios Virtuales (VDI), tales como VMWare Horizon Enterprise y Citrix Virtual Desktop and Application solutions
	La solución hyperconvergente definida por software, deberá tener la capacidad habilitada para entregar a través de protocolo iSCSI el almacenamiento a servidores externos
	Adicionalmente la solución de réplica debe de permitir replicar máquinas virtuales entre hipervisores diferentes para poder facilitar la migración de un hipervisor a otro. Esta funcionalidad podrá ser nativa o tenerla habilitada con software de terceros, deberá tener licencia de funcionamiento durante todo el tiempo de soporte de la plataforma.
Replicación	La solución deberá tener la capacidad habilitada para realizar Backups y Restaurar copias de las máquinas virtuales y archivos desde una nube pública dentro de las más conocidas como Amazon o Azure.
	Se deberá entregar una herramienta grafica que permita el análisis detallado de consumo de los IOPS, ya sea en discos físicos SSD, HDD del cluster. Se deberá entregar una herramienta grafica que permita el análisis en tiempo real el consumo de los recursos de CPU, Memoria Ram y almacenamiento de las máquinas virtuales
Monitoreo	
Hypervisor	El Hypervisor deberá tener habilitada la funcionalidad de migrar entre nodos las máquinas virtuales en ejecución sin interrupciones, además en caso que un host físico esté sobre cargado o se requiera realizar mantenimiento, el hypervisor automáticamente deberá mover la máquina virtual en ejecución o encendida (Power On), sin interrupción, a otro Host, Nodo o Servidor.



Administración de la solución	<p>La consola de Gestión deberá ejecutarse sobre los mismos nodos del cluster que administra, aprovechando la Alta Disponibilidad del mismo (Ej. La consola debe permanecer disponible ante la falla de cualquiera de los nodos).</p> <p>La solución deberá tener habilitada la funcionalidad de balancear las cargas de las máquinas virtuales existentes en el cluster.</p> <p>La solución deberá poder sacar reportes de VMs sobreaprovisionadas</p> <p>La consola de gestión deberá permitir administrar y monitorear a todos los Servidores/Nodos que forman parte del cluster, así como el hypervisor y toda la plataforma virtual</p> <p>Deberá ser accedida mediante un browser y estar basada en HTML5.</p> <p>Deberá proveer una única vista para todo el entorno Virtual</p> <p>La Consola de Gestión deberá poder mostrar:</p> <p>Visualizar la capacidad total de la memoria RAM del cluster</p> <p>Visualizar el consumo en iops de las máquinas virtuales</p> <p>Verificar la salud actual del Entorno Virtual</p> <p>Poder realizar un análisis predictivo de los host pertenecientes al cluster.</p> <p>Análisis y visibilidad unificada del almacenamiento.</p>
Servicios Avanzados	<p>La solución deberá considerar el licenciamiento o suscripción para poder entregar una solución de escritorio como servicio (Desktop as a service), que permita entregar una sesión de escritorio virtual desde un navegador estándar que esté basado en HTML5. Lo anterior debe permitir el ingreso de 20 usuarios nombrados a la solución, y podrá desplegarse en los nodos solicitados, o en los nodos actuales de la entidad. La entidad brindará las licencias de sistema operativo cliente y servidor de la solución, así como las licencias de los aplicativos a utilizar.</p>
Trabajo Remoto	<p>Se debe poder personalizar el espacio de trabajo del usuario, pudiendo elegir entre diferentes configuraciones de aplicaciones y escritorios, incluso poder acceder a instancias con diferentes configuraciones hardware memoria y CPU.</p> <p>Gestión de imágenes simplificadas, con posibilidad de realizar copia y restauración, además de mover imágenes máster en la nube.</p> <p>Posibilidad de reproducción multimedia, sonido, video, audio mediante escritorio virtual con alto rendimiento de hasta 60 fps.</p> <p>Acceso a aplicaciones y escritorios desde navegador HTML5, sin necesidad de instalar software de cliente pesado.</p> <p>Conectividad con herramientas de gestión de datos colaborativos, tipo: OneDrive, Dropbox, GoogleDrive, Box.</p> <p>Integración con proveedores de identidad, doble factor de autenticación, Directorio Activo /ADFS, SAML2.</p> <p>Se debe permitir el uso de escritorios persistentes y no persistentes para contemplar diferentes perfiles de usuarios.</p> <p>Flexibilidad en el modelo de licenciamiento, pudiendo elegir entre usuarios nominales o concurrentes.</p> <p>Virtualizar aplicaciones y escritorios, tipo Windows o Linux.</p>



Sistema de Archivos	<p>La solución debe incluir una solución de almacenamiento especializada en archivos, que haga uso de la misma plataforma de hiperconvergencia ofertada (sin el uso de otro software adicional de terceros), que permita crear repositorios que pueden distribuirse entre los nodos del clúster de la solución, y que entreguen funcionalidades nativas de un servidor de archivos, como son:</p> <ul style="list-style-type: none">Cuotas a nivel de usuarioAutoservicio del usuario para recuperación a nivel de archivoRecursos compartidos / exportaciones SMB y NFS separados en el mismo servidor de archivosIntegración con auditores habilitadosCopia de seguridad nativa y recuperación ante desastresSoporte de escaneo antivirus en líneaSoporte de compresión <p>Se deberá incluir el uso de 50 TIB para la presente oferta, como mínimo.</p>
---------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



SOLUCIÓN DE BACKUP EN DISCO

El equipo deberá tener las siguientes características:

Debe hacer uso de sistemas de almacenamiento de respaldo en disco, basado en "appliance" con un propósito específico de ingestión de datos de copia de seguridad, deduplicación y replicación. Debe tener procesamiento y almacenamiento integrados.

La capacidad mínima de almacenamiento en disco nativo debe ser de al menos 99 TB (Terabytes) útiles, instalados y licenciados sin contar ni con pérdidas causadas por las redundancias (RAID y Hot-Spares) ni ganancias obtenidas con compresión y / o deduplicación, archivo y otras tecnologías que puedan influir en la capacidad mínima requerida.

El equipo ofrecido debe escalar al menos hasta 315 TB de capacidad neta, en un único pool deduplicación sin considerar el uso de almacenamientos externos o de nube para ampliar su capacidad.

El equipo ofertado debe hacer uso de discos SSDs en su nodo de procesamiento con el objetivo de aceleración del rendimiento.

El Dispositivo ofrecido y sus componentes (hardware y software) deben ser nuevos, sin uso previo y fabricación en línea en la fecha de entrega.

Debe tener al menos 06 (seis) puertos LAN Ethernet de 10 Gbps con conectores LC-LC, así como sus respectivos GBIC's / SFP's, para datos, gestión y registro de copias de seguridad a través de LAN.

Debe tener al menos 01 (un) puerto LAN Ethernet de 1 Gb con conectores RJ45, para datos, gestión, replicación, y registro de copias de seguridad a través de LAN.

Debe tener al menos 04 (cuatro) puertos FC - Fibra de Canal con velocidad mínima de 16Gbps (cada) con sus respectivos conectores para presentación a través de VTL.

El rendimiento nativo mínimo en grabación de 20 (veinte) TB/h (TeraBytes por hora) en modo NAS (CIFS o NFS) con deduplicación.

El rendimiento nativo mínimo en la grabación de 24 (veinte y cuatro) TB/h (TeraBytes por hora) en modo OST con deduplicación.

El rendimiento nativo mínimo en la grabación de 35.4 (treinta y cinco puntos cuatro) TB/h (TeraBytes por hora) en modo VTL con deduplicación.

El rendimiento con aceleradores mediante software debe ser de al menos 95 (Noventa y cinco) TB/h (TeraBytes por hora).

*El equipo ofertado debe utilizar discos con protección no menor a RAID 6 o tecnología que proporcione seguridad y rendimiento equivalentes a RAID 6 (máximo de catorce discos por grupo). lo que sumado al área "Hot Spare", proporcionará protección de datos y desempeño de acuerdo con la información técnica del equipo disponible públicamente.

Si la Solución no dispone de "Hot-Spare" o funcionalidad equivalente, el licitante debe proporcionar un dispositivo adicional con las mismas características que el original con fines de replicación, garantizando el acceso y la integridad de los datos.*

Debe permitir la instalación de un rack estándar de 42U, sin exceder la profundidad de 1 (un) metro.

Capacidad de operación y licenciamiento para operar en modo multiprotocolo, con ingesta simultánea por a través de OST, tecnología Open Storage; NAS: mediante protocolos CIFS y NFS; VTL (Virtual Tape Library)

La deduplicación será en tiempo real (en línea) de los datos recibidos para escribir en el disco, no se aceptará el uso de áreas de manobra para la recepción de datos y posterior duplicación.

Debe realizar la deduplicación global, es decir, un único grupo de deduplicación por sistema, deduplicando así globalmente todos los datos de cualquier protocolo (CIFS, NFS, OST y VTL), cliente y / o aplicación. Debe permitir la operación simultánea de todos los protocolos CIFS, NFS y VTL.

Cada cartucho de cintas emulado asignará dinámicamente un espacio de disco equivalente el volumen de datos recibidos, no pudiendo pre asignar la capacidad total de la cinta. (Solo si necesario VTL)

Si no admite la deduplicación global entre todos los recursos compartidos y protocolos, deberá agregarse un 50% de espacio adicional al solicitado con un mínimo de 150TB de espacio usable para mitigar la menor eficiencia en el proceso de reducción de datos.

La deduplicación segmentará automáticamente los datos en bloques de tamaño variable. Debe habilitar la deduplicación en todo el espacio de almacenamiento ofrecido.



La función de deduplicación de datos se realizará directamente con la ingestión y replicación de datos, eliminando la necesidad de almacenamiento intermediario para el almacenamiento en caché de datos. La deduplicación debe tener lugar antes de la grabación de los datos en los discos del appliance. Debe poseer y tener licencia para almacenar datos cifrados sin que haya un impacto en el rendimiento de los equipos ofrecidos.

Si hay un impacto en el rendimiento para realizar el cifrado de datos almacenado, el requisito de rendimiento mínimo debe ser de 40 TB / hora, nativo sin considerar el uso de aceleración del software. Debe tener un software de replicación licenciado para replicar datos deduplicados con otro equipo idéntico, a través de la red TCP/IP. La replicación que se realiza a través del enlace IP, permite el ajuste del ancho de banda de replicación dinámica automatizada mediante programación a través de la interfaz de administración.

Debe verificar constante y automáticamente la integridad de los datos almacenados, de forma nativa, no aceptando la personalización de scripts para esta funcionalidad. Capacidad para emular un mínimo de 64 "shares" en modo NAS.

Debe proporcionar acceso a la consola de gestión a través de una interfaz WEB.

La consola de gestión debe ofrecer: Información de discos y / o Raid groups; información sobre interfaz de canal de fibra y LAN; información sobre el uso de capacidad física y lógica (antes y después de la deduplicación y la compresión); tasa de deduplicación.

El dispositivo debe tener la capacidad auto-monitoreo, detección de fallos, generación de registros, envío de correos electrónicos y traps SNMP.

Software incluido para configuración, gestión, monitorización compatible con Windows/Linux y con licencia para la capacidad solicitada del equipo.

Alimentación: al menos 2 (dos) fuentes de alimentación de tensión eléctrica redundantes clasificado hasta 240 V (doscientos cuarenta voltios) CA a 60 Hz (sesenta hercios). Las fuentes deben trabajar en paralelo para que en caso de falla de uno de ellos (o un grupo de ellos) el resto asume toda la potencia del sistema sin perjuicio de su corrección operación, las fuentes que componen la solución deben permitir su adición y reemplazo sin interrumpir el funcionamiento del sistema de almacenamiento (ENCHUFE o INTERCAMBIO EN CALIENTE);

La solución ofrecida debe integrarse de forma nativa con el software de respaldo.

La solución de dispositivo ofrecida debe admitir y tener una licencia completa para realizar copias de seguridad utilizando aceleradores proporcionados por el fabricante del dispositivo y que operan de forma integrada con la solución de software propuesta.

La solución ofrecida debe admitir al menos, simultáneamente, 40 flujos de escritura de datos, o 25 secuencias de escritura y 15 secuencias de lectura.

La solución ofrecida debe proporcionar la capacidad de mantener el proceso IVMR (Instant VM Recover) para hasta 15 (quince) servidores simultáneamente sin afectar procesos de respaldo y mantenimiento de la capacidad de poner en funcionamiento los 15 servidores directamente desde el grupo de deduplicación, para el movimiento posterior a la virtualización.

La solución ofrecida debe poder realizar la replicación de datos durante la ejecución procesos de copia de seguridad para reducir las ventanas de réplicas con actualización automática del catálogo del software de respaldos.

Deberá contar con un mecanismo de protección contra ataques de Ransomware, asegurando la protección y / o recuperación del sistema de almacenamiento de copias de seguridad en caso de ataques.

Como mínimo el Soporte debe ser de: 24x7 telefónico, Next Business Day en reposición de partes y piezas.

La solución ofertada debe soportar la integración comprobada por matriz de compatibilidad con el software Oracle RMAN, permitiendo que la copia de seguridad y restauración de la base de datos



Oracle se realice directamente en el Appliance de forma deduplicada, sin el uso de scripts o software de Backup Esta funcionalidad debe estar totalmente licenciada.

SOLUCIÓN DE BACKUP LIBRERÍA

El equipo deberá tener las siguientes características:

Cada módulo de biblioteca de cintas robótica debe tener al menos 50 ranuras para cintas magnéticas y poder crecer hasta 400 ranuras agregando módulos de expansión.

La librería deberá contar con un licenciamiento mínimo de 50 Slots.

La librería de cintas deberá contar con 3 (TRES) Tape drives standard de media altura (HH: Half Height) LTO-8

La librería de cintas deberá poseer como mínimo 100 slots físicos para cintas magnéticas (cartridge slots);

Se deberán entregar 100 (cien) cintas LTO 8 para de datos y 10 (Diez) LTO de limpieza;

Los slots deberán ser compatibles con las cintas LTO-8 y LTO-7 formato M8.

*Las unidades de almacenamiento LTO-8 deberán tener una tasa de grabación nominal mínima de 300MB/seg. pudiendo almacenar hasta 12,8 TB de datos en un único cartucho sin compresión de datos *

Ser escalable hasta 400 (Cuatrocientos slots) para cintas magnéticas (cartridge slots) agregando módulos para almacenamiento de cintas y drives

Deberá ser escalable hasta el mínimo de 24 Tape Drives con un factor de forma de media altura (Half Height) agregando módulos de expansión adicionales.

Cada módulo de expansión deberá tener un factor de forma de 3U's y deberá permitir crecimiento de número de slots y Tape Drives.

Cada módulo de expansión deberá permitir poder albergar hasta 3 Drives de media altura (HH) y 50 slots para almacenamiento de medios.

El mismo brazo mecanismo robótico debe tener acceso a todos los slots y tape drive de la librería independientemente de la disposición de los slots en los módulos de control o expansiones.

Cualquier otro tipo de media que necesite slots como, por ejemplo: Tape Clean, Cintas para diagnósticos, importación o exportación de cintas, etc., deberá tener su propia cantidad de slots asignada siguiendo las recomendaciones del fabricante recogidas en la propuesta del proveedor.

El equipo ofertado deberá permitir la adición de módulos para expansión de capacidad de almacenamiento

Los lectores de cintas deberán permitir conectividad FC 8Gbps o 6Gbps SAS y proporcionar los cables necesarios para conexión a los hosts.

Debe soportar la división lógica de la biblioteca hasta en 24 (Veinticuatro) particiones, y permitir la gestión independiente de las mismas.

Deberá permitir la carga de cintas en la estación de entrada / salida (estación de E / S o cargador) sin interrumpir la operación, manteniendo la biblioteca de cintas en condición activa o en línea.

La librería de cintas debe soportar la designación de al menos 5 mail slots por partición independientemente de la cantidad de particiones de la librería.

*La librería contará con protección contra Ransomware utilizando barreras físicas para impedir el acceso al dato:

- Función de "air-gap", que permita el almacenamiento de cintas en una partición off-line (inaccesible para la herramienta de copia de seguridad).

Deberá permitir que todas las ranuras instaladas físicamente en la solución (con o sin licencia de escritura) se utilicen para este propósito. En caso de que no se cumpla con este requisito, todos los slots físicos instalados en la solución ofrecida deben tener licencia para usar la herramienta de respaldo. El número mínimo de slots en la partición fuera de línea debe ser de 50.



- Función de Ransom Block, las cintas ocuparan una posición de stand by, siendo expulsadas solo parcialmente de las ranuras de cintas para impedir el acceso físico a los datos. El robot debe poder escanear los códigos de barras de la cinta, de modo que los administradores del sistema puedan realizar auditorías periódicas y asegurar que las cintas aún estén presentes, pero inaccesibles a través de la red. Para que las cintas sean accesibles, será necesaria la acción física de insertarlas completamente en sus ranuras."

En caso de que la librería ofrecida no cuente protección física de acceso a datos "Anti Ransomware", se deberá entregar una segunda librería con similares características. La librería deberá permanecer Off Line y se encargará de realizar copia adicional de los datos a proteger resultando inaccesible en la red. Debe contar con al menos 50 Slots licenciados y 3 drives LTO8 HH.

La librería de cintas deberá soportar MFA (Multi Factor Authentication).

La librería de cintas debe mantener las operaciones de Backup durante los procesos de inserción y extracción de cintas a través de su estación de entrada y salida (mail slot), independientemente de la cantidad de particiones existente.

La librería de cintas debe permitir actualizaciones automáticas de códigos y Firmware, previa configuración por parte del administrador del sistema.

La librería de cintas deberá tener sensores internos capaces de controlar y almacenar informaciones de temperatura y humedad para garantizar las condiciones ambientales de las cintas almacenadas internamente en la librería.

Debe poder realizar el inventario de los cartuchos almacenados en el sistema.

Debe poder enviar alertas automáticas sobre eventos de falla.

El mismo mecanismo robótico debe tener acceso a todos los slots de la librería de cintas.

Debe tener MSBF ((Mean Swap Between Failure) por encima de 2.000.000 de operaciones.

EL software de gestión debe informar el uso por drive permitiendo el análisis de sobre uso de los mismos.

EL software de gestión debe informar cantidad de montajes por cinta

EL software de gestión debe informar el volumen de datos transferido por unidad

EL software de gestión debe informar el número de fallos por cartucho

EL software de gestión debe informar fallos de las unidades unidades

El acceso remoto a la consola de administración de la unidad de cinta permitirá el control de acceso de usuarios.

La unidad de almacenamiento robótica debe tener un panel frontal de gestión LCD.

Deberá poder mostrar el número de veces que una determinada cinta fue solicitada y leída.

Deberá ser capaz de enviar informes con el análisis de Integridad de las cintas, Análisis de utilización de cintas, Análisis de Utilización de Lectores y reportes de seguridad para casos en los que las cintas fueron extraídas de forma no autorizada.

Debe poseer mecanismos de monitoreo de humedad y temperatura

Debe disponer de control de inserción y extracción de cintas generando reportes a través de un interfaz gráfico.

Debe contar con todos los cables, railes, conectores, lectores, manuales de instalación de software, necesarios para la puesta en marcha y perfecto funcionamiento de la librería de cintas.

Disponer de alimentación eléctrica entre 200 (doscientos) y 230 (doscientos treinta) Voltios, frecuencia de 60 (sesenta) Hertz, y debe ser redundante por 02 (dos) o más fuentes externas independientes para evitar parada en caso de avería de una de las fuentes.

"Las fuentes de Alimentación eléctrica deben contar con el certificado mínimo 80 Plus, garantizando la eficiencia energética del equipamiento ofrecido."

Como mínimo el Soporte debe ser de: 24x7 telefónico, Next Business Day en reposición de partes y piezas.



ADQUISICIÓN DE UN PAQUETE DE LICENCIAMIENTO DE SOFTWARE

Windows Server Data Center para la totalidad de los sistemas operativos y máquinas virtuales a implementar en la solución de hiperconvergencia solicitada

Calculadora de Licenciamiento Windows Server por Núcleo (Core) por servidor como mínimo

LICENCIAMIENTO POR NODO

Número de procesadores físicos en el servidor	:	02
Número de núcleos físicos en el servidor	:	40
Total, de núcleos necesarios a ser licenciados	:	80

Requerimientos de Licenciamiento

Licencia Base Requerida	
Windows Server Datacenter	: Lo que corresponda

Licenciamiento Global

Cantidad de Nodos	:	06
Cantidad de Procesadores Físicos	:	12

Calculadora de Licenciamiento de Base de Datos SQL por servidor como mínimo

Licencia Base Requerida	
SQL Server Edición Enterprise	: 02



**SEGURIDAD GESTIONADA
SOLUCIÓN DE FIREWALLS PERIMETRALES**

DESCRIPCIÓN

Se requiere de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.

La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad, es decir por lo menos 2 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones.

El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes.

El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls

El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Automated Malware Analysis.

El fabricante debe poseer todos los componentes necesarios para adoptar una arquitectura de Zero Trust, debe haber sido catalogado como líder en el último reporte de Forrester Wave: Zero Trust Extended Ecosystem Platform Providers

El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.

La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.

La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.

a. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.

Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware de un día para otro o NBD (next business day).

Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Postor.

Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante, así como exámenes y certificaciones

Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución.

Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. Se requiere que la propuesta incluya documentación pública sobre dicha herramienta explicando su alcance.

La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.



La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.

CAPACIDADES DE EQUIPOS

Throughput de Next Generation Firewall de 2.7 Gbps medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

Throughput de Prevención de Amenazas de 1.3 Gbps medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.

El equipo debe soportar como mínimo 280.000 sesiones simultáneas y 45.00 sesiones por segundo, medidos con paquetes HTTP de 1 byte.

Debe contar con fuente de poder redundante.

Almacenamiento de 120 GB o superior.

Mínimo ocho (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red



CARACTERÍSTICAS GENERALES

El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.

Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).

Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.

Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.

Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.

Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.

Soportar túneles GRE como punto inicio o finalización del túnel.

536

Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales

ALTA DISPONIBILIDAD

Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3).
La configuración en alta disponibilidad debe sincronizar: Sesiones, Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red.
Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces.
Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

FUNCIONALIDADES DE FIREWALL

Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
Permitir el agendamiento de las políticas de seguridad.
Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría.
Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.

DESCIFRADO DE TRÁFICO SSL/TLS

Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.



Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS

Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).

Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio

Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.

Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.

Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).



CONTROL DE APLICACIONES

Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email.

Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2

Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.

Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.

Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.

Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dms, lccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.

Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.

Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.

Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.

Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.

Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.

PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)

Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.

Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa

La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)

La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS

Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo

La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección.

Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route

Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethernertype (Hex).

Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.

PREVENCIÓN DE AMENAZAS CONOCIDAS

Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.

Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos

Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.

El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.

30%

Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.
Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos items.
Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.
Debe identificar las consultas que realizan los hosts infectados: hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.
Los eventos deben identificar el país que origino la amenaza.
Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

ANÁLISIS DE MALWARE DE DÍA CERO

La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.

La plataforma de Sandboxing debe ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.

El Next Generation Firewall debe tener capacidad de analizar 20 archivos por minuto al Sandbox Cloud.

Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines)

Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.

Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras.

El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.

Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, FedRAMP.

Deberá contar con una acreditación que el servicio se encuentra alineado a los estándares HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) y PCI (Payment Card Industry Data Security Standard). Esta acreditación deberá ser dada por una entidad tercera al fabricante.

El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.

Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante.

Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.

El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.

Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.

Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.

Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e .class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.

Permitir la subida de archivos al sandbox de forma manual y vía API.

Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.

La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

FILTRO DE CONTENIDO WEB

Permite especificar la política por tiempo, horario o determinado periodo (día, mes, año, día de la semana y hora)

Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.

Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs

Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.

Debe permitir la creación de categorías personalizadas.

Debe soportar la categorización o crawling de URLs hasta en 40 idiomas

Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.

Debe evitar vulnerabilidades de JavaScript y contenido phishing en el tráfico web utilizando un motor tiempo real basado en machine learning

Debe utilizar machine learning para analizar URL en tiempo real y clasificarlas en categorías benignas o maliciosas

Debe ser capaz de bloquear URLs maliciosas no vistas con anterioridad, es decir, URLs que no hayan sido categorizadas previamente por el fabricante

Debe poseer algoritmos que evalúen URLs en tiempo real para bloquear URLs no categorizadas por crawlers, inclusive URLs resistentes a técnicas de cloaking

Debe incluir escaneo en línea basado en machine learning para detectar ataques de phishing no vistos antes

Debe poseer capacidades anti evasivas para contener evaluaciones de cloaking, Captchas y codificación de caracteres

Debe emplear modelos de aprendizaje automático para analizar imágenes en páginas web y determinar si están imitando marcas conocidas, previniendo intentos de phishing.

Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.

Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.

Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo ataques de phishing.

IDENTIFICACION DE USUARIOS

Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.

Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.

Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.

Debe disponer de un servicio en nube o onpremise que extraiga automáticamente la información del usuario grupos de usuario de varios IDPs y proveedores de SSO como Azure AD, okta, Google Identity y PingID y la ponga a disposición de los NGFW para ser incluidos en la política de seguridad.

Debe disponer de un servicio en nube o onpremise que simplifique la autenticación SAML de usuarios, que actúe como Service Provider único frente a IDPs o proveedores de SSO

Debe disponer de un servicio en nube o onpremise que almacene todos los grupos disponibles del Active Directory, los filtre y ponga a disposición únicamente los grupos necesarios que el NGFW utilice en la política de seguridad

Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.

Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.

Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.

Debe permitir la definición de grupos dinámicos de usuarios.



FILTRO DE DATOS

Los archivos deben ser identificados por extensión y firmas.

Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.

Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos via expresión regular.

VPN

Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.

La VPN IPSec debe soportar como mínimo:

- DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
- Autenticación MD5, SHA-1, SHA-2;
- Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
- Algoritmo Internet Key Exchange (IKEv1 & IKEv2);

504

Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.

Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.

Soportar autenticación via AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).

Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.

Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.

Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:

- Antes del usuario se autentique en la estación;
- Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
- Bajo demanda del usuario;

El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X.

Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.

CONSOLA DE ADMINISTRACION Y MONITOREO

Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante

Permitir exportar las reglas de seguridad en formato CSV y PDF

Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.

Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.

Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)

Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.

Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.

Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).

Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).

Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.

Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (Integrándose a un servidor SMTP).



Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración;

Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.

Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.

Debe permitir el estándar OpenConfig (OC) para automatizar las tareas de configuración del NGFW.

La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

PRESTACIÓN ACCESORIA SOPORTE TÉCNICO

Durante el período de garantía comercial, debe contar con un Centro de Operaciones de Seguridad para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.

El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio en la entidad, así como a la pérdida de la calidad o degradación del mismo. A todo ello se le denominará "falla".

El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".

El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.

El servicio de soporte técnico debe entregar en una recurrencia mensual informes sobre la solución implementada, a nivel de detalle de la totalidad de incidencias generadas en el período de tiempo.

Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.

El postor deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca.

El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del postor, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.

GARANTÍA COMERCIAL

Se requiere que se brinde una garantía comercial de 48 meses del sistema / plataforma adquirida. La garantía debe ser otorgada por el postor y confirmada por el fabricante o el representante de la marca en el país.

Las características de la garantía solicitada son:

- o Las garantías y soporte iniciarán su vigencia desde el momento que se otorgue la conformidad de la puesta en marcha del sistema integral, contados a partir del día siguiente de la firma del Acta de Conformidad de la Instalación.



- Reemplazo de los equipos o partes, por repuestos originales, en caso de fallo, se deberá colocar un equipo de características similares o superiores hasta que se efectúe la revisión correspondiente, esto se deberá de efectuar en un periodo no mayor a 24 horas a partir de la notificación de avería.
- En caso de ser necesario y aplicar el reemplazo de equipos por averías, el postor tendrá un plazo de cuarenta y cinco (45) días para realizar el cambio.

CAPACITACIÓN

El postor deberá considerar una capacitación basada en currícula oficial por un mínimo de 10 horas para un grupo de cinco (05) personas. La capacitación debe comprender lo relacionado a la administración, gestión, resolución de problemas y buenas prácticas de las plataformas de **seguridad gestionada** ofertada.

El postor deberá acreditar para admisión de la oferta ser representante o distribuidor autorizado de la marca ofertada, adjuntando una carta del fabricante haciendo referencia al proceso.



5.3. INSTALACIÓN Y CONFIGURACIÓN:

- El CONTRATISTA deberá presentar un plan de trabajo considerando el plazo máximo de noventa (90) días calendarios como máximo contado a partir del día siguiente de suscrito el Contrato, donde se mencione como mínimo: un plan que incluya el diseño de la arquitectura de la solución a implementar, fecha referencial de la entrega de bienes, instalación, configuración y pruebas de puesta en funcionamiento, asimismo la capacitación y los temas de dicha capacitación de la Plataforma de Servidores Hiperconvergentes. Durante los cinco (05) días posteriores de la firma de contrato, dicho plan debe ser entregado a través de Mesa de Partes del HNDAC.
- El CONTRATISTA deberá realizar la migración de los servidores virtuales/físicos los cuales están en producción en la infraestructura actual. Se adjunta cuadro de la relación de las máquinas virtuales actualmente sobre Hyper-V.
- El CONTRATISTA y la Unidad de Tecnologías de la Información firmara el acta de constitución del proyecto y el acta de kickoff, al día siguiente de la presentación del plan de trabajo.
- El CONTRATISTA deberá considerar todos sus materiales y/o herramientas necesarias para la puesta en funcionamiento de la Plataforma de Servidores Hiperconvergentes.
- EL CONTRATISTA realizará la instalación de la solución de hiperconvergencia en el Centro de Datos Principal del HNDAC.
- El CONTRATISTA deberá acondicionar, montar e instalar dentro del gabinete de auto contenido el PDU y la adquisición de Servidores Hiperconvergentes para los Sistemas Informáticos a Nivel Nacional.
- El CONTRATISTA debe conectar la Plataforma de Servidores Hiperconvergentes con la red de datos y red eléctrica existente para su funcionamiento y puesta en marcha.
- El CONTRATISTA, es responsable de la instalación y configuración de los equipos adquiridos, lo cual no deberá generar costos adicionales a la entidad.
- El CONTRATISTA realizará la instalación y configuración de la Plataforma de Servidores Hiperconvergentes, debiendo dejar todo operativo.
- En el caso de presentarse una "actualización tecnológica" en los bienes y/o elementos que formen parte de la oferta y en cualquier momento anterior a la firma el acta de conformidad de la prestación principal, el CONTRATISTA debe



suministrar tales equipos y/o elementos actualizados, contando con autorización previa del HNDAC, sin que ello implique un cargo adicional para la Entidad.

- Al ser una central de emergencias la cual opera las 24 horas del día, los tiempos de migración de los servidores virtuales podrán posponerse por caso de emergencia reprogramándose. Esto deberá documentarlo el CONTRATISTA para evitar contratiempos.
- Será de total y exclusiva responsabilidad del CONTRATISTA efectuar las tareas necesarias para la puesta en marcha de los sistemas adquiridos.
- El CONTRATISTA deberá asumir la responsabilidad por los daños ocasionados producto de los trabajos contratados durante la instalación, configuración y pruebas de puesta en funcionamiento.
- El CONTRATISTA deberá instalar acondicionar y montar el gabinete de servidores para la instalación y configuración de la Plataforma de Servidores Hiperconvergentes en la Sala de Datos de la UTI (Unidad de Tecnología y la Información).
- El CONTRATISTA, entregará como parte del Informe Técnico Final, las contraseñas de tipo administrador con accesos completos de cada uno de los componentes de la Plataforma de Servidores Hiperconvergentes.
- El CONTRATISTA en la reunión de kickoff solicitará a la entidad todas las direcciones ip necesarias para la implementación de la capa hiperconvergente, incluyendo las de administración del mismo nodo. Podrá ser entregada en físico o vía correo electrónico.



5.4. GARANTÍA COMERCIAL:

Todo el equipamiento, software y accesorios que forman parte del requerimiento deben contar con una garantía de cuatro (04) años, contados a partir del día siguiente de la conformidad de la prestación principal, el mismo que será contra defectos de diseño y/o fabricación, averías o fallas de funcionamiento, o pérdida total de los bienes contratados derivados de desperfectos o fallas ajenas al uso habitual o normal de los bienes no detectables al momento que se dio la conformidad. Dicha garantía cubre la reparación de los bienes, considerando el reemplazo de componentes nuevos, originales y sin uso de los equipos o del equipo en su totalidad.

5.4.1. TIEMPO DE RESPUESTA PARA SUBSANAR FALLAS POR DEFECTOS DE FABRICACIÓN:

- En caso de existir equipos con fallas por defectos de fabricación de hardware y software, en todos los casos, la reparación y/o reemplazo corre por cuenta del CONTRATISTA, por el tiempo de vigencia de la garantía comercial. Dichas atenciones se deberán realizar en un plazo máximo de seis (06) horas después de haberse comunicado al Contratista. Cabe resaltar que el servicio es 24x7 por 365 días. En caso que el tiempo indicado resulte insuficiente, por razones justificadas, se deberá entregar un equipo de respaldo, en tanto dure la solución al desperfecto técnico; El equipo de respaldo será devuelto al Contratista a la entrega del equipo reparado.

- El CONTRATISTA deberá asumir sin costo adicional el reemplazo del equipo para la entidad en caso que sea reparado y muestre la misma falla en más de tres (03) oportunidades de los bienes (de las mismas fallas sobre el bien o componente ofertado durante el lapso de un año).
- Toda la infraestructura ofertada, debe ser nueva, de un mismo fabricante y no puede ser catalogado como "descontinuado" o "re fabricado". Por ello, para la suscripción del Contrato deberá acreditar presentando carta del fabricante con referencia al presente procedimiento de selección, donde se detallen tal condición, así como todos los modelos y números de parte de la solución ofertada.
- El CONTRATISTA deberá proporcionar números telefónicos de atención ante fallos de hardware y software, los cuales deberá presentar como parte de la documentación para la suscripción del contrato.

5.5. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL:

5.5.1. SOPORTE TÉCNICO ESPECIALIZADO.

El CONTRATISTA, deberá de asegurar el soporte técnico especializado, actualizaciones y asesoramientos a la adquisición de la plataforma de la solución Hiperconvergente implementada, cuando se produzca alguna falla y/o averías no imputables a defectos de fabricación o vicios ocultos. Dicho servicio deberá estar a disposición 24x7 durante el periodo contractual, por un periodo de cinco (05) años iniciado desde que el CONTRATISTA recepcione el requerimiento formulado por HNDAC mediante correo electrónico y/o llamada telefónica:

- El CONTRATISTA deberá presentar números de línea 0800 del fabricante y procedimientos de atención mediante Call Center a la firma del contrato.
- El CONTRATISTA tendrá un plazo máximo de cuatro (04) horas presenciales y/o vía remoto para resolver el problema o incidente reportado contabilizado a partir de la recepción del reporte de falla por parte del CONTRATISTA. Para tal fin, el CONTRATISTA deberá disponer de una cuenta de correo electrónico y número telefónico, los mismos que estarán a disposición de la Entidad las 24 horas del día durante el periodo de la ejecución del servicio. Ante el reporte de alguna falla por parte de la Entidad, el CONTRATISTA asignará un número de registro a dicho reporte. El CONTRATISTA para la suscripción del contrato, deberá adjuntar una declaración jurada indicando un correo institucional de dominio propio, y un contacto telefónico.
- El tiempo de atención se inicia desde la recepción del requerimiento de la falla y/o avería por parte del CONTRATISTA.
- El CONTRATISTA ante alguna incidencia deberá proveer personal certificado técnico por la capa hiperconvergente para la atención de soporte en sitio.

5.5.2. CAPACITACIÓN:

El CONTRATISTA deberá efectuar la capacitación al personal de sistemas de HNDAC sobre los siguientes cursos:

Temas a considerar en la Capacitación

Nº	Detalle de Capacitación
1	Curso Oficial de Administración de solución de Hiperconvergencia.
2	Curso Oficial de Administración de la solución de software de virtualización (si el software de virtualización pertenece a la capa hiperconvergente bastara con el curso oficial anterior).
3	Curso No Oficial de Administración de la solución ofertada brindada por personal certificado en la capa Hiperconvergente
4	Curso No Oficial de la solución de Seguridad propuesta

- Los cursos oficiales serán dictados en un Centro Autorizado de Capacitación de la marca ofertada, para dos (02) personas; siendo los capacitadores, personal certificado por el fabricante de la solución ofertada en el curso a dictar.
 - Las constancias del curso deben contener las horas lectivas y las fechas que se realizó la capacitación.
- Los cursos no oficiales serán dictados en las instalaciones en el Centro de Datos, previa coordinación con el HNDAC, estará dirigido a seis (06) personas de UTI como mínimo, con una duración mínima de 4 horas por cada curso; siendo el capacitador, personal certificado por el fabricante de la solución ofertada.
 - Las constancias del curso No oficial deben ser entregados por el CONTRATISTA con la firma del instructor.
- El CONTRATISTA entregará las constancias de participación por cada curso de capacitación dentro del plazo máximo.
- El CONTRATISTA al finalizar capacitación en conjunto con la Unidad de Tecnologías y la Información emitirá las actas de conformidad por la capacitación.
- El CONTRATISTA para la instalación y configuración del software de virtualización contemplara los siguientes puntos:

28





- Instalación y configuración del software de virtualización en los seis (06) nodos Hiperconvergente ofertados.
- En caso que el software de virtualización sea del mismo fabricante de la capa hiperconvergente estos deberán venir preinstalados.
- Configuración de los switches LAN, switches virtuales y almacenamiento entre los nodos.
- Configuración de alta disponibilidad a nivel de capa hiperconvergente.
- Antes de realizar la migración de la actual plataforma de virtualización (plataforma pre existente) a la nueva plataforma adquirida de virtualización, el CONTRATISTA firmara un acta que será responsable de la migración, el cual no debe perderse ninguna información que se tiene en los servidores virtuales.
- Migrar la actual plataforma de virtualización (plataforma pre existente) incluyendo equipos virtualizados a la nueva plataforma ofertada, los cuales se detallan a continuación:

RELACION DE SERVIDORES VIRTUALES DEL CGBVP - HNDAC			
HIPERVISOR	SISTEMA OPERATIVO	VERSION	CANTIDAD
VMWARE	WINDOWS SERVER	2012 R2	30
TOTAL DE SERVIDORES VIRTUALES			30

5.6. LUGAR Y PLAZO DE EJECUCIÓN DE LA PRESTACIÓN DE LOS BIENES:

5.6.1. Lugar de entrega:

La entrega de la totalidad de los bienes debe efectuarse en el Almacén Central de la HNDAC, previa coordinación con el encargado del Área de Almacén, salvo equipos muy pesados y/o muy delicados en traslados que requieran tratamiento especial, previa coordinación con el área usuaria. Todos los costos de traslado para la instalación y configuración de los bienes corren por cuenta del CONTRATISTA.

5.6.2. Lugar de la instalación y configuración:

Todos los equipos requeridos deben ser instalados y configurados por el CONTRATISTA en la Sede Principal de la HNDAC, **Sala de Datos** ubicada en el HNDAC, previa coordinación con la Unidad de Tecnologías de la Información, para su instalación y configuración de los equipos.

5.6.3. Plazo de entrega aceptación de plan de trabajo, entrega de bienes, instalación, configuración, pruebas de puesta en funcionamiento y capacitación de la Prestación Principal:

Como plazo máximo para la aceptación del plan de trabajo, entrega de bienes, instalación, configuración, pruebas de puesta en funcionamiento y capacitación de la Plataforma de Servidores Hiperconvergentes, el CONTRATISTA tendrá como plazo máximo de noventa (90) días calendario contado a partir del día siguiente de suscrito el Contrato.

5.6.3.1. Entrega, instalación, configuración y pruebas de puesta en funcionamiento:

Al finalizar la instalación, configuración y puesta en funcionamiento, la Unidad de Tecnologías y la Información de la HNDAC deberán adjuntar el acta de instalación y configuración del servicio y acta de pruebas de puesta en funcionamiento.

5.7. ENTREGABLES:

El CONTRATISTA, presentará a través de la mesa de partes del HNDAC, el informe técnico de la instalación, configuración, capacitación, pruebas y afinamiento de la solución provista de la prestación principal, dentro del periodo de ejecución y así mismo el Acta de Instalación y puesta en operación del servicio que será presentado una vez culminado dicho periodo. El informe técnico debe considerar aspectos de forma y estar alineado a las buenas prácticas de Gestión de Proyectos debiendo tener un esquema similar al planteado:

El Informe Técnico Final debe considerar aspectos de forma como:

- Índice
- Visados por el responsable de la implementación.
- Paginación foliada.
- En el informe final debe ser físico y virtual (PDF).

5.8. MODALIDAD DE EJECUCIÓN CONTRACTUAL – Llave en mano

La solución a implementar es de tipo llave en mano y puesta en marcha; todos los equipos, suministros, accesorios, software y licencias requeridas, serán suministrados en su totalidad por el CONTRATISTA, debiendo a implementar su instalación, configuración y puesta en funcionamiento a la solución requerida.

5.9. TRANSPORTE:

El contratista debe asumir el costo relacionado al transporte requerido para llevar a cabo la entrega, configuración y puesta en funcionamiento a la solución requerida.

5.10. SEGUROS Y SEGURIDAD Y SALUD EN EL TRABAJO:

El CONTRATISTA deberá contar obligatoriamente con seguro complementario de trabajo contra todo riesgo para todos y cada uno del personal involucrado en la ejecución de la prestación. Esta póliza deberá encontrarse vigente desde el inicio de la ejecución de la prestación hasta su culminación y deberá ser entregado del HNDAC, antes del inicio de los trabajos. Lo cual será acreditado mediante copia simple del documento emitido por la aseguradora para la suscripción del contrato.

El HNDAC no se responsabiliza por accidentes que pudiera sufrir el personal técnico y profesional del contratista, durante la ejecución de los trabajos, debiendo el CONTRATISTA, proveer lo necesario para considerar en sus costos la contratación de un seguro contra accidente.



El CONTRATISTA se compromete a cumplir y observar lo establecido en la Ley de Seguridad y Salud en el Trabajo (aprobado mediante Ley N° 29783) y en su Reglamento (aprobado mediante Decreto Supremo N° 005-2012-TR); durante la ejecución de las prestaciones a su cargo; obligándose a implementar, dotar, proveer y/o suministrar a cada uno de sus trabajadores los implementos de seguridad que corresponda de acuerdo al grado y/o nivel de riesgo que pueda evidenciarse en el desarrollo de las actividades propias de la presente contratación dentro de las instalaciones de la HNDAC.

6. REQUISITOS DEL CONTRATISTA:

6.1. DEL POSTOR

El postor deberá ser una empresa constituida, con experiencia comprobada no menor a Cinco (5) años en ofertar actividades de tecnología de la información – TIC y de servicios informáticos en el territorio peruano.

El postor debe acreditar el monto facturado acumulado equivalente a S/ 8, 960,000.00 (Ocho Millones, Novecientos Sesenta Mil con 00/100 Soles) del monto total por la venta de bienes iguales o similares al objeto de la convocatoria, durante un período de ocho (08) años a la fecha de la presentación de ofertas.

Se consideran bienes similares a los siguientes: Plataforma o soluciones Hiperconvergentes de software o Plataformas Convergentes, o Servidores de Torre o Servidores Blade o Servidores tipo Rack y soluciones de seguridad.

6.2. PERSONAL REQUERIDO:

El CONTRATISTA deberá acreditar como parte de los documentos exigidos para la suscripción del contrato los siguientes vinculados al personal requerido.

Al ser una solución de alta especialización, el personal clave podrá presentarse en uno o más proveedores siempre y cuando este no pertenezca a la planilla de uno de ellos.

Los integrantes (Jefe de Proyecto, Implementador y Capacitador) deberán presentar una carta notarial indicando que tienen conocimiento fehaciente del concurso y están participando en el mismo.

• JEFE DE PROYECTO:

La función es interactuar entre las necesidades del área usuaria del HNDAC y el implementador y/o capacitador.

Un (01) Ingeniero Jefe de Proyecto, el cual será responsable de la planificación, control y cierre del proyecto, así mismo deberá tener la capacidad de gestionar la planificación de la ejecución a realizar. El profesional deberá cumplir y acreditar el siguiente perfil: Ingeniero titulado, de las carreras de Ingeniería de sistemas o telecomunicaciones o Electrónica o Eléctrica.

Con certificación ITIL V3 como mínimo, requeridas para eficiente gestión de servicios.

Con certificación PMP vigente o equivalente en dirección de proyectos requeridas para la eficiente gestión del proyecto.

Con experiencia profesional mínima de tres (03) años en gestión de proyectos de Tecnologías de la Información - TI, como jefe o gerente de proyecto.



• **ESPECIALISTA IMPLEMENTADOR: Personal CLAVE**

Encargado de la instalación y configuración de la solución Hiperconvergente. ESTE ES EL PERSONAL MANDATORIO DE LA IMPLEMENTACION. El profesional deberá cumplir y acreditar el siguiente perfil:

Profesional Titulado y/o Colegiado en carreras Sistemas o Computación e Informática o de Redes y Telecomunicaciones o Electrónica o equivalente, contando con la siguiente certificación:

Una (01) acreditación y/o certificación técnica y/o profesional vigente de la solución de virtualización, si la solución de hiperconvergencia ofertada posee su propio hipervisor entonces bastaran con la certificación de la capa Hiperconvergente ofertada y deberá ser validado con carta de la fabricante ofertada.

Una (01) acreditación y/o certificación indicando que está en capacidad de realizar instalaciones de la capa hiperconvergente ofertada deberá ser validado con carta del fabricante ofertado

Una (01) acreditación y/o certificación indicando que está en capacidad de realizar instalaciones de la capa de seguridad ofertada deberá ser validado con carta del fabricante ofertado.

Deberá acreditar lo solicitado con:

Copia simple de Constancia de egresado y/o Título a nombre de la nación de ser el caso, en caso de ser universitario deberá ser validada en el portal de SUNEDU.

Copia simple de contratos y su respectiva conformidad o constancias o certificados o cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto en hiperconvergencia.

Experiencia mínima en tres (03) implementaciones y configuraciones en un periodo de dos (03) años en soluciones hiperconvergentes.

• **ESPECIALISTA CAPACITADOR (Curso No Oficial)**

El personal capacitador (curso no oficial) podrá ser el mismo personal implementador clave.

Profesional Titulado y/o Colegiado en carreras Sistemas o Computación e Informática o de Redes y Telecomunicaciones o Electrónica o equivalente, contando con la siguiente certificación.

El profesional deberá cumplir y acreditar el siguiente perfil:

Una (01) acreditación y/o certificación técnica y/o profesional vigente de la solución de virtualización, si la solución de hiperconvergencia ofertada posee su propio hipervisor entonces bastaran con una carta de parte del fabricante de la solución ofertada.

Deberá acreditar lo solicitado con:

Copia simple de Constancia de egresado y/o Título a nombre de la nación de ser el caso, en caso de ser universitario deberá ser validada en el portal de SUNEDU.

Copia Simple de algún documento que demuestre en forma fehaciente haber realizado capacitaciones o instalaciones en soluciones Hiperconvergentes.

Copia simple de la certificación técnica y/o profesional de la capa Hiperconvergente ultima versión y/o anterior.

ESPECIALISTA EN CIBERSEGURIDAD

Un (01) Técnico titulado o Bachiller en Ingeniería Electrónica, o en Telecomunicaciones, o en Redes y Comunicaciones de Datos, o Sistemas, o Informática, o de Sistemas de Información.



Deberá contar con certificación vigente del fabricante de la solución ofertada.
Deberá contar con experiencia mínima de dos (02) años en la implementación, configuración y soporte de soluciones de firewalls ofertada.

7. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

7.1. Propiedad Intelectual:

El CONTRATISTA exime de toda responsabilidad a la HNDAC y a sus empleados y funcionarios, por cualquier litigio, acción legal o procedimiento administrativo, reclamación o demanda que pudiera derivarse de cualquier trasgresión o supuesta trasgresión de cualquier patente, uso de modelo, diseño registrado, marca registrada, derechos de autor o cualquier otro derecho de propiedad intelectual que estuviese registrado o de alguna otra forma existente a la fecha del contrato debido a la instalación del bien por parte del CONTRATISTA o el uso de los mismos por parte del HNDAC.

Lo establecido en el párrafo anterior no resultará aplicable si el bien fuese utilizado para fines no previstos en el contrato o para fines que no pudiesen razonablemente inferirse de dicho contrato.

El HNDAC al término de la vigencia del contrato tendrá la propiedad del software (hiperconvergencia, hipervisor, sistemas operativos) pudiendo hacer uso, explotación de todos los documentos, programas y mejoras de los mismos que se creen y desarrollen como consecuencia de la ejecución del servicio objeto del presente contrato en el ámbito de las funciones del HNDAC.

7.2. CONFIDENCIALIDAD:

El CONTRATISTA se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita del HNDAC, toda información que le sea suministrada por ésta última y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el desarrollo o para la realización de sus tareas.

El CONTRATISTA deberá mantener a perpetuidad la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del desarrollo de los procedimientos de selección y la ejecución de las prestaciones contratadas, quedando prohibida revelarla a terceros.

Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades previas a la ejecución de las prestaciones contratadas, durante su ejecución y la producida una vez que se haya concluido el contrato.

Dicha información puede consistir en informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el proveedor.

Asimismo, aun cuando sea de índole pública, la información vinculada, inclusive en el desarrollo de la contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por proveedor para fines publicitarios o de difusión por cualquier medio.

Los documentos técnicos, estudios, informes, grabaciones, películas, programas informáticos y todos los demás que formen parte de su oferta técnica y económica que



se deriven de las prestaciones contratadas serán de exclusiva propiedad del HNDAC. En tal sentido, queda claramente establecido que el contratista no tiene ningún derecho sobre los referidos productos, ni puede venderlos, cederlos o utilizarlos para otros fines que no sean los que se deriven de la ejecución del presente contrato.

7.2.1. Área que recepcionará y brindará la conformidad-Prestación Principal:
El encargado del Área de Almacén del HNDAC estará a cargo de la recepción de los bienes y la conformidad de la prestación principal será otorgada por la Unidad de Tecnologías y la Información.

7.3. Forma de pago:

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en Único Pago.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Recepción de los bienes en el área de almacén.
- Informe del funcionario responsable del Oficina de Estadística y Sistemas Informáticos (OESI) emitiendo la conformidad de la prestación efectuada y la puesta en funcionamiento.
- Constancia de Capacitación al personal establecido en las EE.TT.
- Comprobante de pago.



7.4. PENALIDADES

7.4.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

7.5. RESPONSABILIDAD POR VICIOS OCULTOS:

El contratista será responsable por la calidad ofrecida y los vicios ocultos de los bienes ofertados, conforme a lo indicado en el numeral 40.2 del artículo 40° de la Ley de Contrataciones y Artículo 146° del Reglamento de la Ley de Contrataciones del Estado, por un plazo de un (01) año, contados a partir de la conformidad otorgada por parte del HNDAC.

7.6 ADELANTOS

La entidad entregará un adelanto directo al contratista de acuerdo a lo estipulado en el reglamento, de un treinta por ciento (30%) del monto del contrato original.

I. REQUISITOS DE CALIFICACION:

A	CAPACIDAD TECNICA Y PROFESIONAL
A.1	EXPERIENCIA DEL PERSONAL CLAVE
A.1.1	FORMACION ACADEMICA
	<p>JEFE DE PROYECTO:</p> <p>La función es interactuar entre las necesidades del área usuaria del HNDAC el implementador y/o capacitador.</p> <p>Un (01) Ingeniero Jefe de Proyecto, el cual será responsable de la planificación, control y cierre del proyecto, así mismo deberá tener la capacidad de gestionar la planificación de la ejecución a realizar. El profesional deberá cumplir con el siguiente perfil: Ingeniero titulado, de las carreras de Ingeniería de sistemas o telecomunicaciones o Electrónica o Eléctrica.</p> <p>Con certificación ITIL V3 como mínimo, requeridas para eficiente gestión de servicios.</p> <p>Con certificación PMP vigente o equivalente en dirección de proyectos requeridas para la eficiente gestión del proyecto.</p> <p>Se deberá acreditar una experiencia profesional mínima de tres (03) años en gestión de proyectos de Tecnologías de la Información - TI, como jefe o gerente de proyecto.</p> <p>• ESPECIALISTA IMPLEMENTADOR: Personal CLAVE</p> <p>Encargado de la instalación y configuración de la solución Hiperconvergente. ESTE ES EL PERSONAL MANDATORIO DE LA IMPLEMENTACION. El profesional deberá cumplir el siguiente perfil:</p> <p>Profesional Titulado y/o Colegiado en carreras Sistemas o Computación e Informática o de Redes y Telecomunicaciones o Electrónica o equivalente, contando con la siguiente certificación:</p> <p>Una (01) acreditación y/o certificación técnica y/o profesional vigente de la solución de virtualización, si la solución de hiperconvergencia ofertada posee su propio hipervisor entonces bastaran con la certificación de la capa Hiperconvergente ofertada y deberá ser validado con carta de la fabricante ofertada.</p> <p>Una (01) acreditación y/o certificación indicando que está en capacidad de realizar instalaciones de la capa hiperconvergente ofertada deberá ser validado con carta del fabricante ofertada.</p> <p>Deberá acreditar una Experiencia mínima en tres (03) implementaciones y configuraciones en un periodo de tres (03) años en soluciones hiperconvergentes, la misma que se deberá acreditar con Copia simple de contratos y su respectiva conformidad o constancias o certificados o cualquier otra</p>



490



	<p>documentación que, de manera fehaciente demuestre la experiencia del personal propuesto en hiperconvergencia.</p> <ul style="list-style-type: none"> ESPECIALISTA CAPACITADOR (Curso No Oficial) El personal capacitador (curso no oficial) podrá ser el mismo personal implementador clave. Profesional Titulado y/o Colegiado en carreras Sistemas o Computación e Informática o de Redes y Telecomunicaciones o Electrónica o equivalente, contando con la siguiente certificación. El profesional deberá cumplir el siguiente perfil: Una (01) acreditación y/o certificación técnica y/o profesional vigente de la solución de virtualización, si la solución de hiperconvergencia ofertada posee su propio hipervisor entonces bastarán con una carta de parte del fabricante de la solución ofertada. Copia simple de la certificación técnica y/o profesional de la capa Hiperconvergente última versión y/o anterior. Experiencia: Copia Simple de algún documento que demuestre en forma fehaciente haber realizado capacitaciones o instalaciones en soluciones Hiperconvergentes. ESPECIALISTA EN CIBERSEGURIDAD Un (01) Técnico titulado o Bachiller en Ingeniería Electrónica, o en Telecomunicaciones, o en Redes y Comunicaciones de Datos, o Sistemas, o Informática, o de Sistemas de Información. Deberá contar con certificación vigente del fabricante de la solución ofertada. Deberá acreditar una experiencia mínima de dos (02) años en la implementación, configuración y soporte de soluciones de firewalls ofertada.
B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p>Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 8, 960,000.00 (Ocho Millones, Novecientos Sesenta Mil con 00/100 Soles) por la contratación de servicios 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.</p> <p>Se consideran bienes similares a los siguientes: Plataforma o soluciones Hiperconvergentes de software o Plataformas Convergentes, o Servidores de Torre o Servidores Blade o Servidores Tipo Rack o soluciones de Seguridad.</p> <p>Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y</p>



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 pago¹, 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 referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la 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 sustentadora correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicada por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda.

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

¹ 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 fehacencia 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".

958

	El postor deberá estar habilitado para contratar con el estado.
	El postor deberá ser una empresa constituida, con experiencia comprobada no menor a tres (3) años en ofertar actividades de tecnología de la información – TI y de servicios informáticos. Para tal efecto deberá presentar fotocopia de su ficha RUC.



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).	<p>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:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i = Oferta Pi = Puntaje de la oferta a evaluar Oi = Precio i Om = Precio de la oferta más baja PMP = Puntaje máximo del precio</p> <p>100] puntos</p>

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

Dependiendo del objeto del contrato, de resultar indispensable, puede incluirse cláusulas adicionales o la adecuación de las propuestas en el presente documento, las que en ningún caso pueden contemplar disposiciones contrarias a la normativa vigente ni a lo señalado en este capítulo.

Conste por el presente documento, la contratación ADQUISICION DE SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE), SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE) Y ; EN EL(LA) EESS NAC. DANIEL A. CARRION - BELLAVISTA EN LA LOCALIDAD BELLAVISTA, DISTRITO DE BELLAVISTA, PROVINCIA CONSTITUCIONAL DEL CALLAO, DEPARTAMENTO CALLAO CON EL CUI N° 2554512, que celebra de una parte Hospital Nacional Daniel Alcides Carrión, en adelante LA ENTIDAD, con RUC N° [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [.....], el comité de selección adjudicó la buena pro de la **LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA** para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto ADQUISICION DE SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE), SISTEMAS DE PROCESAMIENTO Y ALMACENAMIENTO (SERVIDORES, STORAGE, LIBRERIAS DE RESPALDO, CLOUDBRIDGE) Y ; EN EL(LA) EESS NAC. DANIEL A. CARRION - BELLAVISTA EN LA LOCALIDAD BELLAVISTA, DISTRITO DE BELLAVISTA, PROVINCIA CONSTITUCIONAL DEL CALLAO, DEPARTAMENTO CALLAO CON EL CUI N° 2554512

CLÁUSULA TERCERA: MONTO CONTRACTUAL

El monto total del presente contrato asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

Este monto comprende el costo del bien, 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.

CLÁUSULA CUARTA: DEL PAGO¹²

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR EL DETALLE DEL PAGO ÚNICO O PAGOS A CUENTA, SEGÚN CORRESPONDA], 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.

Para tal efecto, el responsable de otorgar la conformidad de la prestación deberá hacerlo en un

¹² En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

plazo que no excederá de los siete (7) días de producida la recepción, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, en cuyo caso la conformidad se emite en un plazo máximo de quince (15) días, bajo responsabilidad de dicho funcionario.

LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

En caso de retraso en el pago por parte de LA ENTIDAD, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tendrá derecho al pago de intereses legales conforme a lo establecido en el artículo 39 de la Ley de Contrataciones del Estado y en el artículo 171 de su Reglamento, los que se computan desde la oportunidad en que el pago debió efectuarse.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO. EN LA MODALIDAD DE LLAVE EN MANO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].

Importante para la Entidad

En el caso de contratación de prestaciones accesorias, se puede incluir la siguiente cláusula:

CLÁUSULA ...: PRESTACIONES ACCESORIAS¹³

“Las prestaciones accesorias tienen por objeto [CONSIGNAR EL OBJETO DE LAS PRESTACIONES ACCESORIAS].

El monto de las prestaciones accesorias asciende a [CONSIGNAR MONEDA Y MONTO], que incluye todos los impuestos de Ley.

El plazo de ejecución de las prestaciones accesorias es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL CUMPLIMIENTO DE LAS PRESTACIONES PRINCIPALES, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO].

[DE SER EL CASO, INCLUIR OTROS ASPECTOS RELACIONADOS A LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS].”

Incorporar a las bases o eliminar, según corresponda

CLÁUSULA SEXTA: 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 SÉTIMA: GARANTÍAS

EL CONTRATISTA entregó al perfeccionamiento del contrato la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de LA ENTIDAD, por los conceptos, montos y vigencias siguientes:

- De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida

¹³ De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesorias, pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

por [SEÑALAR EMPRESA QUE LA EMITE]. Monto que es equivalente al diez por ciento (10%) del monto del contrato original, la misma que debe mantenerse vigente hasta la conformidad de la recepción de la prestación.

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la [INDICAR EL TIPO DE GARANTÍA PRESENTADA] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE], la misma que debe mantenerse vigente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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.

Importante para la Entidad

Sólo en el caso que la Entidad hubiese previsto otorgar adelanto, se debe incluir la siguiente cláusula:

CLÁUSULA NOVENA: ADELANTO DIRECTO

“LA ENTIDAD otorgará [CONSIGNAR NÚMERO DE ADELANTOS A OTORGARSE] adelantos directos por el [CONSIGNAR PORCENTAJE QUE NO DEBE EXCEDER DEL 30% DEL MONTO DEL CONTRATO ORIGINAL] del monto del contrato original.

EL CONTRATISTA debe solicitar los adelantos dentro de [CONSIGNAR EL PLAZO Y OPORTUNIDAD PARA LA SOLICITUD], adjuntando a su solicitud la garantía por adelantos mediante carta fianza o póliza de caución acompañada del comprobante de pago correspondiente. Vencido dicho plazo no procederá la solicitud.

LA ENTIDAD debe entregar el monto solicitado dentro de [CONSIGNAR EL PLAZO] siguientes a la presentación de la solicitud del contratista.”
Incorporar a las bases o eliminar, según corresponda.

CLÁUSULA DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

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 [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA DE ALMACÉN O LA QUE HAGA SUS VECES] y la conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

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 cumpliera 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 UNDÉCIMA: 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 DUODÉCIMA: 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 [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: 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.

Importante

De haberse previsto establecer penalidades distintas a la penalidad por mora, incluir dichas penalidades, los supuestos de aplicación de penalidad, la forma de cálculo de la penalidad para cada supuesto y el procedimiento mediante el cual se verifica el supuesto a penalizar, conforme el artículo 163 del Reglamento de la Ley de Contrataciones del Estado.

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Estos dos (2) tipos de penalidades pueden alcanzar cada una un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, o de ser el caso, del ítem que debió ejecutarse.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora o el monto máximo para otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

CLÁUSULA DÉCIMA CUARTA: 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 QUINTA: 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 SEXTA: 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 SÉTIMA: 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 OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹⁴

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 DÉCIMA NOVENA: 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.

¹⁴ De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

CLÁUSULA VIGÉSIMA: 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: [.....]

DOMICILIO DEL CONTRATISTA: [CONSIGNAR EL DOMICILIO SEÑALADO POR EL POSTOR GANADOR DE LA BUENA PRO AL PRESENTAR LOS REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO]

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 integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

“LA ENTIDAD”

“EL CONTRATISTA”

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹⁵.

¹⁵ 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 N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [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 compra¹⁶

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.

¹⁶ 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 N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 compra¹⁷

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]

¹⁷ 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 N° 2

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

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 N° 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 N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 N° 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 N° [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] [%]¹⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]¹⁹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²⁰

¹⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁰ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

[CONSIGNAR CIUDAD Y FECHA]

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

.....
Consortiado 2
Nombres, apellidos y firma del Consortiado 2
o de su Representante Legal
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 N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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”.*

Incluir o eliminar, según corresponda

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
1										
2										
3										
4										

²¹ 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.

²² **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.

²³ 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”*.

²⁴ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁵ 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.

²⁶ 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 ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶	
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 N° 9

DECLARACIÓN JURADA (NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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 N° 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

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 03-2023-HNDAC-CS-1 PRIMERA CONVOCATORIA

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.