

BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

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> <div>Importante</div> <ul style="list-style-type: none"> • Abc </div>	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	<div> <div>Advertencia</div> <ul style="list-style-type: none"> • Abc </div>	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	<div> <div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz </div>	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 de 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

UNIVERSIDAD NACIONAL DEL ALTIPLANO



BASES ESTÁNDAR DE CONCURSO PÚBLICO PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

CONCURSO PÚBLICO N° 001-2024-UNDA-1
PRIMERA CONVOCATORIA

BASES INTEGRADAS

**CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A
INTERNET, SEGURIDAD ADMINISTRADA E
INTERCONEXIÓN DE SEDES PARA LA UNIVERSIDAD
NACIONAL DEL ALTIPLANO-PUNO**

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

- *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*

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>

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 y condiciones de los Términos de Referencia, detallados 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.*
- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 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-emitar-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 servicios, 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 : UNIVERSIDAD NACIONAL DEL ALTIPLANO
RUC N° : 20145496170
Domicilio legal : Av. El Sol N° 329 Puno
Teléfono: : 051 - 36 88 44
Correo electrónico: : contrataciones.abastecimiento@unap.edu.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A INTERNET, SEGURIDAD ADMINISTRADA E INTERCONEXIÓN DE SEDES PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO-PUNO, según términos de referencia:

ITEM	DESCRIPCIÓN	UNIDAD DE MEDIDA	CANTIDAD
1	Servicio de Internet	SERVICIO	1

Importante para la Entidad

- En caso de procedimientos de selección según relación de ítems o por paquete consignar el detalle del objeto de estos.
- En caso de proyectos de inversión, se debe consignar el servicio materia de la convocatoria, y no la denominación del proyecto.

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases.

1.3. EXPEDIENTE DE CONTRATACIÓN

°El expediente de contratación fue aprobado mediante FORMATO N° 02- APROBACIÓN DE EXPEDIENTE DE CONTRATACIÓN N° 0404 el 10 de diciembre de 2024

1.4. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados - RDR

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 SUMA ALZADA, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.6. DISTRIBUCIÓN DE LA BUENA PRO

No aplica

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

La prestación del servicio será por un periodo de 1100 días calendarios, contados a partir del día siguiente de la firma del acta de la habilitación y puesta en funcionamiento del servicio de internet (inicio del servicio).

-La implementación se realizará máximo en noventa (90) días calendarios siguientes al perfeccionamiento del contrato, el plazo de instalación comenzará a computarse desde que la entidad cumpla con las condiciones necesarias para la ejecución del servicio (disponibilidad de locales y ambientes, suministro adecuado de energía, entrega de información, etc.) y permisos correspondientes.

1.9. 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 la suma de cinco y 00/100 soles (S/. 5.00) en la Oficina de Tesorería y recabar una copia en la Unidad de Procesos de Selección, sitos en la Av. el sol N° 329 ciudad de Puno - 2do piso del Edificio de Educación Continua.

Importante

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

1.10. BASE LEGAL

- LEY N° 31953 - Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
 - LEY N° 31856 - Ley de Equilibrio Financiero del Presupuesto del Sector Público para el Año Fiscal 2024.
 - Decreto Supremo N° 082-2019-EF que aprueba el TUO de la Ley N° 30225 – Ley de Contrataciones del Estado.
 - Decreto Supremo N° 344-2018-EF que aprueba el Reglamento de la Ley N° 30225 - Ley de Contrataciones del Estado, modificado por Decreto Supremo N° 377-2019-EF, Decreto Supremo N° 168-2020-EF y por Decreto Supremo N° 162-2021-EF.
 - Decreto Supremo N° 004-2019-JUS que Aprueba el TUO de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
 - Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública, aprobado por Decreto Supremo N° 043-2003-PCM.
 - Ley N° 29973 - Ley General de la Persona con Discapacidad.
 - Decreto Supremo N° 013-2013-PRODUCE que Aprueba el TUO de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial.
 - Código Civil.
 - Directivas y Opiniones del OSCE.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado

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

- Declaración jurada de datos del postor. (**Anexo N° 1**)
- 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.

- Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- Declaración jurada de cumplimiento de los Términos de Referencia contenidos 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/>

- d.1 El postor deberá presentar carta del fabricante que confirme que su red WAN está equipada con tecnología MPLS de la marca.
- d.2 El postor deberá presentar un diagrama de la salida internacional detallando los nombres de los proveedores TIER I.
- d.3 Certificado vigente emitido por una empresa consultora externa (Certificadora en infraestructura y centros de comando de control) que acredite la operación e infraestructura propia del NOC & SOC.
- e) Declaración jurada de plazo de prestación del servicio. **(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 [CONSIGNAR LA MONEDA EN LA QUE SE DEBE PRESENTAR LA OFERTA]. 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.*
- *En caso de requerir estructura de costos o análisis de precios, esta se presenta para el perfeccionamiento del contrato.*

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

⁴ En caso de considerar como factor de evaluación la mejora del plazo de prestación del servicio, el plazo ofertado en dicho anexo servirá también para acreditar este factor.

- 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

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 comunicación ⁶ (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) Estructura de costos⁸.
- k) Declaración jurada confirmando que el DNS cumple con las características solicitadas.
- l) Declaración jurada confirmando la propiedad del Data Center y que estos se encuentran en territorio nacional.

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 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 periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2> opción consulta de empresas acreditadas en el REMYPE.*
- 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

⁵ Para mayor información de las Entidades usuarias 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 cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

- *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, debe presentar la documentación requerida en **Unidad de Trámite Documentario** Ubicado en el primer piso del Edificio de Educación Continua sito en Av. El Sol 329 de la ciudad de Puno.

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 servicios, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200,000.00).

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en forma mensual y en partes iguales.

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

- Informe del funcionario responsable del jefe de la oficina de tecnologías de la información – UNAP emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en la Unidad de Abastecimiento sito en Av. Floral N° 329- 2do piso del Edificio de Educación Continua, ciudad de Puno.

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

CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. TÉRMINOS DE REFERENCIA



UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO
OFICINA DE TECNOLOGÍAS DE INFORMACIÓN



TÉRMINOS DE REFERENCIA: "CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A INTERNET, SEGURIDAD ADMINISTRADA E INTERCONEXIÓN DE SEDES PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO"

DENOMINACIÓN DE LA CONTRATACIÓN

"CONTRATACIÓN DEL SERVICIO DE ACCESO DEDICADO A INTERNET, SEGURIDAD ADMINISTRADA E INTERCONEXIÓN DE SEDES PARA LA UNIVERSIDAD NACIONAL DEL ALTIPLANO - PUNO"

FINALIDAD PÚBLICA

El presente proceso tiene como finalidad optimizar y asegurar el funcionamiento de los servicios de comunicaciones vía internet con la adecuada seguridad e interconexión, en las actividades Académicas de Pregrado, Posgrado, Investigación, Emprendimiento y actividades Administrativas de la Universidad Nacional del Altiplano Puno en adelante UNA-PUNO.



ANTECEDENTES

A la fecha la Universidad Nacional del Altiplano Puno (UNAP), cuenta con un contrato para el servicio de internet el mismo que ya finalizó, asimismo cuenta con un Backbone de fibra óptica instalado en el Campus Universitario, el servicio de internet proveído actualmente llega al Data Center ubicado en la Oficina de Tecnologías de Información (OTI). El servicio proveído actualmente es insuficiente para cubrir las necesidades actuales de la UNA Puno, por ello es urgente poder contratar servicios de acuerdo con los avances tecnológicos y exigencias actuales.

1. OBJETIVOS DE LA CONTRATACIÓN

1.1. OBJETIVO GENERAL

Contratar una empresa de telecomunicaciones que brinde los servicios de internet, seguridad perimetral e Interconexión de sedes para la UNA Puno, de forma eficiente e ininterrumpidamente los 365 días del año durante el plazo de ejecución contractual de 1110 días calendarios.



1.2. OBJETIVOS ESPECÍFICOS

- Contar con un servicio de internet ininterrumpido con una tasa garantizada de por lo menos 99,0%, con un overbooking 1:1, para toda la UNA Puno y sus sedes de acuerdo con el requerimiento de ancho de banda de cada una de estas.
- Contar con un servicio de seguridad gestionada de última generación y tecnología vigente perimetral que proteja la infraestructura de internet de las sedes de la universidad.
- Contar con un servicio de Interconexión de sedes de forma eficiente con una tasa garantizada de por lo menos 99.0% con un overbooking 1:1 y con un ancho de banda de acuerdo con el requerimiento para cada una de estas.
- Contar con un SLA no menor al 98% para las sedes de Chuquibambilla y Chucuito.

ALCANCE Y DESCRIPCIÓN DE LOS SERVICIOS A CONTRATAR

Sector 1

Sedes	Dirección	Ancho de Banda Internet	Cantidad de Ips Públicas	Ancho de Banda Interconexión de sedes	Seguridad Nivel 1	Seguridad Nivel 2
Ciudad Universitaria	Av. Floral N° 1153 – Puno	3200 Mbps	60	300 Mbps	Seguridad Gestionada	DDoS, Sandbox, WAF
Edificio de Educación Continua	Av. El Sol N° 329 – Puno	500 Mbps	12	75 Mbps	Seguridad Gestionada	
Edificio Facultad de Ciencias Jurídicas y Políticas	Esquina Jr. Grau con Jr. Conde de Lemos – Puno	300 Mbps	12	75 Mbps	Seguridad Gestionada	
Edificio Centro de Idiomas	Jr. Lima N° 272 – Puno	300 Mbps	12	75 Mbps	Seguridad Gestionada	
Edificio CEPREUNA e Instituto de Informática INFOUNA	Jr. Acora N° 235	300 Mbps	12	75 Mbps	Seguridad Gestionada	

Sector 2

Sedes	Dirección	Ancho de Banda Internet	Cantidad de Ips Públicas	Seguridad Nivel 1	Coordenadas
Sede Chuquibambilla	Carrera Panamericana Km 17 Sector Chuquibambilla - Ayaviri	400 Mbps	6	Seguridad Gestionada	https://maps.app.goo.gl/UK18eiHMCwqFubYe7 -14.790235255092048, -70.72565546735643
Sede Chucuito	Jr. Piscicultura S/N Chucuito - Puno	100 Mbps	2	Seguridad Gestionada	https://maps.app.goo.gl/1vsbbkCeUwBxvHUU6 -15.896938486227203, -69.89649979256338

CARACTERÍSTICAS TÉCNICAS

2.1. GENERALIDADES

- El proveedor en coordinación con el personal de la Sub Unidad de Redes y Comunicaciones de la OTI, deberá implementar lo solicitado en el presente proceso.
- El proveedor tiene la obligación de realizar los servicios de acuerdo con lo establecido en los Términos de Referencia, teniendo la responsabilidad total sobre la instalación, implementación, pruebas y puesta en marcha de los servicios contratados y la infraestructura tecnológica que la soportara según la topología existente a la fecha.
- El proveedor será responsable de todo el despliegue y los elementos necesarios para la implementación de lo solicitado.
- El proveedor es responsable de efectuar los estudios de ingeniería respectivos que le permitan cumplir con lo solicitado, incluyendo realizar el cableado de acometida de las fibras ópticas, quien asumirá los costos que puedan involucrar. Para la realización de los trabajos de

Pág. 2



implementación dentro del local, se brindará todas las facilidades y accesos necesarios para la ejecución del servicio.

- El proveedor realizará lo establecido en los términos de referencia sin generar costo adicional alguno a la entidad durante el periodo de vigencia del contrato.
- El proveedor será responsable de mantener actualizado con las últimas versiones de firmware de los equipos y así mismo las actualizaciones de seguridad y otras actualizaciones que sean lanzadas a nivel mundial por los fabricantes de los equipos que forman parte de los servicios.
- El proveedor deberá tener en cuenta que el tendido de la fibra óptica en las sedes de la entidad no debe estar expuesto por lo cual deberá de utilizar las canalizaciones existentes tanto para las sedes de Ciudad Universitaria y Edificio de educación continua y además la fibra óptica que se instale para las nuevas sedes deberá ser protegida con canaleta o ductería según sea el caso y las condiciones de infraestructura de cada sede. La fibra para utilizar deberá estar correctamente interconectada, ordenada e identificada para cada una de las sedes.
- El proveedor deberá garantizar y velar por mantener la seguridad adecuada y el orden de los elementos en las áreas de trabajo donde se esté realizando los servicios. Debiendo tomar las debidas precauciones para evitar daños y debiendo garantizar su restauración completa en caso de que esto suceda.
- Todos los gastos de transporte del proveedor hacia la entidad necesarios para la instalación de los equipos, así como de los materiales y demás componentes necesarios para la instalación, implementación pruebas y puesta en marcha de los servicios serán asumidos por el proveedor.

2.2. DE CARÁCTER ESPECÍFICO

2.2.1. ANCHO DE BANDA SERVICIO INTERNET SECTOR 1



- Overbooking 1:1 a nivel nacional.
- Enlace transparente a los servicios sobre IP con capacidad para soportar todos los servicios y protocolos estándar de internet sin limitaciones, filtros o restricciones.
- La disponibilidad del servicio mensual será como mínimo de 99.0%.
- La tecnología para utilizar para la prestación del servicio estará basada enteramente en MPLS. No se aceptarán opciones en MetroEthernet. Para tal fin el proveedor deberá presentar una carta del fabricante que confirme que ha desplegado equipos para la MPLS del postor.
- El proveedor deberá tener la disponibilidad de protocolo de ruteo IPv4 e IPv6.
- Teniendo en cuenta que el postor, tiene que asegurar la comunicación constante durante toda la ejecución del servicio, el postor deberá contar con salidas internacionales de al menos (02) dos proveedores TIER I, con capacidad mínima de 100 Gbps, tanto como para su salida principal como para su salida de contingencia (100 % fibra óptica), para ello el postor deberá presentar en su propuesta, un diagrama de la salida internacional detallando los nombres de los proveedores TIER I.
- El medio de acceso de acceso físico de última milla del proveedor deberá ser 100% fibra óptica, podrá ser tendido de manera aérea y/o canalizada. No se aceptarán soluciones de última milla como radio enlaces u otra tecnología inalámbrica.
- El postor debe contar con un servicio de alto nivel de conectividad y con diversas opciones de acceso a los principales operadores, debiendo ser miembro activo del NAP (Network Access Point) con lo cual, se podrá ampliar la conexión a internet, aprovechando la red de los proveedores, respaldando sus acuerdos de intercambio y permitiendo una conexión continua y de baja latencia, para ello, el postor deberá presentar en su propuesta, una constancia del NAP que demuestre ser miembro de la Asociación NAP Perú, en calidad de operador ISP, con capacidad de 2 enlaces x 100 Gbps y así mismo deberá presentar una impresión del tráfico de la página web oficial del NAP (Opcional).
- El postor ganador de la buena Pro, deberá contar con su propio Centro de Operaciones de Red (NOC - Network Operations Center) y su propio Centro de Operaciones de Seguridad (SOC -

Security Operations Center). Dichos centros, deberán asegurar la comunicación directa con el proveedor ganador del servicio (sin la intervención de empresas externas). Para ello la entidad supervisará la atención de solicitudes y plazos establecidos en la presente base, por lo que el postor deberá presentar en su propuesta, su licencia de funcionamiento de la dirección del inmueble y un certificado vigente emitido por una empresa consultora externa (Certificadora en infraestructura y centros de comando de control) que acredite la operación e infraestructura propia del NOC & SOC.

- El postor deberá incluir en su servicio, un entorno web, con usuario y clave para el servicio redundado del DNS (Sistema de Nombres de Dominio) el cual deberá crear, actualizar, modificar y eliminar configuraciones de los registros DNS, permitiendo utilizar el entorno web, para un servicio autogestionado y seguro. Por lo tanto, el postor deberá presentar una declaración jurada, detallando que el DNS, cumple con las características solicitadas, estará alojado en territorio peruano y es de propiedad del postor.
- Por seguridad, el postor deberá contar como mínimo, con (02) servidores DNS (Principal y redundado) ubicados en Data Center (Centro de Datos) distintos a nivel nacional.
- Considerando la importancia, de que el postor asegure una correcta calidad del servicio, confirme la seguridad de la información y asegure la continuidad del servicio. El postor deberá contar con su certificación vigente del ISO 22301:2019, el cual incluirá como mínimo, la provisión, Instalación, Soporte, Monitoreo, Mantenimiento y Gestión, relacionados a los Servicios Cloud, Acceso Dedicado a Internet, Fibra oscura, Centro de Datos, Interconexión de Sedes y Servicios de Seguridad para clientes. Para ello, el postor deberá de presentar el certificado en la presentación de oferta; y en el caso de consorcio cada miembro deberá presentar su propia certificación.
- De acuerdo a la consulta N° 119 del pliego de consultas, será considerado como válido que los postores consideren como opcional el certificado ISO 22301:2019.
- El proveedor deberá entregar reportes mensuales o deberá entregar el acceso a una plataforma en línea para la generación de los reportes requeridos por el servicio utilizado (Utilización de ancho de banda, latencia, pérdida de paquetes y salud del router a nivel de CPU y memoria) en documento electrónico durante la primera semana siguiente de culminado el mes, durante el plazo del contrato.
- El proveedor debe tener una herramienta de monitoreo y supervisión en línea del enlace de internet y transporte de datos.



2.2.2. ANCHO DE BANDA SERVICIO INTERNET SECTOR 2

- Los enlaces a brindar deberán tener al menos las siguientes características
- Ancho de banda de al menos 400 Mbps y 100 Mbps según lo indicado en la tabla.
- El Contratista proporcionará un equipo router que soporte de ancho de banda solicitado.
- Alimentación de los equipos: 220 VAC
- Soporte técnico remoto 24x7, durante la operación del servicio se podrá acordar medios adicionales o alternativos de coordinación.
- EL CONTRATISTA debe proveer equipos homologados que sea exigencia del Ministerio de Transportes y Comunicaciones - MTC.
- Se suscribirá un acta conformidad al término de la Fase Pre-operativa luego de que el CONTRATISTA realice la entrega de los equipos a la ENTIDAD en la dirección acordada.
- Una vez finalizado el plazo contractual se procederá a la devolución total de los equipos que le hayan sido entregados y/o instalados bajo cualquier modalidad (incluyendo equipos, accesorios, routers, switches y/o cualquier otro de propiedad del Contratista) sin más desgaste que el de su uso normal y diligente. Teniendo un plazo máximo de 30 días calendario una vez finalizado el plazo del contrato. Aceptando que en caso de pérdida, deterioro o robo deberán asumir el costo de los mismos.



2.2.3. ASIGNACIÓN DE IP PÚBLICA

Sector 1: El proveedor entregará direcciones IPv4 y asignará 108 direcciones IPv4 públicas para el uso de la UNA-PUNO según el siguiente detalle:

LOCAL	DIRECCIÓN	Ancho de Banda Internet	CANTIDAD IP PÚBLICAS (*)
Ciudad Universitaria	Av. Floral N° 1153 – Puno	3200 Mbps	60
Edificio de Educación Continua	Av. El Sol N° 329 – Puno	500 Mbps	12
Edificio Facultad de Ciencias Jurídicas y Políticas	Esquina Jr. Grau con Jr. Conde de Lemos – Puno	300 Mbps	12
Edificio Centro de Idiomas	Jr. Lima N° 272 – Puno	300 Mbps	12
Edificio CEPREUNA e Instituto de Informática INFOUNA	Jr. Acora N° 235	300 Mbps	12



- (*) El proveedor deberá asignar las IP públicas a las interfaces de los ruteadores, IP públicas de acceso a la WAN. La Cantidad de direcciones indicadas en la tabla anterior son direcciones reales, de las cuales 3 direcciones se utilizarán para asignarlas a la configuración de los equipos.
- Para el caso de la sede Ciudad Universitaria el proveedor deberá de utilizar direcciones IP públicas para las interfaces del firewall principal y secundario y demás direcciones IP públicas que permitan la alta disponibilidad de equipamiento arrendado por el proveedor.

Sector 2: El proveedor entregará direcciones IPv4 y asignará direcciones IPv4 públicas para el uso de la UNA-PUNO según el siguiente detalle:

Sedes	Dirección	Ancho de Banda Internet	Cantidad de Ips Públicas
Sede Chuquibambilla	Carrera Panamericana Km 17 Sector Chuquibambilla - Ayaviri https://maps.app.goo.gl/UK18eiHMCwqFubYe7 -14.790235255092048, -70.72565546735643	400 Mbps	6
Sede Chucuito	Jr. Piscicultura S/N Chucuito – Puno https://maps.app.goo.gl/1vsbbkCeUwBxvHUU6 -15.896938486227203, -69.89649979256338	100 Mbps	2

[Handwritten signature]



El proveedor deberá asignar las IP públicas a los dispositivos de salida a internet.
Para ambas sedes el proveedor deberá de utilizar direcciones IP públicas para la solución de seguridad.

2.2.4. TRANSPORTE DE DATOS VPN

- El proveedor del servicio deberá de integrar las sedes de Edificio Educación Continua, Edificio Facultad de Ciencias Jurídicas y Políticas, Edificio Centro de Idiomas y Edificio Instituto de Informática INFOUNA – CEPREUNA, con el campus universitario mediante un enlace en Capa 3 con un transporte mínimo de 75Mbps de ancho de banda para cada sede.
- En la sede Campus universitario deberá haber un enlace de datos de 300Mbps de ancho de banda.
- Enlace de datos será dedicado por fibra óptica del proveedor.
- El servicio entregado deberá ser 100% en fibra óptica hasta la última milla para todas las sedes.

Pág. 5

- La disponibilidad del servicio será como mínimo 99.0%.
- La tecnología para utilizar para la prestación del servicio estará basada enteramente en MPLS. No se aceptarán opciones en MetroEthernet. Para tal fin el proveedor deberá presentar una carta del fabricante que confirme que ha desplegado equipos para la MPLS del postor.

2.2.5. EQUIPAMIENTO REQUERIDO

- El proveedor deberá instalar en todas las sedes el siguiente equipamiento como mínimo para garantizar la óptima prestación del servicio.

- Equipo Ruteador para el enlace de Internet.
- Equipo Ruteador para el servicio de transporte de datos VPN.
- Equipo de seguridad perimetral para todas las sedes.

Todos los equipos, elementos y/o accesorios deben ser nuevos, sin uso y con garantía vigente del fabricante por el periodo del servicio. Todos los equipos serán instalados en un gabinete estándar, para lo cual deberán contar con todos sus accesorios y elementos a ser rackeados.

- Para el caso de la sede Ciudad Universitaria el proveedor deberá de considerar 2 equipos Firewall configurados en Alta Disponibilidad por tratarse de una sede de alta contingencia en caso de falla de equipamiento.
- Todos los equipos deberán estar dimensionados por el proveedor con la suficiente capacidad de procesamiento, memoria y almacenamiento para brindar el servicio en óptimas condiciones.
- El proveedor será el responsable por la actualización del firmware y todo el software que posea el equipamiento, así como realizar y almacenar las copias de respaldo de la configuración de cada equipo.
- La administración y gestión de los equipos de seguridad será compartida con el administrador de redes de la UNA-PUNO, así como de la configuración y gestión de cambios, creación de políticas y demás modificaciones.
- El equipamiento propuesto no debe ser del tipo End Of Sale.
- Se deberá adjuntar la carta del fabricante y/o distribuidor autorizado que confirme la vigencia técnica de los equipos, la cual deberá entregarse durante la etapa del inicio del servicio.

2.2.6. EQUIPAMIENTO REQUERIDO PARA LA GESTIÓN DE SEGURIDAD Gestionada –NIVEL 1 – SECTOR 1

- a. El software del equipo ofrecido deberá ser en su versión más reciente.
- b. El dispositivo debe estar catalogado como NGFW (Next Generation Firewall / Firewall de Nueva Generación).
- c. Debe incluir las funciones de Firewall, VPN (IPSec y SSL), SDWAN, Control de Aplicaciones, IPS, Antivirus y Filtro Web.
- d. Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers).
- e. El dispositivo contará con la capacidad de establecer instancias virtuales sobre el mismo dispositivo, de ser el caso deberá contar con el licenciamiento aplicado y disponible por el tiempo de contrato de la solución.
- f. Los equipos de seguridad ofertados deben corresponder a un fabricante que figure como líder en los últimos años (Se aceptará 2021 y 2022) en el cuadrante mágico de Gartner para la solución de Network Firewalls.
- g. Deben ser adecuados para montaje en rack 19"

- h. Deberán estar asociados con una solución de Reportería Avanzada ya sea on-premise o en la nube del proveedor la cual deberá brindar reportes mensuales de tráfico e informes ejecutivos para toma de decisión.
- i. Asimismo, deberán cumplir las siguientes características mínimas:

2.2.6.1 EQUIPAMIENTO PARA LA SEDE CIUDAD UNIVERSITARIA

- Throughput de NGFW debe ser de 11.5 Gbps como mínimo. Se tomará en consideración mediciones de throughput tomadas con 100% de tráfico http, Enterprise mix o tráfico real, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 25544, 2647 o 1242. En caso, el fabricante tenga publicados múltiples números de desempeño, solamente se aceptará el valor más pequeño.
- Throughput de prevención de amenazas (Firewall, control de aplicaciones, protección antivirus y antimalware) debe ser de 10 Gbps como mínimo y debe estar medido en condiciones reales o con tráfico mixto.
- En caso de que el fabricante tenga publicados múltiples números de desempeño (Throughput) para cualquiera de las funcionalidades, solamente se aceptará el de valor más pequeño.
- Throughput de VPN IPSec debe ser de 55 Gbps como mínimo.
- Throughput de Inspección de SSL debe ser de 9 Gbps como mínimo
- Soportar 8 Millones de conexiones o sesiones concurrentes.
- Soportar 550 000 nuevas conexiones o sesiones por segundo.
- Tener al menos dieciocho (18) Interfaces 10/100/1000 RJ45.
- Tener al menos Ocho (08) Interfaces 1G SFP.
- Tener al menos Cuatro (04) Interfaces 10G SFP+.
- Tener al menos Cuatro (04) Interfaces 25G SFP28
- 01 interface de tipo consola o similar.
- 02 fuentes de poder AC redundantes
- Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance.
- Debe proporcionar una base de datos dinámica de aplicaciones en la nube como aplicaciones SaaS, donde las direcciones IP cambian con frecuencia
- Debe poder reconocer por lo menos 4200 aplicaciones diferentes, incluyendo el tráfico relacionado a P2P (Peer-to-Peer), redes sociales, acceso remoto, update de software, protocolos de red, VOIP, audio, video, proxy, mensajería instantánea, compartición de archivos, email.
- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware o Antimalware integrados en el propio equipamiento.
- La solución deberá poder integrarse con Active Directory de Microsoft. Esta integración permitirá identificar el usuario y aplicar políticas de firewall por medio de cuentas y grupos de usuarios basados en el Active Directory.
- Filtrado de contenido basado en categorías en tiempo real. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías.
- Soportar VPN SSL o VPN IPsec para clientes o usuarios
- La solución debe soportar al menos 10000 clientes VPN SSL simultáneos.
- Las VPN SSL deben permitir que el usuario realice la conexión por medio de agente instalado en su dispositivo (PC, Laptop) o por medio de interfaz WEB.

Pág. 7

- Las VPN SSL deben soportar autenticación vía AD o LDAP o base de usuarios local.
- El agente de VPN SSL e IPsec debe ser compatible al menos con: Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Mac OS, Apple iOS y Android, se deben incluir todas las licencias asociadas a este servicio.
- La consola de administración de la solución puede ser interna o externa al equipo firewall para lo cual, de ser externa, el contratista debe incluir el hardware y licencias que cumplan con lo definido en las presentes especificaciones técnicas.
- La solución deberá soportar acceso vía SSH, cliente WEB (HTTPS) o interfaz GUI.
- En caso de que sea necesario la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operativos Windows.



2.2.6.2 EQUIPAMIENTO PARA LAS SEDES EDUCACIÓN CONTINUA, SEDE CIENCIAS JURÍDICAS Y POLÍTICAS, EDIFICIO CEPREUNA E INSTITUTO DE INFORMÁTICA INFOUNA, SEDE EDIFICIO CENTRO DE IDIOMAS

- Throughput de NGFW debe ser de 3.2 Gbps como mínimo. Se tomará en consideración mediciones de throughput tomadas con 100% de tráfico http, Enterprise mix o tráfico real, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 25544, 2647 o 1242. En caso, el fabricante tenga publicados múltiples números de desempeño, solamente se aceptará el valor más pequeño.
- Throughput de prevención de amenazas (Firewall, control de aplicaciones, protección antivirus y antimalware) debe ser de 3 Gbps como mínimo y debe estar medido en condiciones reales o con tráfico mixto.
- En caso de que el fabricante tenga publicados múltiples números de desempeño (Throughput) para cualquiera de las funcionalidades, solamente se aceptará el de valor más pequeño.
- Throughput de VPN IPsec debe ser de 8 Gbps como mínimo.
- Throughput de Inspección de SSL debe ser de 3.4 Gbps como mínimo
- Soportar 3 millones de conexiones o sesiones concurrentes.
- Soportar 280 000 nuevas conexiones o sesiones por segundo.
- Tener al menos dieciocho (18) Interfaces 10/100/1000 RJ45.
- Tener al menos Ocho (08) Interfaces 1G SFP.
- Tener al menos Cuatro (04) Interfaces 10G SFP+.
- 01 interface de tipo consola o similar.
- 02 fuentes de poder AC o DC, redundantes incorporadas en el chasis.
- Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance.
- Debe proporcionar una base de datos dinámica de aplicaciones en la nube como aplicaciones SaaS, donde las direcciones IP cambian con frecuencia
- Debe poder reconocer por lo menos 4000 aplicaciones diferentes, incluyendo el tráfico relacionado a P2P (Peer-to-Peer), redes sociales, acceso remoto, update de software, protocolos de red, VOIP, audio, video, proxy, mensajería instantánea, compartición de archivos, email.
- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware o Antimalware integrados en el propio equipamiento.





- Debe contar con funcionalidad de Análisis de archivos sospechosos o detección de malware desconocido en la nube (emulación de sandboxing).
- La solución deberá poder integrarse con Active Directory de Microsoft. Esta integración permitirá identificar el usuario y aplicar políticas de firewall por medio de cuentas y grupos de usuarios basados en el Active Directory.
- Filtrado de contenido basado en categorías en tiempo real. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías.
- Soportar VPN SSL o VPN IPsec para clientes o usuarios
- La solución debe soportar al menos 500 clientes VPN SSL simultáneos.
- La solución debe soportar 500 túneles VPN client-to-site IPsec simultáneos.
- Las VPN SSL deben permitir que el usuario realice la conexión por medio de agente instalado en su dispositivo (PC, Laptop) o por medio de interfaz WEB.
- Las VPN SSL deben soportar autenticación vía AD o LDAP o base de usuarios local.
- El agente de VPN SSL e IPsec debe ser compatible al menos con: Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS, Apple iOS y Android, se deben incluir todas las licencias asociadas a este servicio.
- La consola de administración de la solución puede ser interna o externa al equipo firewall para lo cual, de ser externa, el contratista debe incluir el hardware y licencias que cumplan con lo definido en las presentes especificaciones técnicas.
- La solución deberá soportar acceso vía SSH, cliente WEB (HTTPS) o interfaz GUI.
- En caso de que sea necesario la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operativos Windows.

[Handwritten signature]





2.2.7. EQUIPAMIENTO REQUERIDO PARA LA GESTIÓN DE SEGURIDAD Gestionada – NIVEL 1 – SECTOR 2

- a. La solución deberá estar catalogado como NGFW (Next Generation Firewall / Firewall de Nueva Generación) y deberá ser un equipo físico de propósito específico.
- b. Debe incluir las funciones de Firewall, VPN (IPsec y SSL), Control de Aplicaciones, IPS, Antivirus y Filtro Web.
Por seguridad y facilidad de administración, no se aceptan equipos de propósito genérico (PCs o servers).
Deberán estar asociados con una solución de Reportería Avanzada ya sea on-premise o en la nube del proveedor la cual deberá brindar reportes mensuales de tráfico e informes ejecutivos para toma de decisión.
- e. Asimismo, deberán cumplir las siguientes características mínimas:

2.2.7.1 EQUIPAMIENTO PARA LAS SEDE CHUQUIBAMBILLA Y SEDE CHUCUITO

- Throughput de NGFW debe ser de 2.5 Gbps como mínimo. Se tomará en consideración mediciones de throughput tomadas con 100% de tráfico http, Enterprise mix o tráfico real, no se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 25544, 2647 o 1242. En caso, el fabricante tenga publicados múltiples números de desempeño, solamente se aceptará el valor más pequeño.



- Throughput de prevención de amenazas (Firewall, control de aplicaciones, protección antivirus y antimalware) debe ser de 2.2 Gbps como mínimo y debe estar medido en condiciones reales o con tráfico mixto.
- En caso de que el fabricante tenga publicados múltiples números de desempeño (Throughput) para cualquiera de las funcionalidades, solamente se aceptara el de valor más pequeño.
- Throughput de VPN IPsec debe ser de 20 Gbps como mínimo.
- Throughput de Inspección de SSL debe ser de 2.6 Gbps como mínimo.
- Soportar 3 millones de conexiones o sesiones concurrentes.
- Soportar 120 000 nuevas conexiones o sesiones por segundo.
- Tener al menos Ocho (08) Interfaces 10/100/1000 RJ45.
- Tener al menos Dos (02) Interfaces 10G SFP+
- Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance.
- Debe proporcionar una base de datos dinámica de aplicaciones en la nube como aplicaciones SaaS, donde las direcciones IP cambian con frecuencia
- Debe poder reconocer por lo menos 4000 aplicaciones diferentes, incluyendo el tráfico relacionado a P2P (Peer-to-Peer), redes sociales, acceso remoto, update de software, protocolos de red, VOIP, audio, video, proxy, mensajería instantánea, compartición de archivos, email.
- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware o Antimalware integrados en el propio equipamiento.
- Debe contar con funcionalidad de Análisis de archivos sospechosos o detección de malware desconocido en la nube (emulación de sandboxing).
- La solución deberá poder integrarse con Active Directory de Microsoft. Esta integración permitirá identificar el usuario y aplicar políticas de firewall por medio de cuentas y grupos de usuarios basados en el Active Directory.
- Filtrado de contenido basado en categorías en tiempo real. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías.
- Soportar VPN SSL o VPN IPsec para clientes o usuarios
- La solución debe soportar al menos 50 clientes VPN SSL o IPSEC simultáneos.
- La solución debe soportar 50 túneles VPN client-to-site IPsec simultáneos.
- Las VPN SSL deben permitir que el usuario realice la conexión por medio de agente instalado en su dispositivo (PC, Laptop) o por medio de interfaz WEB.
- Las VPN SSL o IPSEC deben soportar autenticación vía AD o LDAP o base de usuarios local.
- El agente de VPN SSL e IPsec debe ser compatible al menos con: Windows 7, Windows 8, Windows 8.1, Windows 10, Mac OS, Apple iOS y Android, se deben incluir todas las licencias asociadas a este servicio.
- La consola de administración de la solución puede ser interna o externa al equipo firewall para lo cual, de ser externa, el contratista debe incluir el hardware y licencias que cumplan con lo definido en las presentes especificaciones técnicas.
- La solución deberá soportar acceso via SSH, cliente WEB (HTTPS) o interfaz GUI.
- En caso de que sea necesario la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operativos Windows.

**2.2.8. EQUIPAMIENTO REQUERIDO PARA LA GESTIÓN DE SEGURIDAD Gestionada – NIVEL 2 –
SOLO SEDE CIUDAD UNIVERSITARIA**

2.2.8.1. SERVICIO DE PROTECCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO

- El postor deberá ofrecer un servicio de mitigación de ataques DDoS ubicado en la infraestructura del proveedor.
- La mitigación en la nube se realizará cuando el enlace de conexión a Internet sea saturado por un ataque DDoS volumétrico.
- El postor debe proteger el enlace de Internet del campus universitario con un servicio de detección y mitigación de ataques de Denegación de Servicio Volumétricos dirigidos a las IPs públicas de la Entidad.
- Deberá ser una solución con capacidad de mitigación de al menos 80 Gbps dentro de la infraestructura del proveedor.
- El servicio de mitigación ofertado debe basarse en tecnologías que analicen el patrón de tráfico hacia el cliente y solo al detectar un inminente ataque hagan un desvío del tráfico hacia un centro de limpieza.
- El sistema desplegado en la red del postor debe ser un appliance diseñado específicamente (Stateless) para proporcionar disponibilidad de servicios IP y debe estar dedicado a esta función, por lo que no se aceptarán dispositivos que mantengan estado de las conexiones como cortafuegos, sistemas de prevención y detección, y las variantes o combinaciones como UTM, NGFW, NGIPS; ya que al conservar el estado de la conexión se vuelven ellos mismos susceptibles a ataques DDoS.
- El sistema debe ser capaz de informar la cantidad de tráfico malicioso bloqueado en bps y durante una mitigación activa.
- Se deberá brindar un usuario de lectura para la solución de Mitigación de ataques de DDoS (Opcional).

2.2.8.2. SERVICIO DE FIREWALL DE APLICACIONES

- La solución deberá ser brindada con un appliance dedicado onpremise para la protección de aplicaciones web publicadas e internas dentro de la institución.
- La solución debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web (WAF –Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.
- El equipo debe tener un throughput HTTP de 500 Mbps.
- Debe contar con un almacenamiento interno de 480GB SSD o 1TB HDD.
- El equipo no debe tener limitación en cuanto a cantidad de aplicaciones a proteger. El límite debe estar definido únicamente por la capacidad del equipo.
- Debe contar con cuatro (04) interfaces GE RJ45 y cuatro (04) SFP GE.
- La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP.
- La solución debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web (WAF –Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.
- Debe tener soporte nativo de HTTP/2.
- Debe soportar traducción de HTTP/2 a HTTP 1.1
- Deberá soportar interoperabilidad con OpenAPI 3.0
- Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica.
- La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de

Pág. 11



[Handwritten signature]



- datos que contiene los últimos y más peligrosos virus.
- Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no.
 - Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial.
 - Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo.
 - El perfil aprendido de forma automática debe de poder ser ajustado.
 - Tener la capacidad de creación de firmas de ataques customizables
 - Tener la capacidad de protección contra ataques tipo:
 - Adobe Flash binary (AMF) protocol
 - Botnet
 - Browser Exploit Against SSL/TLS (BEAST)
 - Acceso por fuerza bruta
 - Clickjacking
 - Cambios de cookie
 - Zero Day Attacks
 - Credit Card Theft
 - Cross Site Request Forgery (CSRF)
 - Cross site scripting (XSS)
 - Denial of Service (DoS)
 - HTTP header overflow
 - Local File inclusion (LFI)
 - Man-in-the-middle (MITM)
 - Remote File Inclusion (RFI)
 - Server Information Leakage
 - Low-rate DoS
 - Slow POST attack
 - Slowloris
 - Malformed XML
 - SYN flood
 - Forms Tampering
 - Manipulación de campos ocultos
 - Tipo Directory Traversal
 - Access Rate Control
 - Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection).
 - Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold.
 - Permitir configurar reglas de bloqueo a métodos HTTP no deseados.
 - Permitir que se configuren reglas de límite de upload por tamaño del archivo.
 - Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país.
 - Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado.
 - Permitir configurar listas negras de bloqueo y listas blancas de confianza, basadas en dirección IP de origen.
 - Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución.



- Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation.
- Tener la capacidad de conectarse a una base de datos en Internet para validar que las credenciales que usan los usuarios para acceder a algún sistema no sean credenciales robadas.
- Tener la capacidad de prevención contra pérdida de información (DLP), bloqueando la pérdida de información del encabezado HTTP.
- Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo.
- Tener la funcionalidad de antivirus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo.
- Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado.
- Debe de ser capaz de hacer aceleración de tráfico SSL basada en hardware.
- La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleración de tráfico.
- Para SSL/TLS offload soportar al menos TLS 1.0, 1.1, 1.2 y 1.3
- La solución debe tener la capacidad de almacenar certificados digitales de CA's.
- La solución debe de ser capaz de generar CSR para ser firmado por una CA.
- La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL.
- La solución debe contener las firmas de bot conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones
- La solución debe de tener un sistema de bloqueo con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizado automáticamente.
- La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores.
- La solución debe permitir la customización o reenvío de solicitudes y respuestas HTTP en el HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body y HTTP Location.
- La solución debe permitir crear reglas definiendo el orden con que las páginas deben de ser accedidas para prevenir ataques como cross-site request forgery (CSRF).
- La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP.
- La solución debe tener la capacidad de proteger contra detección de campos ocultos. Permitir que se configuren firmas customizadas de ataques y DLP, a través de expresiones regulares
- La solución contar con una herramienta de análisis de vulnerabilidades o debe permitir la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, etc, para proveer parches virtuales.
- Debe generar perfil de protección automáticamente a partir de reporte en formato XML generado por scanner de vulnerabilidad de terceros. El análisis deberá realizarse al menos cada 3 meses.
- Debe permitir programar la verificación de vulnerabilidades.
- La solución debe generar un reporte de análisis de vulnerabilidades en formato HTML.
- Soportar redirección y reescritura de requisiciones y respuestas HTTP.
- Permitir redirección de requisiciones HTTP para HTTPS.
- Permitir reescribir la línea URL del encabezado de una requisición HTTP.
- Permitir reescribir el campo HOST del encabezado de una requisición HTTP.
- Permitir reescribir el campo REFERER del encabezado de una requisición HTTP.
- Permitir redirigir requisiciones para otro website.



- Permitir enviar respuesta HTTP 403 Forbidden para requisiciones HTTP
 - Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección HTTP de un servidor web.
 - Permitir reescribir el cuerpo ("body") de una respuesta HTTP de un servidor web.
 - Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando en modo proxy reverso.
 - La solución debe de soportar reglas para definir si las requisiciones HTTP serán aceptadas en función de la URL y origen de la petición y, si necesario, aplicar una tasa específica de velocidad (rate limit).
- La solución debe de soportar combinación de control de acceso y autenticación utilizando mecanismos como HTML Form, Basic y soporte a SSO, métodos como LDAP y RADIUS para consultas e integración de los usuarios de la aplicación.
- Tener capacidad de caching para aceleración web.
 - La solución debe de ser capaz de enviar archivos para solución de sandboxing del mismo fabricante, a través de una política de restricción de carga del archivo.
 - Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes.

2.2.8.3. SERVICIO DE PROTECCIÓN DE CORREO

Se requiere 01 unidad de appliance físico, de propósito específico. Este equipo debe incluir las siguientes capacidades:

1.1. Características generales

- a) Ninguno de los modelos ofertados podrá estar listados en la página web del fabricante como listas de end-of-life (EOL) ni end-of-sale (EOS).
- b) Debe ser mínimo 01 unidad de rack 19" e incluir componentes de montaje.



1.2. Características de rendimiento

- a) Permitir configurar por lo menos 25 dominios.
- b) Soportar como mínimo 140 000 mensajes por hora o 38 correos por segundo, con análisis de antispam, antivirus y sandboxing habilitado.

1.3. Debe contar con un almacenamiento interno de al menos 2 TB.

1.4. Funcionalidades y capacidades

- a) El producto debe tener una efectividad de detección de SPAM mínimo del 99%. Deberá entregarse información de sustento para certificar esta funcionalidad.
- b) La solución debe incluir capacidades activas de antispam, antivirus, antiphishing, DLP, filtro URL, a fin de inspeccionar y bloquear correo entrante y saliente según las políticas. Se aceptará capacidades activas de protección BEC o de suplantación de identidad solo para correo entrante según las políticas.
- c) La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.
- d) La solución debe soportar listas de permitidos y de bloqueados para emisores y destinatarios de correo, a nivel de usuario, de dominio y global para todo el sistema.
- e) La solución debe soportar listas de bloqueo de terceros tales como DNSBL y SURBL.
- f) Debe asignar automáticamente un puntaje a los dispositivos endpoint emisores de correo y permitir colocarlos en una lista de bloqueo según un umbral de puntaje obtenido.
- g) La solución debe ser capaz de mantener listas de reputación de remitentes identificados al menos por IP pública, en base a como mínimo: número de virus enviado y la cantidad de correos spam.



h) La solución debe ser capaz de ejecutar el análisis antivirus o antimalware sobre archivos comprimidos como ZIP y RAR.

i) Debe permitir bloquear archivos comprimidos cuando estén cifrados con contraseña.

j) Debe permitir inspeccionar archivos comprimidos protegidos por contraseña, mediante listas de contraseñas y que pueda usar contraseñas encontradas en el cuerpo del mensaje de correo.

k) La solución debe poder definir el reenvío de correo (relay) a una IP específica, tomando como base a la IP origen del mensaje.

l) Debe permitir establecer límites en la tasa de correos enviados y recibidos, así como límite para el tamaño de los correos electrónicos.

m) La solución debe ser compatible con la implementación de políticas por destinatario y por dominio, del tráfico entrante o saliente.

n) La solución debe permitir definir como mínimo las siguientes acciones para los correos analizados: aceptar, reenviar, rechazar o descartar, enviar a cuarentena, archivar, enviar copia oculta BCC, modificar el subject.

o) La solución debe ser capaz de verificar la existencia de los usuarios en una base de LDAP como validación para entregar el correo.

p) La solución debe soportar cuarentena de correo entrante y saliente por usuario, permitiendo que cada usuario pueda gestionar por web o POP3 sus propios mensajes en cuarentena, mediante la eliminación o la liberación de los mensajes que no considere spam.

q) La solución debe poder escanear nuevamente los correos que han sido liberados de la cuarentena por el usuario en busca de contenido de virus o malware.

r) La solución debe ser capaz de programar el envío de reportes de cuarentena.

s) La solución debe ser capaz de mantener la cola de correo en caso de fallo en la conexión de salida, retrasos o errores de entrega.

t) La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.

u) Debe ser capaz de recibir y entregar correos electrónicos para cualquier red IPv4 e IPv6 y aplicando políticas de contenido, alineado al "Plan de Transición al Protocolo IPv6 en las entidades de la Administración Pública".

v) La solución debe proporcionar un control/verificación de DNS reverso.

w) La solución debe bloquear orígenes cuestionables basado en una base de datos de reputación de IP's suministrada por el fabricante.

x) Debe bloquear spam en otros idiomas aparte del español.
La solución debe bloquear correo como spam al revisar las URL's que contenga el mensaje y comparándolas con la base de datos de URL's suministrada por el fabricante.
La revisión de URL's debe permitir seleccionar las categorías URL que serán permitidas o restringidas en los correos analizados. Esta base de datos de categorías será actualizada por el fabricante.

aa) La solución debe ser capaz de realizar análisis de imágenes y PDF, identificando con este criterio si el correo es SPAM.

bb) La solución debe ser compatible con Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) y Domain Based Message Authentication (DMARC).

cc) La solución debe incluir capacidades de evaluar, retener y/o bloquear correos que contengan amenazas avanzadas desconocidas, de día cero, mediante el análisis de archivos con herramientas de sandboxing.

dd) La solución debe proteger contra ataques del tipo Bounce Attack.

ee) Debe incluir el análisis de sandboxing con soluciones on-premise o en la nube.

ff) Debe ser capaz de remover o neutralizar contenido potencialmente malicioso (links, macros, scripts) de documentos de Microsoft Office y PDF como mínimo y que permita entregar los documentos al destinatario sin el contenido potencialmente malicioso. Se aceptará también una solución de equipo appliance más un servicio en nube, siempre y cuando en conjunto cubran los requerimientos en su totalidad.



- gg) La solución debe analizar las imágenes en busca de tipos de imágenes inapropiadas, que contengan contenido para adultos.
- hh) La funcionalidad DLP debe permitir definir la información a bloquear como palabras, frases, expresiones regulares, fingerprint de archivos específicos que se aplique sobre archivos adjuntos (attachments) y contenido del mensaje de correo.
- ii) Debe soportar cifrado de mensajes de correo, donde al ser interceptada la comunicación no sea legible para el atacante y debe mantener un proceso de autenticación para el acceso del destinatario al mensaje. Se aceptará IBE (Identity Based Encryption) o S/MIME u otros sistemas de cifrado que cumplan o superen lo requerido.
- jj) Debe soportar comunicaciones seguras de correo por SMTPS y SMTP over TLS como mínimo, u otros sistemas de cifrado que cumplan o superen las especificaciones de SMTPS y SMTP over TLS o superior.
- kk) La solución debe ser capaz de realizar almacenamiento y retención de correo electrónico (Archivado/archiving) localmente o remotamente para al menos 30 cuentas de correo de usuarios top.

1.5. Gestión

- a) La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS).
- b) Debe permitir agregar el logo de la entidad en la interfaz gráfica web.
- c) Debe tener disponible un API REST para fines de monitoreo, automatización y orquestación, donde el API REST permita como mínimo agregar direcciones IP's para que se bloqueen correos desde dichas fuentes en el equipo.
- d) La solución debe contar con herramientas gráficas para visualizar fácilmente las sesiones TCP activas en el equipo, resumen de estadísticas de: actividad de correo, encolamiento, malware y spam detectado, consumo de recursos.
- e) La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura/escritura (Read/Write) o de sólo lectura (Read Only).
- f) La solución debe permitir configurar administradores por dominio, los cuales no puedan realizar cambios de configuración para otros dominios.
- g) La solución debe soportar integrarse con soluciones de autenticación de doble factor y soluciones RADIUS como mínimo para el inicio de sesión de usuarios administradores.
- h) La solución debe permitir esquemas de alta disponibilidad, Activo-Activo y Activo-Pasivo.
- i) La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos al menos a 3 servidores remotos (monitoreo SOC, syslog server de administración de seguridad y dispositivo de analítica para incidentes) a través de Syslog. Los registros (logs) del antispam deben contener información de la regla utilizada. Estos registros (logs) no deben ser modificables.
- k) Debe ser capaz de utilizar SNMPv3 para la supervisión y traps (alertas).
- l) La solución debe generar reportes a demanda y programados para intervalos de tiempo específicos, en PDF o HTML.
- m) Debe tener la capacidad de conectarse en tiempo real a una base de datos centralizada en el fabricante para descargar actualizaciones de software y firmas durante la vigencia de la licencia.



2.2.8.4. SERVICIO DE CONTROL DE ACCESOS PRIVILEGIADOS

Implementación

- El proveedor será responsable de considerar lo necesario en software y hardware para brindar el servicio solicitado, para lo cual, la entidad brindará todas las facilidades necesarias.

Funcionalidades Generales

- Solución de Privileged Access Management (PAM) que permita auditar el acceso a la administración de plataformas, servidores y aplicaciones por diferentes protocolos (SSH, Telnet, HTTP (S), RDP, etc), llevando registros históricos de los accesos, incluida la grabación de la sesión, (La grabación será por un periodo de 30 días y solo se considera el sector 1).
- La solución Privileged Access Management (PAM) basada en appliance físico o máquina virtual (VM), compatible con: VMWare, Microsoft Hyper-V, Azure y Aws.
- Se requiere suscripción para 5 usuarios administradores internos
- Gestor de sesiones privilegiadas con soporte para protocolos SSH, Telnet, RDP y VNC (función de proxy) y proxy RDP / VNC
- Gestor de claves (bóveda).



Gestión de sesiones

- Debe tener la capacidad de controlar, monitorear y auditar cifrado sesiones de administrador.
- Debe ejecutarse como pasarela entre los usuarios y los puntos finales de destino (enfoque de Intermediario de la sesión privilegiada).
- Debe soportar implementación con o sin instalación de agentes de software para acceder a puntos finales. Si es necesario, se utilizará un jump host donde se instale un agente (proxy de conexiones).
- Debe ser de rápida implementación y sin impacto en la experiencia de usuario final.
- Se podrá instalar una solución en la nube del proveedor, manteniendo las mismas capacidades solicitadas en bases.

Gestión de claves

- Debe asegurar que el usuario real de la cuenta local sea indiscutible.
 - Debe registrar que usuario real utilizó el otp (contraseña de un solo uso), junto con el inicio y fin de su uso.
 - Debe limitar el tiempo de uso de claves.
 - Debe asegurar que se utilicen claves fuertes mediante la generación automática de las estas.
 - Debe guardar las claves en una bóveda segura.
 - Debe mantener actualizados todos los servicios y aplicaciones cliente con contraseña nueva haciendo que el gestor de claves los actualice.
- La contraseña no debe ser conocida por el usuario que solicitó el acceso al momento de realizar el login, sino que ésta debe ser inyectada directamente en el aplicativo.



Administración

- Debe permitir una administración centralizada.
- Debe tener capacidad para denegar a usuarios administradores el acceso para visualizar password o aprobar solicitudes de requerimientos de password.
- Debe tener la capacidad de aprovisionar usuarios en forma automática a partir de un Active Directory o LDAP, para así contar con un aprovisionamiento automático y transparente de cuentas que reflejen los cambios en dichos directorios.
- Debe ser capaz de administrar cuentas de altos privilegios basadas en directorio activo de Microsoft.
- Debe tener capacidad para administrar cuentas de altos privilegios de plataformas (servidores Windows, Linux, y dispositivos de red).

- Debe tener capacidad para administrar cuentas de altos privilegios de dispositivos de red vía SSH debe soportar cualquier dispositivo de red mediante conexión SSH.
- Debe soportar el uso de clientes de escritorio remoto nativos de Windows para el acceso directo.
- Debe proporcionar mecanismos para organizar las cuentas de altos privilegios y facilitar el acceso a los usuarios administradores.

Arquitectura

- Debe ser escalable mediante un diseño modular para adaptarse a crecimientos de utilización o de inclusión de más plataformas, por lo que no se debe adquirir módulos adicionales.
- Debe ser capaz de manejar la pérdida de conectividad con el repositorio central de passwords, sin que esto afecte los accesos administrados.
- La solución debe tener la capacidad de integración nativa con arquitecturas de la solución ZTNA propuesta.
- Debe tener la capacidad de integrarse con fuentes de identificación externa, por ejemplo, LDAP y mecanismos propios de autenticación. Debe tener la posibilidad de integrarse con servidores de autenticación vía SAML.
- Debe tener un algoritmo de cifrado SSH de alta resistencia.

Gestión de contraseñas y credenciales

- Debe tener la capacidad de cambiar un password.
- De acuerdo con una política (por un período de días establecido o bajo demanda).
- Mediante cambios manuales efectuados por un usuario.
- De forma automática, cuando un password no ha sido sincronizado (falla en verificación). Debe tener la capacidad de asignar passwords de valores aleatorios.
- Debe permitir excluir palabras o cadenas de caracteres dentro de la contraseña.
- Debe tener la capacidad de cambiar manualmente un password por un administrador en cualquier momento.
- Debe contar con un mecanismo de cambio de contraseñas.
- Capacidad de cambiar automáticamente el password de una cuenta que acaba de ser definida en el sistema.
- Debe tener la capacidad de configurar una longitud mínima de contraseña y complejidad para cuentas de superusuarios de todos los sistemas (excepto directorio activo).
- Debe tener la capacidad de ofrecer contraseñas únicas por dispositivo.
- Debe tener la capacidad de establecer políticas unificadas para la administración de cuentas de altos privilegios y monitoreo de sesiones.
- Debe tener la capacidad de enviar notificaciones vía correo electrónico u otros métodos de envío por tipos de actividad.
- Capacidad de soportar conexiones transparentes a un dispositivo destino, sin la necesidad de ver o ingresar la contraseña para la conexión.
- Debe tener la capacidad de soportar conexión directa a dispositivos Windows.
- Debe tener la capacidad de soportar conexión directa a dispositivos Unix / Linux de administración (SSH).
- Debe tener la capacidad de enviar correos electrónicos para lo siguiente:
 - Accesos a sistemas.
 - Cambios a sistemas.
 - Uso de contraseñas.
 - Solicitudes de aprobación de contraseña.



[Handwritten signature]



Monitoreo y Grabación de Usuarios

- Debe tener la capacidad de grabar sesiones de altos privilegios en: Windows, virtual servers, Linux, dispositivos de red.
- Debe contar con métodos de monitoreo de actividad de usuario.
- La grabación de la sesión no debe impactar el rendimiento del dispositivo destino.
- Debe tener la capacidad de que las conexiones remotas pueden ejecutarse sin tener que exponer las credenciales de cuentas de altos privilegios aun manteniendo un control de acceso estricto.
- Debe tener la capacidad de forzar control de acceso a dispositivos objeto de supervisión.
- Debe tener la capacidad de asegurar responsabilidad personal cuando se abre una sesión de altos privilegios con una cuenta compartida, de tal manera que los atributos de la identidad estén disponibles para poder realizar notificaciones, seguimiento y reportes.
- Debe tener la capacidad de ayudar a investigar la causa raíz y al análisis forense.
- Debe tener la capacidad de soportar conexiones remotas seguras a los dispositivos objeto de supervisión.
- Debe tener la capacidad para ejecutar búsquedas de comandos de altos privilegios dentro de las grabaciones de video.
- Debe ser eficiente en la reproducción de grabaciones.
- Debe tener la capacidad de ver y controlar (dualcontrol) las sesiones en vivo/tiempo real del monitoreo de sesiones.
- Debe tener la capacidad de intervenir y/o terminar remotamente una sesión en tiempo real cuando se ejecuta actividad sospechosa.
- Debe tener la capacidad de proveer a los usuarios administradores Unix / Linux con una interfaz cli para iniciar la grabación de sesiones de altos privilegios.
- Debe tener la capacidad de ofrecer grabaciones de todas las sesiones de altos privilegios.
- Debe tener la capacidad de permitir a los usuarios administradores Unix / Linux iniciar sesiones desde clientes SSH (Putty).

2.2.8.5. SERVICIO DE SANDBOXING EN NUBE

Se debe incluir un servicio de sandboxing, que podrá ser brindado desde la nube del postor o con un appliance dedicado onpremise, para la detección de amenazas avanzadas desconocidas, el servicio debe estar integrado al firewall de la ciudad universitaria y debe cumplir como mínimo con las siguientes características:

- La solución debe proporcionar la funcionalidad de inspección del tráfico entrante en busca de malware desconocido (APT: amenazas persistentes avanzadas y amenazas de día cero), ransomware con filtro de amenazas avanzado y análisis de ejecución en tiempo real, e inspección del tráfico saliente de callbacks.
- Poseer la capacidad de prevenir amenazas desconocidas
- Debido a que el malware es muy dinámico y un Antivirus reactivo común no puede detectarlos con la misma velocidad que se crean sus variaciones, la solución que se ofrece debe tener características para la prevención de malware desconocido incluídas en la propia herramienta (día cero)
- La solución debe soportar el análisis de 3000 archivos/día.
- La solución debe contar con la nube de inteligencia propia del fabricante que se encarga de actualizar toda la base de seguridad a través de firmas.
- Debe ser capaz de monitorear y analizar el tráfico generado por archivos maliciosos y así determinar la naturaleza del tráfico y sus conexiones.



[Handwritten signature]



- La solución debe poder inspeccionar el tráfico cifrado SSL.
- Compatibilidad con el análisis de archivos de paquetes de Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class), APK de Android y Linux en un entorno sandbox. Para los archivos APK de Android y Linux, el análisis podrá ser estático.
- Debe soportar los siguientes tipos de archivos: 7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .elf, .exe, .gz, .htm, .html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, .rl, .vbs, WEblink, .wsf, .xlam, .xls, .xlsb, .xlsx, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- Debe ser capaz de diferenciar los archivos analizados en al menos dos categorías: las que se identificaron como virus maliciosos y/o malignos y archivos sospechosos por tener comportamiento no esperado o características indeseables
- Debe ser capaz de clasificar los archivos sospechosos de acuerdo con el riesgo que suponen.
- Debe ser capaz de exportar los resultados del análisis de archivos maliciosos y sospechosos a PDF desde su propia interfaz de gestión
- Debe tener la capacidad de analizar en sandbox enlaces (HTTP y HTTPS) presentes en el cuerpo de los mensajes del correo electrónico SMTP. Debe generarse un informe si la apertura del enlace por el sandbox lo identifica como malicioso.
- Debe soportar el monitoreo de archivos transferidos en internet (HTTPS, FTP, HTTP, SMTP)
- La solución debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos.
- Seleccionar mediante política qué tipos de expedientes serán objeto de este análisis y prevención.
- Implementar e identificar malware en archivos adjuntos de correo electrónico y URL conocidos.
- Implementar detección y bloqueo inmediatos de malware que utilice un mecanismo de explotación en archivos PDF.
- El sistema de análisis debe proporcionar información sobre las actividades de los archivos maliciosos y sospechosos en las máquinas virtuales infectadas, información tal como qué procesos se inician por el archivo, los archivos creados, los archivos eliminados, los cambios realizados en el registro, el comportamiento de la red, como direcciones URL utilizadas por los programas maliciosos (seguros y no seguros) cambios de registros proporcionando información sobre el usuario infectado (al menos su dirección IP).
- Debe permitir la descarga de malware identificados a partir de la interfaz de gestión propia
- Se debe tener mecanismo de integración para proporcionar corrección automática. Una vez que se detecta el código malicioso, un paquete de firmas de antivirus basado en amenazas detectadas debe ser desarrollado y enviado a los dispositivos registrados como firewalls, y estaciones de trabajo de usuarios para ayudar en la mitigación.
- En caso de un veredicto positivo, debe presentar un desglose del comportamiento de la máquina comprometida, que contenga al menos información para fines de auditoría:
 - Sobre el Tipo de archivo
 - IP de origen del malware
 - IP de destino (cliente que descargó el malware)
 - virus Link to Reference Total
 - Resumen del comportamiento del malware.
- La solución local debe permitir la gestión a través de la interfaz de línea de comandos (CLI).
- La solución debe soportar las reglas YARA como estándar para la creación de reglas para la detección de malware
- La solución local va a crear cuentas de administrador con al menos dos perfiles distintos: la lectura y escritura y solamente lectura.
- La solución local debe permitir la creación de cuentas de administrador con autenticación local o remota a través de servidores RADIUS.



- La solución local debe permitir la configuración del servicio de envío de correo electrónico de notificaciones cuando se detectan archivos maliciosos y reportes automáticos frecuentes.
- La solución local es instalar los paquetes de actualización de los módulos de seguridad tan pronto como estén disponibles.
- Deben soportar el análisis de los archivos maliciosos en un ambiente controlado con al menos los sistemas operativos Windows 10, Windows 8.1, Windows 7, Linux y/o Android.
- La solución local debe ser compatible con la compra, descarga e instalación de máquinas virtuales adicionales.
- El sistema de análisis debe trabajar en forma que permita que el firewall envíe archivos para su análisis de forma automática.
- Permitir a los usuarios introducir una lista de contraseñas predeterminada para los archivos para analizar bajo demanda
- Permite subir archivos y/o URLs manualmente para su inspección conductual, implica hasta 5 archivos y/o URLs al mes.
- Deberá permitir la interacción con las máquinas virtuales mientras se realiza el análisis bajo demanda.
- Todo análisis y bloqueo de malware y/o código malicioso debe ocurrir en tiempo real y el bloqueo debe ser inmediato, no se aceptarán soluciones que solo detecten malware y/o código malicioso.

3. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL

3.1. SOPORTE TÉCNICO

- El proveedor deberá ofrecer un centro de Atención (NOC/SOC) para gestionar cualquier avería o incidencia sobre los servicios y equipos ofertados por el proveedor con operación de 24x7x365 días del año. Los medios de comunicación que deben de habilitarse son: vía telefónica (Call Center llamada gratuita) y/o correo electrónico.
 - El tiempo de recepción de la avería o incidentes del servicio, así como a consultas y asesorías técnicas deberán ser no mayor a cuarenta y cinco (45) minutos, considerado desde que se recibe la llamada por parte de la entidad hasta la generación del ticket. En caso de resolución se debe considerar para la solución de avería remota 06 horas y de 08 horas para averías que no puedan resolverse de forma remota.
- El tiempo máximo de solución ante averías o incidentes por enlace desde la notificación, deberá ser según el siguiente cuadro.

N°	DESCRIPCIÓN	TIEMPO MÁXIMO DE SOLUCIÓN
1	Solución de avería de forma remota	06 horas
2	Solución de averías que no puedan resolverse de forma remota.	08 horas
3	Avería causada por rotura del medio físico o causado por terceros.	12 horas

- Los tiempos definidos hacen referencia específicamente a los enlaces de internet y a la interconexión de sedes.
- Todo equipo reemplazado deberá ser por otro equipo igual o de mayor capacidad que lo ofertado (aplica para el equipamiento de enlace de red y datos).

Pág. 21





- Para el cambio de equipamiento, el plazo será no mayor a 72 horas, desde el reporte de la avería.
- Toda actividad o provisión de bienes que tenga que ejecutar el proveedor para subsanar una avería e incidente serán sin costo alguno para la entidad, debiendo realizar sin límites de intervenciones.
- El Centro de operaciones de seguridad (NOC/SOC) deberá remitir un reporte de seguridad cada vez que se presente una incidencia de seguridad de ataques encontrado en la red, esto hace referencia únicamente al tráfico que pasa por el firewall. El reporte será emitido a inicios del siguiente mes.
- Para el servicio de internet y datos, el proveedor deberá proveer al jefe de la OTI de la entidad una cuenta de usuario y contraseña para acceder a un servidor web para la verificación del consumo del ancho de banda de los circuitos de datos que permita:
 - o Visualizar las estadísticas gráficas del tráfico entrante y saliente de cada enlace.
 - o Visualizar los registros de pérdidas de conexión de manera diaria, semanal, mensual y anual.
 - o Monitorear el estado de las líneas de comunicación y otras que permitan tomar conocimiento del evento.
- Para la imputación de responsabilidades por la existencia de averías en el servicio (corte, caída o degradación del servicio), se evaluará previamente si estas deberán recaer sobre el contratista o sobre la Entidad, siendo que, de comprobarse que la referida contingencia fue originada por la entidad o por un hecho ajeno a las partes (caso fortuito o fuerza mayor), no se generará ningún tipo de penalidad en contra del contratista.

3.2. CAPACITACIÓN



- Se requiere traslado de conocimientos para administración y gestión de los equipos de seguridad perimetral ofertados por el proveedor.
- Adicionalmente, se requiere capacitaciones para un mínimo de (15) personas de la OTI de la UNA Puno, las capacitaciones se coordinarán exclusivamente durante la etapa de implementación así mismo se debe incluir el sílabo de la capacitación a dictarse.
- Las capacitaciones deberán ser en lo siguiente: Entrenamiento Oficial en Networking, entrenamiento Oficial en ITIL y entrenamiento Oficial en Gestión de Proyectos PMP.
- Las capacitaciones podrán ser de forma remota o presencial y con previa coordinación con la oficina de OTI.
- Se deberá otorgar las correspondientes constancias de participación a los asistentes, las cuales serán emitidas por la entidad encargada de dictar los cursos de capacitación.
- El proveedor deberá asumir el costo de la capacitación otorgada.
- Las capacitaciones deberán tener una duración mínima de 40 horas.

4. RECURSOS A SER PROVISTOS POR EL PROVEEDOR

- Todos los equipos, elementos y/o accesorios necesarios serán provistos por el proveedor e instalados en la UNA-PUNO, utilizados en la infraestructura de comunicaciones y provistos por el proveedor, serán de tecnología vigente, de última generación. Deberán ser nuevos y de primer uso. Esta condición deberá ser acreditada en la solución ofertada del proveedor, con carta del fabricante o distribuidor autorizado del país o dueño de la marca de los equipos (equipamiento instalado en la universidad), el cual será presentado pata la etapa del inicio del servicio.

5. RECURSOS A SER PROVISTOS POR LA ENTIDAD

- La Entidad proporcionará espacio físico en los gabinetes de comunicaciones de las distintas

sedes en donde se instalarán los equipos que forman parte de los servicios, así como energía estabilizada UPS, pozo a tierra y puntos de toma eléctrica.

- La Entidad brindará la seguridad necesaria para los equipos que se instalen en los gabinetes de la entidad a fin de que estos no sean manipulados por personas ajenas al proveedor o personal de la OTI.
- Facilitará el acceso a la infraestructura de la universidad para que realice las instalaciones que correspondan para una correcta y eficaz prestación del servicio.

INSPECCIÓN Y PRUEBAS



- Una vez culminada la implementación de los servicios, el proveedor y el jefe de la Sub Unidad de Redes y Comunicaciones de la OTI en forma conjunta, realizarán los procedimientos de inspección y pruebas sobre la infraestructura y equipos instalados.
- Las pruebas se realizarán en los lugares de instalación e implementación de los servicios.

GARANTÍA

La garantía por los trabajos realizados, así como la garantía técnica por parte de la marca de los equipos que forman parte de los servicios deberá ser por el periodo de la ejecución contractual.

VISITA TÉCNICA

Se podrá realizar al menos (01) visita técnica a las sedes donde es requisito instalar los servicios solicitados, la cual tiene por finalidad que el postor realice el levantamiento de la información necesaria para el dimensionamiento de la solución a implementarse.

6. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

6.1. LUGAR

El lugar de la prestación del servicio será en la Oficina de Tecnologías de Información (OTI):

- Sitio 1: Av. Floral N° 1153 – Puno - Ciudad Universitaria Coordinadas: -15.823634, -70.016937
- Sitio 2: Av. El Sol N° 329 – Puno Educación Continua. Coordinadas: -15°83'41.01"S, -70°02'36.29"W
- Sitio 3: Edificio Facultad de Ciencias Jurídicas y Políticas - Esquina Jr. Grau con Jr. Conde de Lemos – Puno
- Sitio 4: Edificio Centro de Idiomas - Jr. Lima N° 272 – Puno
- Sitio 5: Edificio CEPREUNA e Instituto de Informática INFOUNA - Jr. Acora N° 235
- Sitio 6: centro experimental Chucuito
- Sitio 7: centro experimental Chuquibambilla

6.2. PLAZO DE PRESTACIÓN DEL SERVICIO

La prestación del servicio será por un periodo de 1100 días calendarios, contados a partir del día siguiente de la firma del acta de la habilitación y puesta en funcionamiento del servicio de internet (inicio del servicio).

6.3. PLAZO DE IMPLEMENTACIÓN DEL SERVICIO

La implementación se realizará máximo en noventa (90) días calendarios siguientes al perfeccionamiento del contrato, el plazo de instalación comenzará a computarse desde que la entidad

Pág. 23

cumpla con las condiciones necesarias para la ejecución del servicio (disponibilidad de locales y ambientes, suministro adecuado de energía, entrega de información, etc.) y permisos correspondientes.

7. PERSONAL CLAVE

Dado la importancia de que nuestra entidad cuente con una comunicación directa y fluida durante toda la etapa de implementación y ejecución del servicio, con el postor ganador de la buena Pro, el postor deberá presentar personal de planilla del postor.



JEFE DE PROYECTO

- Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica y/o Empresarial y de Sistemas. Colegiatura vigente y habilitado
- Capacitación de mínimo 120 horas en gestión de proyectos y certificado de PMP vigente (Project Management Profesional)
- Capacitación de mínimo 25 horas en ITIL v4 y certificado ITIL v4
- Capacitación de mínimo 40 horas en SCRUM
- Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.



GESTOR DE PROYECTO

- Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica y/o Empresarial y de Sistemas y/o redes y comunicaciones y/o computación y sistemas. Colegiatura vigente y habilitado.
- Capacitación de mínimo 32 horas en gestión de proyectos y certificado PMP vigente.
- Capacitación de mínimo 40 horas en SCRUM
- Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

ESPECIALISTA DE REDES

- Bachiller y/o título universitario en electrónica y/o telecomunicaciones y/o sistemas y/o informática y/o computación y/o electrónica y/o Industrial y/o redes y/o comunicación y/ de datos y/o Empresarial y de Sistemas.
- Certificado del equipo router y/o CPE ofertado vigente
- Capacitación de mínimo 50 horas en redes
- Experiencia mínima de 05 años en implementación de proyectos de redes

ESPECIALISTA DE SEGURIDAD

- Técnico y/o bachiller y/o título universitario en electrónica y/o telecomunicaciones y/o sistemas y/o informática y/o computación y/o electrónica y/o Industrial y/o redes y/o comunicación y/ de datos y/o Empresarial y de Sistemas.
- Certificado del equipo y/o solución de seguridad ofertado vigente
- Capacitación de mínimo 50 horas en seguridad.
- Experiencia mínima de 03 años en implementación de proyectos de seguridad.



8. ENTREGABLES

Planeamiento del proyecto

- El proveedor deberá hacer entrega del plan de trabajo, hasta los diez (10) días hábiles siguientes de la suscripción del contrato, el cual deberá detallar lo siguiente:
 - Cronograma Gantt indicando las actividades a desarrollar.
 - Listado del personal propuesto por el proveedor para la realización de la prestación. Se deberá señalar por cada persona, el cargo, nombres completos, N° DNI, correo electrónico, así como Nros de celulares y adjuntar los currículos vitae documentado.
 - Listado del equipamiento, software y materiales que forman parte de su propuesta técnica.
 - Protocolos de pruebas, reportes de las pruebas realizadas.
 - Plan de capacitación detallado.
 - Credenciales de acceso a las plataformas de reportería y verificación del consumo del ancho de banda.
 - Las credenciales de acceso serán solo de lectura de los equipamientos físicos y en la nube.

Puesta en operación del servicio

Suscrita el acta de inicio de servicio, el proveedor contará con un plazo no mayor a cuatro (4) días hábiles siguientes, para la entrega a la OTI del informe final que deberá ser foliada y firmada en su totalidad por el jefe de proyecto. Este documento deberá incluir lo siguiente:

- Diagrama de la arquitectura y topología de la solución implementada (interconexión, redes, protocolos), excluyendo la conexión interna en el lugar de prestación, interconexión de última milla de la UNA-PUNO a los nodos del proveedor), así como su interconexión con los backbone internacionales y su conexión al NAP.
- Plano de recorrido de la fibra óptica instalada en las sedes UNA-PUNO identificándose los empalmes.
- Configuraciones implementadas como buenas prácticas de seguridad en los equipos que forman parte de los servicios (Envío de configuraciones de los equipos de seguridad y los CPE).
- Lista de Pool de IPs.
- Las credenciales para el acceso de lectura de los equipos físicos instalados en la entidad y en la nube del proveedor; soluciones y herramientas que forman parte de los servicios.
- Backups de la configuración de los routers, equipos, soluciones y herramientas que formen parte de los servicios e instalados en la entidad.
- Procedimientos de atención de incidencias y averías y niveles de escalamiento. Se deberá indicar los números telefónicos gratuitos (call center) para la recepción de la atención así mismo la dirección de correo electrónico.



- Copias acta de inicio de servicio
- Copias de las constancias de participación

Para la ejecución contractual de los servicios

- El proveedor presentará hasta los diez (10) días hábiles posteriores a cada periodo mensual de facturación, un informe de estado del servicio de internet y VPN y un informe del servicio de seguridad perimetral actualizada al periodo mensual:
 - Informe del estado del servicio Internet y VPN: contendrá como mínimo reporte del tráfico de salida y entrada, consumo de ancho de banda promedio, estadísticas del consumo de ancho de banda en el mes, reporte de estado y disponibilidad de los enlaces de internet y VPN. Este informe podrá ser reemplazado por el informe arrojado por la plataforma web.
 - Informe de seguridad de los servicios: contendrá como mínimo estadística de incidentes de seguridad, top de ataques, principales fuentes y destinos, log de eventos, recomendaciones y sugerencias de mejora en la seguridad informática.
 - Toda documentación entregable deberá ser en formato digital o puede ser impresa formato A4. Dirigido a la dirección de la OTI (Av. Floral N° 1153 – Puno Ciudad Universitaria) o al correo electrónico oti@unap.edu.pe.
 - Los entregables son requisitos para emitir la conformidad de la prestación.



9. CONFORMIDAD DE LA PRESTACIÓN

- Conformidad de la implementación: Sera dado por el jefe de la OTI, previo informe técnico del jefe de la Sub Unidad de Redes y Comunicaciones de la UNA Puno. La cual será validada con los entregables y se realizará un Acta de Conformidad luego de la inspección de la totalidad de la implementación.
- Conformidad de la prestación del servicio: Se remitirá mensualmente mediante informe del jefe de la Sub Unidad de Redes y Comunicaciones de la UNA Puno, durante el periodo de la prestación emitiendo su conformidad respecto a la prestación efectuada, para lo cual se deberá tomar en consideración los reportes mensuales que entregará el proveedor. Asimismo, con el fin de transparentar las actuaciones, se remitirá al contratista la conformidad mensual del servicio.

[Handwritten signature]



10. FORMA DE PAGO

El pago de los servicios se realizará de forma mensual y en partes iguales. Luego de finalizado el mes de los servicios prestados y otorgada la conformidad por parte de la OTI, previa entrega del Informe de Estado de los Servicios, informe de seguridad de los servicios correspondiente al mes, conformidad del servicio y comprobante de Pago (Factura y/o recibo detallado) por parte del proveedor.

11. CONFIDENCIALIDAD

El proveedor se compromete a mantener reserva absoluta y queda prohibida revelar a terceros sobre la información institucional a la que tenga acceso y/o información confidencial consistente en la totalidad de la tecnología, información, datos, especificaciones, sistemas de cómputo, métodos, procesos en general y todos los aspectos relacionados con el funcionamiento de la UNA-PUNO, toda la información a la que tenga acceso y que se encuentren relacionados con la prestación son de propiedad de la UNA-PUNO y en tal virtud, la divulgación, comunicación, transmisión o utilización para beneficio de cualquier persona distinta a la UNA-PUNO será considerada ilegal.

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

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



12. RESPONSABILIDAD POR VICIOS OCULTOS

El proveedor es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por el plazo de un (01) año, después de otorgada la conformidad.

13. OTRAS PENALIDADES

N°	CONCEPTO DE APLICACIÓN DE LA PENALIDAD	FORMA DE CALCULO	PROCEDIMIENTO
1	<p>Identificación de la penalidad por corte de servicio sin atención inmediata establecida en el tiempo indicado: La infracción puede ser clasificada como leve, grave o muy grave, según su naturaleza y el impacto que cause. OSIPTEL establece escalas de penalidad para cada tipo de infracción.</p> <ul style="list-style-type: none"> Infracciones leves: Corte de servicio por causas menores, sin impacto significativo. De 6 a 8 horas. Infracciones graves: Cortes prolongados sin atención adecuada o falta de mantenimiento preventivo. De 8 a 12 horas. Infracciones muy graves: Interrupciones de servicio a gran escala, reincidencias frecuentes o daños graves a los usuarios. De 12 a más horas. 	<p>Fórmula general para el cálculo de la penalidad:</p> <p>Penalidad = (0.5% del valor de la UIT) x (Número de días de retraso)</p> <p>El valor de la UIT será según el año que corresponda</p>	Mediante informe del área usuaria



- Ante la identificación de penalidades, se informará al contratista el detalle de las mismas y se le otorgará cinco (5) días hábiles para que presente sus descargos.

14. CONSIDERACIONES PARA LA PRESENTACIÓN DE PROPUESTAS

Las propuestas deberán ser presentadas de forma detallada obligatoriamente por cada equipo

Pág. 27

indicando cantidades aproximadas, marca, modelo, número de parte y adjuntando hojas de información técnica, que deberán ser sustentadas con la presentación contenida en folletos, instructivos o catálogos oficiales propios de la marca.

15. REQUISITOS DE CALIFICACIÓN

Los requisitos de calificación se encuentran en el Anexo N° 1 de los presentes términos de referencia. Deberán ser cumplidos de forma obligatoria.



ANEXO N° 1: REQUISITOS DE CALIFICACIÓN

1. REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
	HABILITACIÓN
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none">• El postor debe estar debidamente registrado y habilitado ante las entidades y en conformidad con lo establecido con la Ley General de Telecomunicaciones, como empresa proveedora de Telecomunicaciones. <p><u>Acreditación:</u> Presentar copia simple de la Resolución del Ministerio de Transportes y Comunicaciones, que lo acredite como operador de Telecomunicaciones y/o el certificado de valor añadido emitido por el MTC y/o el contrato de concesión del servicio público de telecomunicaciones.</p> <p><u>Requisitos:</u></p> <ul style="list-style-type: none">• El postor debe acreditar pertenecer al NAP PERÚ como socio de esta Asociación (Opcional) <p><u>Acreditación:</u></p> <ul style="list-style-type: none">• Certificado de incorporación al NAP PERÚ y/o declaración jurada de pertenecer al NAP PERÚ (Opcional).

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	CALIFICACIONES DEL PERSONAL CLAVE
B.1.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>JEFE DE PROYECTO Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica y/o Empresarial y de Sistemas. Colegiatura vigente y habilitado</p> <p>GESTOR DE PROYECTO Título universitario en ingeniería electrónica y/o ingeniería de telecomunicaciones y/o ingeniería de sistemas y/o Ingeniería electrónica y/o Empresarial y de Sistemas. Colegiatura vigente y habilitado.</p> <p>ESPECIALISTA DE REDES Bachiller y/o título universitario en electrónica y/o telecomunicaciones y/o sistemas y/o informática y/o computación y/o electrónica y/o Industrial y/o redes y/o comunicación y/ de datos y/o Empresarial y de Sistemas.</p> <p>ESPECIALISTA DE SEGURIDAD Técnico y/o bachiller y/o título universitario en electrónica y/o telecomunicaciones y/o</p>

	<p>sistemas y/o informática y/o computación y/o electrónica y/o Industrial y/o redes y/o comunicación y/ de datos y/o Empresarial y de Sistemas.</p> <p><u>Acreditación:</u> El TÍTULO PROFESIONAL será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : http://www.titulosinstitutos.pe/, según corresponda.</p> <p>Importante para la Entidad</p> <p><i>El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.</i></p> <p>En caso TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
	<p>B.1.2 CAPACITACIÓN DEL PERSONAL CLAVE</p> <p><u>Requisitos:</u></p> <p>JEFE DE PROYECTO</p> <ul style="list-style-type: none"> • Capacitación de mínimo 120 horas en gestión de proyectos y certificado de PMP vigente (Project Management Profesional) • Capacitación de mínimo 25 horas en ITIL v4 y certificado ITIL v4 • Capacitación de mínimo 40 horas en SCRUM <p>GESTOR DE PROYECTO</p> <ul style="list-style-type: none"> • Capacitación de mínimo 25 horas en ITIL v4 y certificado ITIL v4 • Capacitación de mínimo 32 horas en gestión de proyectos y certificado PMP vigente. • Capacitación de mínimo 40 horas en SCRUM <p>ESPECIALISTA DE REDES</p> <ul style="list-style-type: none"> • Certificado del equipo router y/o CPE ofertado vigente • Capacitación de mínimo 50 horas en redes <p>ESPECIALISTA DE SEGURIDAD</p> <ul style="list-style-type: none"> • Certificado del equipo y/o solución de seguridad ofertado vigente • Capacitación de mínimo 50 horas en seguridad. <p><u>Acreditación:</u> Se acreditará con copia simple de constancias, certificados o diplomas.</p>

B.1.3 EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

JEFE DE PROYECTO

- Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

GESTOR DE PROYECTO

- Experiencia mínima de 05 años en Gestión de proyectos y/o servicios de telecomunicaciones tales como internet y/o transmisión/ comunicación/ enlace/ interconexión de datos y/o telefonía y/o seguridad.

ESPECIALISTA DE REDES

- Experiencia mínima de 05 años en implementación de proyectos de redes

ESPECIALISTA DE SEGURIDAD

- Experiencia mínima de 03 años en implementación de proyectos de seguridad.




Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.



B2	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
  	<p>Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/ 3'000,000.00 (Tres Millones 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, 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. Se consideran servicios similares a los siguientes: Servicio de internet; y/o servicio de interconexión y/o Servicio de enlaces de comunicación y/o Servicio de internet y Enlace dedicado y/o Servicio de telefonía digital y servicio de línea dedicada de acceso a internet.</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 fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad. <u>En</u> el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p>



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

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

Importante

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



Ing. Nelson Nicolás Tapia Frisancho
Jefe Sub Unidad de Redes y Comunicaciones
Oficina de Tecnologías de Información - UNAP

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

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

Importante

En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*
- *El cumplimiento de los Términos de Referencia se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de estos. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*
- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<p><u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>	<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>i</i> = Oferta <i>P_i</i> = Puntaje de la oferta a evaluar <i>O_i</i> = Precio <i>i</i> <i>O_m</i> = Precio de la oferta más baja <i>PMP</i> = Puntaje máximo del precio </p> <p style="text-align: right;">85 puntos</p>

B. MEJORAS A LOS TÉRMINOS DE REFERENCIA	
<p>MEJORA 01 Evaluación: Por seguridad de la información, al menos (01) servidor DNS, deberá estar alojado en el Data center propio del postor, certificado vigente en la norma ANSI/TIA RATED-3 de Diseño y/o Construcción y/u operación.</p> <p>Acreditación: El postor deberá presentar en su propuesta el/los certificados vigentes de ANSI/TIA de Diseño y/o Construcción y/o operación a nombre del postor. En caso que el postor se presente en consorcio, cada uno de sus integrantes, debe acreditar que cuenta con la certificación para obtener el puntaje.</p>	<p>(Máximo 10 puntos)</p> <p>Mejora 01: 06 puntos</p> <p>No presenta mejora 0 Puntos</p>
<p>MEJORA 02 Evaluación: El postor debe garantizar la adecuada protección de la información, gestionar los riesgos de seguridad y cumplir con estándares internacionales en la gestión de la seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos. Para ello el postor deberá contar con su certificación vigente del ISO/IEC 27001:2022, el cual incluirá como mínimo, los procesos de Provisión, Instalación, Soporte, Monitoreo, Mantenimiento y Gestión, relacionados a los Servicios Cloud, Acceso Dedicado a Internet, Fibra oscura, Centro de Datos, Interconexión de Sedes y Servicios de Seguridad para clientes.</p>	<p>Mejora 02: 04 puntos</p> <p>No presenta mejora 0 Puntos</p>

<p>Acreditación: El postor deberá presentar su certificado vigente incluyendo sus características. En caso de consorcio, cada miembro deberá presentar su propia certificación.</p> <div data-bbox="293 376 1083 1008"> <p>Importante</p> <p>De conformidad con la Opinión N° 144-2016-OSCE/DTN, constituye una mejora, todo aquello que agregue un valor adicional al parámetro mínimo establecido en las especificaciones técnicas o términos de referencia, según corresponda, mejorando su calidad o las condiciones de su entrega o prestación, sin generar un costo adicional a la Entidad.</p> <p>En este factor se pueden incluir aspectos referidos a la sostenibilidad ambiental o social, tales como el compromiso de que durante la ejecución del contrato se verifiquen condiciones de igualdad de género o de inclusión laboral de personas con discapacidad; el uso de equipos energéticamente eficientes o con bajo nivel de ruido, radiaciones, vibraciones, emisiones, etcétera; la implementación de medidas de ecoeficiencia; el uso de insumos que tengan sustancias con menor impacto ambiental; la utilización de productos forestales de fuentes certificadas, orgánicos o reciclados, el manejo adecuado de residuos sólidos, entre otros.</p> </div>	
C. SISTEMA DE GESTIÓN DE LA CALIDAD	
<p><u>Evaluación:</u> -El postor debe garantizar el cumplimiento de estándares internacionales de calidad, implementar procesos eficientes, asegurar la adecuada prestación del servicio y comprometerse con la mejora continua, minimizando riesgos en el servicio solicitado. Para ello el postor deberá contar con su certificación vigente del ISO 9001:2015, el cual incluirá como mínimo, el planeamiento de soluciones tecnológicas sobre fibra óptica, radio enlaces, monitoreo, soporte, mantenimiento del servicio y atención al cliente.</p> <p><u>Acreditación:</u> El postor deberá presentar su certificado vigente incluyendo sus características. En caso de consorcio, cada miembro deberá presentar su propia certificación.</p>	<p>(Máximo 5 puntos)</p> <p>Presenta ISO 9001:2015: 05 puntos No presenta ISO 9001:2015 0 Puntos</p>
PUNTAJE TOTAL	100 puntos¹⁰

Importante

Los factores de evaluación elaborados por el órgano encargado de las contrataciones o el comité de selección, según corresponda, son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de las Especificaciones Técnicas ni los requisitos de calificación.

¹⁰ Es la suma de los puntajes de todos los factores de evaluación.

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 del servicio de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], 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 del **CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]** 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 [CONSIGNAR EL OBJETO DE LA CONTRATACIÓN].

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

CLÁUSULA CUARTA: DEL PAGO¹¹

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR SI SE TRATA DE PAGO ÚNICO, PAGOS PARCIALES O PAGOS PERIÓDICOS], 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 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 de las contraprestaciones pactadas a favor del CONTRATISTA dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo

¹¹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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 ÚLTIMO CASO].

Importante para la Entidad

De preverse en los Términos de Referencia la ejecución de actividades de instalación, implementación u otros que deban realizarse de manera previa al inicio del plazo de ejecución, se debe consignar lo siguiente:

“El plazo para la [CONSIGNAR LAS ACTIVIDADES PREVIAS PREVISTAS EN LOS TÉRMINOS DE REFERENCIA] es de [.....], el mismo que se computa desde [INDICAR CONDICIÓN CON LA QUE DICHAS ACTIVIDADES SE INICIAN].”

Incorporar a las bases o eliminar, según corresponda.

Importante para la Entidad

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

CLÁUSULA ...: PRESTACIONES ACCESORIAS¹²

“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 ÚLTIMO 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:

¹² 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) accesoria(s), 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.

- De fiel cumplimiento del contrato: [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]. 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.

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

“De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo.”

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

Al amparo de lo dispuesto en el numeral 151.2 del artículo 151 del Reglamento de la Ley de Contrataciones del Estado, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato de la prestación accesorias como garantía de fiel cumplimiento de prestaciones accesorias, debe consignarse lo siguiente:

- “De fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo.”*

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 por 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: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. 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 servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD no otorga la conformidad, 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 conformidad del servicio 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 CONTROVERSIAS¹³

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.

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 Digitales¹⁴.

¹³ 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).

¹⁴ 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

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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) :			
MYPE ¹⁵		Sí		No	
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 servicios¹⁶

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.

¹⁵ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el postor ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento.

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 servicios.

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

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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) :			
MYPE ¹⁷		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁸		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁹		Sí	No	
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.

¹⁷ En los contratos periódicos de prestación de servicios, esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en consideración, en caso el consorcio ganador de la buena pro solicite la retención del diez por ciento (10%) del monto del contrato, en calidad de garantía de fiel cumplimiento, según lo señalado en el numeral 149.4 del artículo 149 y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹⁸ Ibídem.

¹⁹ Ibídem.

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 servicios²⁰

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 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.

²⁰ 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 servicios.

ANEXO N° 2

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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 LOS TÉRMINOS DE REFERENCIA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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 servicio de [CONSIGNAR OBJETO DE LA CONVOCATORIA], de conformidad con los Términos de Referencia 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 los términos de referencia, conforme a lo indicado en el acápite relacionado al contenido de las ofertas de la presente sección de las bases.

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a prestar el servicio objeto del presente procedimiento de selección en el plazo [CONSIGNAR EL PLAZO OFERTADO]

[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

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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 al **CONCURSO PÚBLICO 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] [%]²¹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²²

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%²³

[CONSIGNAR CIUDAD Y FECHA]

²¹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²² Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²³ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

.....
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.

Importante para la Entidad

En caso de la prestación de servicios bajo el sistema a suma alzada incluir el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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
PRESTACION PRINCIPAL, servicio objeto de la contratación	
PRESTACIONES ACCESORIAS	
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 servicio 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

Importante para la Entidad

Si durante la fase de actos preparatorios, las Entidades advierten que es posible la participación de proveedores que gozan del beneficio de la exoneración del IGV prevista en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, incluir el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases

ANEXO N° 7

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley N° 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

- 1.- Que el domicilio fiscal de la empresa²⁴ se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);
- 2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);
- 3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y
- 4.- Que la empresa no presta servicios fuera de la Amazonía.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

²⁴ En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquellas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁶	EXPERIENCIA PROVENIENTE ²⁷ DE:	MONEDA	IMPORTE ²⁸	TIPO DE CAMBIO VENTA ²⁹	MONTO FACTURADO ACUMULADO ³⁰
1										
2										
3										
4										

²⁵ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicios o de cancelación del comprobante de pago, según corresponda.

²⁶ 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.

²⁷ 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”*.

²⁸ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁹ 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 Servicios o de cancelación del comprobante de pago, según corresponda.

³⁰ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁵	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁶	EXPERIENCIA PROVENIENTE ²⁷ DE:	MONEDA	IMPORTE ²⁸	TIPO DE CAMBIO VENTA ²⁹	MONTO FACTURADO ACUMULADO ³⁰
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

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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/mp/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.

Importante para la Entidad

En el caso de procedimientos por relación de ítems cuando la contratación del servicio va a ser prestado fuera de la provincia de Lima y Callao y el monto del valor estimado de algún ítem no supere los doscientos mil Soles (S/ 200,000.00) debe considerarse el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases.

ANEXO N° 10

**SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO
(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ÍTEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)])**

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que el domicilio de mi representada se encuentra ubicado en la provincia o provincia colindante donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *Para asignar la bonificación, el comité de selección, verifica el domicilio consignado por el postor en el Registro Nacional de Proveedores (RNP).*
- *Para que el postor pueda acceder a la bonificación, debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.*

Importante

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

ANEXO N° 10

**SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO
(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ÍTEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)])**

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

Mediante el presente el que se suscribe, [...], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que los domicilios de todos los integrantes del consorcio se encuentran ubicados en la provincia o provincias colindantes donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *Para asignar la bonificación, el comité de selección, verifica el domicilio consignado de los integrantes del consorcio, en el Registro Nacional de Proveedores (RNP).*
- *Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.*

Nota para la Entidad

En el caso de procedimientos por relación de ítems cuando el monto del valor estimado de algún ítem corresponda a una Adjudicación Simplificada, se incluye el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases

ANEXO N° 11

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

Señores

COMITÉ DE SELECCIÓN

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 12

**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

CONCURSO PÚBLICO N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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.