

BASES INTEGRADAS DE ADJUDICACIÓN SIMPLIFICADA 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>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda 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 sombreado.
- 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 marzo, junio y diciembre de 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

BASES INTEGRADAS DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

PRIMERA CONVOCATORIA

CONTRATACIÓN DE SERVICIO DE "SERVICIO ANUAL DE INTERNET"

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, así como el literal a) del artículo 89 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada. 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 el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 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. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 y en el artículo 90 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 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.*

1.7. 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.

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>

En la apertura electrónica de la oferta, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

1.8. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el numeral 74.1 y el literal a) del numeral 74.2 del artículo 74 del Reglamento.

En el supuesto de que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se efectúa siguiendo estrictamente el orden establecido en el numeral 91.1 del artículo 91 del Reglamento.

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

Importante

En el caso de contratación de servicios en general que se presten fuera de la provincia de Lima y Callao, cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00), a solicitud del postor se asigna una bonificación equivalente al diez por ciento (10%) sobre el puntaje total obtenido por los postores con domicilio en la provincia donde prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región. El domicilio es el consignado en la constancia de inscripción ante el RNP². Lo mismo aplica en el caso de procedimientos de selección por relación de ítems, cuando algún ítem no supera el monto señalado anteriormente.

1.9. 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.

1.10. 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.

1.11. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

² La constancia de inscripción electrónica se visualizará en el portal web del Registro Nacional de Proveedores: www.rnp.gob.pe

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

1.12. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

1.13. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) 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 la Entidad convocante, y es conocido y resuelto por su Titular, cuando el valor estimado sea igual o menor a cincuenta (50) UIT. Cuando el valor estimado sea mayor a dicho monto, el recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

En los procedimientos de selección según relación de ítems, el valor estimado total del procedimiento determina ante quién se presenta el recurso de apelación.

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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda.

- *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, o en la Unidad de Trámite Documentario de la Entidad, según corresponda.*

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 cinco (5) 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 cinco (5) 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.

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), en los que se puede perfeccionar con la recepción de la orden de servicios, conforme a lo previsto en la sección específica de las bases.

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 valor estimado del ítem corresponda al parámetro establecido en el párrafo anterior.

Importante

El órgano encargado de las contrataciones o el comité de selección, según corresponda, debe consignar en la sección específica de las bases la forma en que se perfeccionará el contrato, sea con la suscripción del contrato o la recepción de la orden de servicios. En caso la Entidad perfeccione el contrato con la recepción de la orden de servicios no debe incluir la proforma del contrato establecida en el Capítulo V de la sección específica de las bases.

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 accesoria, la misma que debe ser renovada periódicamente hasta el cumplimiento total de las obligaciones garantizadas.

Importante

- *En los contratos cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no superen el monto señalado anteriormente, 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 el 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-emitir-cartas-fianza>).

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los 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 : INSTITUTO NACIONAL MATERNO PERINATAL
RUC N° : 20144329148
Domicilio legal : JR. SANTA ROSA 941 LIMA - LIMA - LIMA
Teléfono: : (01) 3281012
Correo electrónico: : cacosta@iemp.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio ANUAL DE INTERNET

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante MEMORANDO N°1544-2024-OEA-INMP el 04 de setiembre

1.4. FUENTE DE FINANCIAMIENTO

RO-RECURSOS ORDINARIOS

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE

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

Los servicios materia de la presente convocatoria se prestarán en el plazo máximo de hasta sesenta (60) días calendarios para la instalación, implementación y prueba de funcionamiento y el servicio de enlace de internet será por un periodo de doce (12) meses el cual se computará desde la culminación de la instalación, implementación y prueba de funcionamiento del servicio previa suscripción de un acta de Conformidad de Instalación, implementación y prueba de

funcionamiento del servicio previa suscripción de un Acta de inicio de contrato de (01) un año en concordancia con lo establecido en el expediente de contratación. Dicho plazo constituye un Requerimiento técnico mínimo que debe coincidir con lo establecido en el expediente de contratación.

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 el importe de S/. 5.00 (Cinco con 00/100 Soles) en Caja de la Entidad (Consultorios Externos) sitio en Jr. Santa Rosa N°941 – Cercado de Lima y recogerlo en la Oficina de Logística 2do Piso en Jr. Santa Rosa N°941 – Cercado de Lima.

1.10. BASE LEGAL

- Ley N.º 31953 Ley de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N.º 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Decreto Legislativo N.º 1440, Decreto Legislativo del Sistema Nacional de Presupuesto Público
- Decreto Supremo N°082-2019-EF que Aprueba el TUO de la Ley N°30225 – Ley de Contrataciones del Estado y sus modificatorias.
- Decreto Supremo N°344-2018-EF que Aprueba el Reglamento de la Ley N°30225 Ley de Contrataciones del Estado, y sus modificatorias.
- Ley N.º 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Decreto Supremo N°004-2019-JUS que aprueba el TUO de la Ley N°27444 – Ley de Procedimiento Administrativo General.
- Directivas y Opiniones del OSCE.
- Código Civil.
- Memorando N.º 1197-2024-OEPE/INMP de fecha 25.07.2024 (Disponibilidad Presupuestal).
- Resolución Directoral N.º 231-2024-DG/INMP-MINSA de fecha 27 de agosto del 2024 (Inclusión al Plan Anual de Contrataciones).
- Memorando N.º 1544-2024-OEA-INMP Aprobación de Expediente.
- Resolución Ejecutiva de Administración N.º 135-OEA-INMP-2024 de fecha 06 de setiembre del 2024 (Conformación de Comité de Selección)
- 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 documentos³, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

- a) Declaración jurada de datos del postor. (**Anexo N° 1**)
- b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁴ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

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

³ La omisión del índice no determina la no admisión de la oferta.

⁴ 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) Deberán presentar documentación técnica sustentando con copia simple u original de catalogo o brochure o folleto de la tecnología a utilizar, los equipos y accesorios, así como también el diagrama respectivo de la solución.

- e) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**⁵
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- g) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6**.

El precio total de la oferta y los subtotales que lo componen son expresados con dos (2) decimales.

Importante

- *El órgano encargado de las contrataciones o el comité de selección, según corresponda, 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:

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁶.
- b) Solicitud de bonificación por tener la condición de micro y pequeña empresa. **(Anexo N° 11)**

⁵ 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.

⁶ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

2.3. PRESENTACIÓN DEL RECURSO DE APELACIÓN

"El recurso de apelación se presenta ante la Unidad de Trámite Documentario de la Entidad.

En caso el participante o postor opte por presentar recurso de apelación y por otorgar la garantía mediante depósito en cuenta bancaria, se debe realizar el abono en:

N ° de Cuenta : 00-068-368448
Banco : BANCO DE LA NACION
N° CCI⁷ : 018-068-000068368448-74

"

2.4. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- a) Garantía de fiel cumplimiento del contrato.
- b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
- c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.

Advertencia

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 – PIDE⁸ 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 comunicación⁹. (**Anexo N° 12**).
- i) Detalle de los precios unitarios del precio ofertado¹⁰.
- j) Estructura de costos¹¹.
- k) Deberá presentar la relación del personal jefe de Proyecto y Especialista en Ciberseguridad con su respectiva CV y documentación que acredite la experiencia.
- l) Presentar documentación pública del Fabricante adjuntando el link que lo respalde para comprobar el requerimiento de Throughput.

⁷ En caso de transferencia interbancaria.

⁸ 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/>

⁹ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

¹⁰ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

¹¹ Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

- m) Presentar Copia simple de documento de fabricante de la Soluciones de Seguridad Perimetral, Antispam y WAF.
- n) Se presentará carta de fabricante certificando los equipos de garantía de seguridad perimetral, Filtro de Mensajería (Antispam), solución de protección de aplicación web.
- o) Adjuntar carta de fabricante indicando que el Postor o empresa subcontratista deberá ser PARTNER del producto ofertado.

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- *En los contratos 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 y el 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 cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya¹².*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

¹² Según lo previsto en la Opinión N° 009-2016/DTN.

2.5. 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 La Oficina de Logística 2do piso; lugar Jr. Santa Rosa N° 941 Cercado de Lima.

2.6. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS PERIÓDICOS.

CRONOGRAMA DE PAGOS PERIODICOS											
1°	2°	3°	4°	5°	6°	7°	8°	9°	10°	11°	12°
8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.33 %	8.37 %

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

- Informe del funcionario responsable jefe de la Oficina de Estadística e Informática y el responsable jefe del Equipo Funcional de Informática emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Orden de Servicio
- Factura.

Dicha documentación se debe presentar en La Oficina de Logística 2do piso; lugar Jr. Santa Rosa N° 941 Cercado de Lima.

CAPÍTULO III REQUERIMIENTO

3.1. TERMINOS DE REFERENCIA

MINSA – INSTITUTO NACIONAL MATERNO PERINATAL

TERMINOS DE REFERENCIAS

NOMBRE Y CÓDIGO DEL SERVICIO SEGÚN CATALOGO SIGA – MEF

- **CODIGO SIGA – MEF** : 87050030019
- **NOMBRE SIGA – MEF** : SERVICIO DE INTERNET

1. Áreas Usuarias Solicitantes

Oficina de Estadística e Informática.

2. Finalidad Pública del Requerimiento

Contar con el servicio de internet por parte de usuarios del INMP como medio de comunicación institucional, para uso de servicios y sistemas de aplicación web del sector y del gobierno central y contar también con un servicio especializado de seguridad informática perimetral; para el cumplimiento de los objetivos institucionales.

3. Servicio Requerido

SERVICIO DE INTERNET IP – 500 Mbps

4. Objetivo de la Contratación

Proveer al Instituto Nacional Materno Perinatal de un Servicio de Internet IP – 500 Mbps

5. Plan Operativo Institucional 2024

El presente requerimiento esta vinculo al POI 2024 a través de Plan Operativo Informático 2024 - PLAN IMPLEMENTACION DE SERVICIOS INFORMATICOS.

Meta:

6. Características de la Necesidad del Servicio a Realizar:

CARACTERÍSTICAS GENERALES:

SERVICIO DE INTERNET IP

- Internet de 500Mbps
- El overbooking del enlace debe de ser de 1:1 local e internacional hasta la salida del operador.
- El enlace debe soportar la Implantación de servidores Web, Mail, DNS, etc.
- Asignación de 32 direcciones IP Publicas IPV4 como mínimo, estas incluyen las direcciones IP de la red, Gateway y broadcast.
- Enlace de Fibra Óptica 100 % dedicado.
- En caso de ser Enlace de Fibra Óptica (última milla) debe llegar hasta la sala de servidores del INMP.
- El acceso a Internet otorgado por el postor del servicio debe ser abierto y sin restricciones permitiendo al INMP otorgar información y/o servicios al alcance de cualquier usuario conectado a Internet.

- El enlace de Internet proporcionado a la entidad deberá tener conexión directa al NAP (Network Access Point).
- La disponibilidad requerida sobre el servicio debe ser del 99,95% mensual, para el enlace de acceso a Internet. Este parámetro está referido a averías imputables al postor. El tiempo de inoperatividad del servicio se calculará desde el reporte de la falla por parte del INMP hasta la verificación de la solución de la avería por parte del INMP.
- Para cumplir con el SLA de 99.95% se requiere que el postor presente un enlace de contingencia de Fibra óptica con diferente ruta de acceso y atendido de un nodo distinto que el enlace principal.
- El postor del servicio debe garantizar que el ancho de banda contratado sea el mismo desde la puerta de enlace en la oficina correspondiente del INMP hasta la salida Internacional, es decir no aplicará compresión alguna a este nivel.
- El postor deberá contar con 02 proveedores Internacionales TIER1 con una capacidad mínima de por lo menos 10 Gbps
- El postor del servicio debe garantizar la confidencialidad de la información desde la puerta de enlace en la oficina correspondiente del INMP hasta la salida Internacional.
- El Contratista deberá contar en su infraestructura de red con una plataforma de mitigación de ataques DDoS que cumpla las siguientes características:
 - Deberá estar desplegada como parte de la arquitectura de la red del Contratista y deberá proteger la salida a Internet del proveedor.
 - La plataforma deberá incluir la protección contra ataques de denegación de servicio a nivel de aplicación sin estados (stateless) por lo que no deberá tener límite de conexiones ni sesiones concurrentes para el tráfico total (incluyendo tráfico atacante).
 - El equipamiento deberá estar licenciado de tal manera que pueda mitigar como mínimo un throughput de 1 Gbps de ataque.
 - El equipamiento en la Red del Postor deberá ser de propósito específico, no se aceptarán soluciones basadas en funcionalidades adicionales de equipos como Firewalls, NGFW, UTM, Balanceadores, etc.
 - El fabricante de la solución ofertada deberá encontrarse en el Top 8 Distributed Denial of Service (DDoS) Protection Tools de PeerSpot 2022 o Líder en el Forrester Wave 2021 DDoS Mitigations Solutions.
- El servicio deberá incluir herramientas de monitoreo vía Web (previa autenticación), que le permita al personal del INMP, visualizar el consumo del tráfico entrante/saliente (en Kbps) y estadísticas de cada enlace. Para tal efecto, se debe indicar el link, usuario y contraseña posterior a la instalación del servicio de internet.
- El postor presentará información con respecto a la tecnología a utilizar, los equipos y accesorios así como también el diagrama o topología respectivo de la solución, en la etapa de implementación como parte del plan de trabajo. donde se visualice la tecnología a utilizar, medios de transmisión, equipos (marca y modelo) propuestos.
- El servicio es a todo costo y debe considerar el alquiler de equipos y/o accesorios de comunicaciones, así como el mantenimiento de los mismos y soporte técnico.
- Debe considerarse un equipo router por cada enlace los cuales deben contar con al menos 4 interfaces 10/100/1000, 1GB de memoria RAM y/o 1GB de memoria FLASH.
- El equipo ha de tolerar el ancho de banda requerido y un 40% adicional como crecimiento (de presentarse la necesidad se revisará como adenda).
- El router no deberá exceder los dos (02) RU de altura.
- El router deberá ser rackable, se aceptará el uso de bandejas.
- El Router no deberá ser de propósito genérico (PC o Servidor) sobre el cual pueda instalarse sistemas operativos base como GNU/Linux, BSD, Sun Solaris, Microsoft Windows, Apple OS-X o similar.

SEGURIDAD INFORMATICA PERIMETRAL (NEXT GENERATION FIREWALL)

- El Servicio Especializado de Seguridad Informática debe considerar; control por políticas, control de aplicaciones, prevención de amenazas, análisis de malware moderno, filtro de contenidos, identificación de usuarios, calidad de servicio, filtro de datos, geolocalización, red privada virtual VPN spam firewall.
- El servicio debe considerar de una solución de seguridad de red con funcionalidades de dos (02) equipos tipo Next Generation Firewall (NGFW) que deberá ser de tecnología vigente y que no se encuentren en etapa de end of sale y/o end of support, la solución ofertada debe estar presente en los últimos 06 reportes del cuadrante mágico de Gartner, que incluya consola de administración y monitoreo en la misma solución. La solución debe estar en Alta Disponibilidad (activo/pasivo)
- La solución debe considerar ser del tipo appliance, chassis o hardware diseñado exclusivamente para la función específica de seguridad, es decir, no se aceptarán equipos de propósito genérico (PC o Servers). Debe ser reconocido como líder en el cuadrante de Gartner última versión.
- Debe incluir filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware "Zero Day", bien como controles de transmisión de datos y acceso a Internet.
- Con soporte para no menos de Throughput de 1.9 con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Seguridad del tráfico DNS, Antivirus/Antimalware de red, Antispyware/AntiBot, Sandboxing, Filtro de Archivos y Logging activo.
- Si el fabricante tuviera diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad.
 - Soporte a, como mínimo, 290.000 de conexiones simultáneas;
 - Soporte a, como mínimo 50000 nuevas conexiones por segundo;
 - IPSEC VPN throughput 1.6 Gbps
 - Fuente 120/240 AC o DC.
 - Ocho (08) interfaces de red 10/100/1000 base-TX;
 - 1 (una) interface de red dedicada para administración;
 - 1 (una) interface de tipo consola o similar;
- Permitir un número no menor a 2500 políticas configuradas.
- Los contextos virtuales deben las funcionalidades nativas del gateway de seguridad incluyendo: Firewall, IPS, Antivirus, Anti-Spyware, Filtro de Datos, VPN, Control de Aplicaciones, QOS, NAT e Identificación de usuarios
- Por consola de administración y monitoreo, se entiende el licenciamiento de software necesario para las dos funcionalidades.
- La consola de administración y monitoreo deberá ser parte de la solución de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función.
- Para efectos de la propuesta, ningún componente de la solución ofertada podrá estar listada en el site del fabricante como listas de end-of-life y end-of-sale.
- Por funcionalidades de NGFW se entiende:
 - Reconocimiento de aplicaciones.
 - Prevención de amenazas
 - Identificación de usuarios.
 - Control granular de permisos
- La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7
- El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operacional de uso genérico, las mismas deben generar sus propios reportes.
- Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19", 1U, standard rack (1.75"H x 17" D x 17" W)
- El software deberá ser ofrecido en su versión más estable y/o más avanzada.
- Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:
 - VLAN Tags 802.1q
 - Agregación de links

- Enrutamiento basado en políticas
- Forwarding basada en políticas
- Ruteo Multicast
- Jumbo Frames
- Sub-Interfaces ethernet lógicas
- Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3;
- Soportar sub-interfaces ethernet lógicas.
- Los equipos podrán ser nuevos o de segundo uso.
- Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
- Debe soportar los siguientes tipos de NAT:
 - NAT de Origen;
 - NAT de Destino;
 - Soportar NAT de Origen y NAT de Destino simultáneamente;
- Enviar log para sistemas de monitoreo externos, simultáneamente;
- Soportar diferentes características de networking operando en el protocolo IPv6, como mínimo: ruteo estático OSPFv3, MP-BGP, policy based routing o policy based forwarding, ECMP, dual-stack, QoS, DSCP, NPTv6, NAT64, LLDP, BFD, DHCPv6 Relay, SLAAC, SNMP.

Alta disponibilidad

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

Funcionalidades de Firewall

- Control de políticas puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos).
- Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- Debe realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.
- Debe permitir la definición de grupos dinámicos de direcciones IP, que permita colocar de manera automática direcciones IP en grupos de cuarentena si éstos realizan acciones maliciosas o restringidas. Estas acciones, deberán poder ser personalizadas en la consola del equipo.

Descifrado de Trafico SSL/TLS

- Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en las estaciones de trabajo.
- Permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el NGFW.
- Deberá soportar al menos los siguientes algoritmos: RSA, DHE, ECDHE; 3DES, RC4, AES128, AES256, CHACHA20-POLY1305; MD5, SHA1, SHA256, SHA384.
- Capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos y/o no fiables, a pesar de no descifrar el tráfico.
- Debe soportar certificados que utilicen Subject Alternative Name (SAN) y Server Name Indication (SNI).
- Permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar excluir del descifrado a páginas con contenido sensible y descifrar el resto de las páginas.
- Permitir excluir sitios a los cuales no se les aplicará la política de descifrado en base al Common Name del certificado.
- Debe contar con un dashboard que muestre gráficamente la proporción del tráfico descifrado, aplicaciones y dominios con descifrado correcto, errores de descifrado.
- Debe contar con un panel de logs dedicados a monitorear el tráfico de descifrado SSL/TLS, estos logs deberán permitir una identificación rápida de problemas del descifrado.
- Desde la consola gráfica deberá mostrar todo el detalle de la sesión SSL/TLS identificada, tales como IP origen y destino, subject common name, issuer common name, server name indication, datos del certificado digital (fecha de expiración, serial number), versión de TLS, algoritmo asimétrico, algoritmo simétrico, hash, estado del descifrado (correcto o con error), motivo del error del descifrado Este detalle de logs no deberá afectar el performance del equipo.
- El postor tiene la libertad de incorporar en su oferta técnica una plataforma tercera que realice descifrado del tráfico y cumpla todas las especificaciones indicadas, en caso el NGFW propuesto no pueda realizarlo o no esté diseñado para ello.

Protección ante ataques de denegación de servicio (dos)

- Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.
- Debe ser posible utilizar SYN Cookies como medida de defensa.
- La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor).
- Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo.
- Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
- Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.

Visibilidad en capa 7 y control de aplicaciones

- La solución propuesta deberá reconocer por lo menos 4000 aplicaciones, incluyendo, más no limitando a aplicaciones de tipo peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email.
- Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. Debe ser capaz de determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.

- Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación. Es decir, si 2 aplicaciones utilizan el mismo puerto y protocolo, se debe poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.
- Deberá contar con un módulo de aprendizaje que permita migrar las políticas basadas en puertos específicos y políticas con puertos ALL/ANY, a políticas basadas en aplicaciones.
- El módulo de aprendizaje deberá ser específico por cada política de seguridad.
- El módulo de aprendizaje deberá mostrar el nombre de la(s) aplicación(es) que han pasado por una política de seguridad, fecha de primera y última ocurrencia y volumen de datos transferido por cada aplicación.
- Deberá contar con un wizard que permita convertir una política basada en puertos (capa 4) a una política basada en aplicaciones (capa 7) en base al aprendizaje realizado.
- En caso la solución propuesta no tenga este módulo de aprendizaje el postor deberá incluir en su oferta técnica el servicio de migración de todas las políticas de seguridad basadas en puertos a políticas basadas en aplicaciones.

Prevención de amenazas

- La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar de forma permanente, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
- El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.
- Deberá contar con un mecanismo que permita identificar los equipos potencialmente infectados en base al análisis de su tráfico DNS, inclusive si el tráfico entre la potencial víctima y su servidor DNS utilizado no pasa por el NGFW.
- Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS.
- El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.
- El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.
- Deberá ser capaz de identificar y bloquear amenazas avanzadas indetectables por firmas o heurística, incluyendo ataques de inyección y command and control realizados con herramientas de Cobalt Strike, Brute Ratel C4.
- La protección contra amenazas avanzadas indetectables por firmas, heurística o reputación del dominio o contenido deberá estar basado en mecanismos de inteligencia artificial, tales como deep learning y/o machine learning.
- Respecto a ataques de malware, las firmas deberán estar basadas en patrones y no únicamente en hashes, con el objetivo de identificar y bloquear el malware polimórfico que pertenezca a una misma familia.
- Con la finalidad de contar con una protección robusta contra amenazas emergentes a nivel mundial, la solución deberá ser capaz de actualizar su base de firmas de malware en tiempo real sin afectar el performance del equipo.
- Deberá contar con un mecanismo basado en aprendizaje de máquina que sea capaz de analizar en tiempo real los archivos desconocidos no identificables por firmas ni heurística; el análisis deberá identificar si los archivos son maliciosos, en cuyo caso el equipo deberá bloquear su ingreso para evitar la infección por amenazas de día cero.
- Debe incorporar una plataforma de sandbox basada en nube para el análisis de ejecutables desconocidos.

- Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SFTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.

Prevención de amenazas avanzadas en DNI

- La plataforma deberá ser alimentada por un servicio de inteligencia global de amenazas capaz de identificar millones de dominios maliciosos con análisis en tiempo real.
- La protección del tráfico DNS deberá contar con mecanismos avanzados de protección, para identificar ataques imposibles de mitigar con firmas y/o reputación del dominio. Para lo cual se requiere que el tráfico DNS sea analizado con técnicas de inteligencia artificial.
- Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algorithm) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.
- Deberá soportar el manejo excepciones para poder mitigar los falsos positivos.
- Deberá contar con dashboards y estadísticas sobre la cantidad, tipo de peticiones DNS, clasificación de la amenaza, generadas por los dispositivos internos de la Empresa/Institución.
- El análisis del tráfico DNS podrá ser realizar de manera local en el mismo equipo, una solución externa (en nube u onpremise) del mismo u otro fabricante.
- En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA.

Sandboxing

- La plataforma de Sandbox podrá ser ofrecido en Nube (Cloud).
- Deberá ser capaz de emular el potencial malware en entornos Windows, Linux y MacOS.
- El Firewall propuesto deberá ser capaz de enviar 1100 archivos por hora al sandbox.
- El sandbox deberá ser capaz de analizar 1100 archivos por hora realizando análisis dinámico del archivo (entiéndase por análisis dinámico aquel que no está basado en firmas, ni prefiltros, sino en emulación completa del potencial malware).
- También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.
- El análisis dinámico deberá realizarse de forma paralela para todos los archivos enviados y no deberá tomar más de 10 minutos en dar un veredicto
- Deberá tener una disponibilidad de al menos 99.9% contabilizados mensualmente.
- Deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II Plus de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- Debe proveer información forense sobre las acciones realizadas por el malware, tales como resumen del comportamiento visto, actividad sobre los archivos, peticiones DNS, conexiones de red, actividad de los archivos, procesos y registros. Esta información deberá poder se extraída en un reporte PDF.
- Deberá ser capaz de analizar archivos sospechosos que se transfieran por los protocolos SMTP, POP3, IMAP, SMB, FTP, HTTP y HTTPS.
- Debe ser capaz de identificar amenazas de tipo Fileless.
- Deberá contar con al menos 20 técnicas patentadas para realizar el análisis del malware.
- Luego del análisis realizado por el sandbox, éste deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. Las firmas deben estar basadas en patrones del malware y no únicamente hashes, de tal forma que sea capaz de bloquear el malware polimórfico con una única firma.
- Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- Debe permitir al administrador la descarga del archivo original analizado por el sandbox.
- Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.

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

Filtro de contenido Web

- Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.
- Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs
- Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.
- El análisis en tiempo real deberá determinar si la página web desconocida (no categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.
- Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.
- Debe permitir la creación de categorías personalizadas.
- Debe permitir la personalización de la página de bloqueo.
- Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.
- Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet
- Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.
- Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de robo de credenciales.

Identificación de usuarios

- Debe permitir la creación de políticas de seguridad basadas en la identidad del usuario y grupo al cual pertenece, a través de la integración de servicios de autenticación como Active Directory, Novell eDirectory, Open LDAP y base de datos local.
- Debe contar con varios mecanismos para la identificación del usuario y la dirección IP del equipo en donde se encuentra autenticado. Como mínimo deberá poder integrarse a las siguientes plataformas para cubrir este requerimiento:
- Eventos de login gestionados en Domain Controller y/o Microsoft Exchange.
- Capacidad de leer eventos de login y logout usando el protocolo WinRM.
- Terminal Server de Microsoft o Citrix
- Consultando directamente a cada estación de trabajo a través del protocolo WMI
- Lectura de la cabecera XFF al integrarse con soluciones terceras de Proxy
- Capacidad de extraer la información de IP y usuarios a través de la lectura y extracción de datos del tráfico syslog.
- Integración con soluciones de Wireless LAN Controller basadas en 802.1x y Soluciones NAC, con el objetivo de que el NGFW no dependa del Domain Controller para identificar al usuario.
- A través de agentes instalados en las estaciones de trabajo, que reporten directamente al NGFW el usuario y dirección IP de cada equipo.
- Deberá contar con un componente que permita integrarse a diversas plataformas de identidades tales como Azure LDAP, Google Directory, Okta, Cisco Duo, PingID.
- Debe contar con la funcionalidad de Portal Cautivo (Captive Portal), de tal manera que el NGFW muestre un portal al usuario para que se autentique manualmente. Las cuentas podrán ser definidas localmente en el NGFW o integradas con plataformas terceras.
- Debe tener integración con plataformas de MFA (Multi Factor Authentication), de tal forma que cuando un dispositivo requiera acceder a recurso, se le solicite el OTP.

- Debe permitir la definición de grupos dinámicos de usuarios, que permita colocar de manera automática a los usuarios en grupos de cuarentena si éstos realizan acciones maliciosas o restringidas. Estas acciones, deberán poder ser personalizadas en la consola del equipo.

QoS

- Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube o Netflix), se requiere que la solución tenga la capacidad de controlarlas a través de políticas personalizables.
- Soportar la creación de políticas de QoS por: dirección de origen y destino, por grupo de usuario de LDAP, por aplicaciones, por puerto.
- El QoS debe permitir la definición de clases por: ancho de banda garantizado, ancho de banda máximo, prioridad.
- Soportar marcación de paquetes DSCP, inclusive por aplicaciones;
- Permitir el monitoreo en tiempo real del tráfico gestionado por el QoS.

VPN

- Soportar VPN Site-to-Site en protocolo IPSec
- La VPN site to site debe soportar como mínimo:
- DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
- Autenticación MD5, SHA-1, SHA-2;
- Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
- Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- Permitir aplicar QoS dentro de los túneles VPN.
- Soportar VPN client-to-site pudiendo operar usando el protocolo IPSec o SSL.
- Permitir la conexión por medio de agente instalado en el sistema operativo.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS.
- Capacidad de integrarse con plataformas de Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN, incluyendo el soporte de Split DNS.
- El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y el Dominio.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
- Antes del usuario se autentique en la estación.
- Después de la autenticación del usuario en la estación usando Single Sign On (SSO).
- A demanda, de forma manual por parte del usuario.
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.
- La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada, de manera manual y automática. Los equipos en cuarentena no deberán tener conexión con ningún recurso de red protegido por la solución.

- Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar determinadas características del equipo y en base al nivel de cumplimiento (compliance) del host permitir, denegar o limitar el acceso a los recursos de la red interna. Por lo menos se deberá poder configurar los siguientes casos de uso y una combinación de ellas:
- Sistema operativo del equipo
- Serial number del equipo
- Pertenencia al dominio corporativo
- Software antivirus instalado y habilitado en tiempo real
- Software antivirus con la base de datos de firmas actualizada en un número de días personalizable
- Haber realizado un escaneo del malware en un equipo dentro de un número de días personalizable
- Marca del software antivirus
- Parche de seguridad instalado, según su nivel de criticidad
- Firewall de host habilitado
- Software de cifrado de disco instalado
- Software de DLP instalado
- Permitir añadir validaciones de aplicaciones personalizadas añadiendo la Clave de Registro (en caso de Windows) o Plist (en caso de MacOS)
- Todos los parámetros indicados deberán poder ser realizados desde la consola gráfica de la plataforma. No se aceptarán configuraciones a través de CLI.

FILTRO DE SEGURIDAD PARA CORREO ELECTRONICO (ANTISPAM)

Características generales

- La solución debe ser una plataforma 100% nube que brinde un servicio de tipo SaaS.
- La solución debe estar licenciada para 1000 buzones de correo electrónicos.
- Función de notificación por correo de manera automática a los usuarios con resumen del contenido de la casilla de correos en cuarentena
- Sistema Modular, con soporte de protección Antivirus.
- Zombie detection & flood protection
- Deberá contar con un módulo de Sandbox para análisis de amenazas de día cero.
- Deberá contar con administración de políticas de DLP (Prevención de fuga de información) y cumplimiento de normas (HIPAA, SOX, GLBA, PCI-DSS)
- Capacidad de bloquear el paso de tipos de archivo por extensión y contenido del archivo
- Integración con los sistemas LDAP y Active Directory.
- Sin límite de cantidad de dominios de correo electrónico a proteger
- Capacidad para el control de las conexiones y prevenir ataques de negación de servicio
- Efectividad de detección igual o superior al 99%
- Capacidad para el Bloqueo de Phishing
- Protección de Directorio Harvest Attacks y NDRs (Non-delivery reports)
- Soporte de Protocolos de correo: SMTP/ESMTP sobre TLS
- Capacidad de generar políticas al tráfico entrante y al tráfico saliente de forma independiente.
- Uso de Tecnología Heurística o bayesian para la detección del spam
- Capacidad para detectar el idioma del correo (7 idiomas como mínimo)
- Soporte a implementaciones en alta disponibilidad para redundancia y/o balanceo de cargas
- Creación de Políticas, por dominio, por usuario o por grupo.
- Notificación Automática a los usuarios indicando los correos SPAM que tiene almacenado para que ellos pueden gestionar su contenido.
- Poseer una base de datos para el bloqueo de direcciones IP y de base de datos por reputación, desarrollada y mantenida por el fabricante.
- Soporte de agregación de encabezados con mensajes propios de la Entidad para notificación a los usuarios por eventos que se requieran informar.

- La solución debe poseer un sistema de actualización automática con nuevas formas de ataques.
- La herramienta debe tener la capacidad de configurar: clasificación y categorización remitentes permitidos, opción con la cual se pueda especificar a qué mensajes de correo no deben aplicarse la comprobación de Antispam y/o anti-Phishing. Estos remitentes pueden ser por redes y dominios determinados.
- Separación de políticas de filtrado de contenido del tráfico entrante y saliente.
- Realizar excepciones a las reglas de filtrado para usuarios determinados.
- Bloqueo de archivos adjuntos de acuerdo con el asunto del mensaje (subject), texto del mensaje, extensión nombre de archivo y al usuario de destino.
- Posibilidad de configurar filtros con capacidad de análisis de encabezado, asunto y contenido.
- Configuración del límite de la cantidad de mensajes por sesión de SMTP.
- Configuración del límite de los attachments (size en KB o MB) a nivel de TCP. Estas funcionalidades luego de configuradas deben ser ejecutadas en forma automática y sin Intervención manual del administrador.
- Debe poseer capacidad de identificación y bloqueo de SPAM en distintos idiomas.
- Capacidad de marcado de mensajes en el sujeto o encabezado y posterior envío a buzón alternativa de usuario.
- La solución debe manejar sistema agente de transporte de mensajes MTA.
- La herramienta debe notificar al administrador de la solución sobre eventos, cuarentenas, reportes de mensajes procesados, de forma automática vía e-mail.
- Enrutamiento del spam según niveles de forma selectiva de acuerdo con la puntuación de correo no deseado.
- Generación de listas blancas y negras según políticas establecidas por la organización.
- Reglas de filtrado por destino, remitente, copia carbón, encabezado de correo, cuerpo, tamaño, archivos adjuntos, contenido malicioso, bloqueo de archivos, cabecera MIME
- Opciones de Configuración ANTI-RELAY
- Múltiples opciones de respuesta: eliminar adjunto, eliminar mensajes, entrega normal, enviar a cuarentena.
- Soportar el manejo de colas de envío y recepción de correo en paralelo (por destino), por dominio o dirección IP.
- Deberá soportar SPF (Sender Policy Framework Verification)
- Deberá soportar DKIM (Domain Keys Identified Mail)
- Deberá Soportar DMARC (Domain Message Authentication Reporting)
- Soporte para ruteo de mensajes por dominio, tabla de alias y LDAP.
- Debe poseer compatibilidad LDAP con Active Directory, Notes, Domino y Open LDAP servers.
- Soporte para enmascaramiento de dominio, por LDAP en el correo saliente.
- La autenticación por LDAP se podrá aplicar durante la conversación SMTP o durante el procesamiento de los mensajes.
- Soportar manejo de máximas conexiones concurrentes desde una sola IP configurable por dominio o IP origen.
- Soportar manejo de máximos mensajes por conexión configurable por dominio o IP origen.
- Soportar manejo de límite de máximo destinatarios por mensaje configurable por dominio o IP origen.
- Soportar manejo de límite de recepción de correo (rate limit) configurable por dominio o dirección IP origen.
- Incluir actualizaciones periódicas o inmediatas, de nuevas reglas y algoritmos de correo no deseado.
- Distribución diaria de las actualizaciones, incluyendo la actualización gratuita, continua y automática contra firmas de ataques.
- El fabricante proveerá actualizaciones en modo online, sin requerir corte reinicio o apagado del sistema.

Administración

- Debe poseer una interfaz de administración vía browser sobre protocolo HTTPS
- Sistema de tener reportes exportable a HTML, PDF, CSV y por tareas automáticas programables en fechas y horas, por periodos diarios, semanales, mensuales, etc.

- Proveer un sistema de reportes estadísticos por virus, SPAM, ataques, IP origen, IP destino, Dominio de Redes, detallando los propietarios de las redes.
- Debe poseer un sistema seguimiento de mensajes (messages tracking) desde la misma consola web de administración.
- Factibilidad de generación de solicitudes de soporte con el fabricante desde la consola de administración.
- Debe permitir la creación de múltiples usuarios administradores con distintos niveles de permiso de acceso.
- Soporte de backup y restore de toda la configuración realizada
- Reporte automático de alertas y/o alarmas a través de correo electrónico

Funcionalidades de módulo de Antivirus

- Debe proveer una solución Antivirus embebida en el sistema sin instalar software o hardware adicionales.
- Debe soportar al menos 02 (dos) motores de antivirus embebidos en el sistema para análisis y detección de virus y licenciado al menos uno de los motores.
- Debe detectar virus, malware y otros tipos de software indeseados por medio de secuencias de códigos específicos que se encuentran en los virus.
- Facultad de manejo de múltiples opciones para el manejo de mensajes, en caso estén infectados, encriptados no pudieron ser escaneados.
- Debe contar con un sistema de cuarentena.
- Debe permitir colocar etiquetas a los mensajes infectados, limpiados, encriptados y los que no se han podido escanear.

Funcionalidades de módulo de Sandbox

- Debe proveer una solución de sandbox en la nube sin necesidad de instalar otro appliance para esta funcionalidad.
- El módulo de sandbox deberá ser multi-motor.
- Deberá detectar y bloquear amenazas hasta el veredicto, los archivos no deberán llegar hasta el usuario hasta que el sandbox del veredicto sobre el archivo.
- El servicio deberá incluir protección avanzada de URL
- que analice dinámicamente URL's incrustados para bloquear y poner en cuarentena mensajes con URL's maliciosas antes de que alcancen la bandeja de entrada de los usuarios
- Sistema de sandbox completo con emulación y virtualización

Funcionalidades de buzón de usuarios

- Autenticación SMTP de entrada/salida
- Buzón de emergencia que permite almacenar correos hasta por 7 días en caso de caída del servidor de correo
- Junk Box por usuario
- Agresividad de Anti-Spam por usuario
- Detalles del juicio del SPAM

SOLUCIÓN DE PROTECCION DE APLICACIONES WEB

- La solución deberá soportar por lo menos cinco (05) aplicaciones y un ancho de banda **mínimo de 25 Mbps 20Mbps**.
- La solución deberá estar catalogada como líder en el cuadrante de gartner de los últimos 2 años.
- La implementación de la solución deberá requerir únicamente cambiar la configuración de DNS para los Dominios web que apuntan a los Aplicativos Web. Es decir, no requiere la instalación de hardware o software adicional o hacer cambios en la programación de las aplicaciones.

- La solución deberá soportar cualquier aplicación web, sin importar la plataforma, tamaño del sitio, lenguaje o escenario de implementación.
- La solución deberá ofrecer los siguientes servicios en una única plataforma integrada
- Web Application Firewall WAF
- Detección de Backdoors en aplicativos Web
- CDN con failover y redundancia
- Almacenamiento en Cache
- Optimización de Contenido
- Servicio de Mitigación de ataques DDoS L3/L4/L7
- Servicio de Mitigación de ataques DDoS al servicio DNS
- Herramientas de monitoreo en tiempo real de conexiones, ancho de banda y ataques.
- Capacidad de exportar los eventos de seguridad a una herramienta tipo SIEM
- Una vez configurada, la solución tendrá la opción de deshabilitarse/habilitarse sin tener que hacer cambios en la Aplicación o DNS. Sin afectar el servicio a los usuarios.
- La solución deberá garantizar un SLA del 99.999%
- La solución deberá contar con la Certificación de Proveedor PCI Nivel 1
- La solución deberá contar con la certificación "SOC 2" tipo "I y II", con los cuales garantice que los sistemas utilizados, su diseño y su efectividad operacional, son adecuados para cumplir con los principios de confianza definidos por la AICPA
- El proveedor deberá contar con una capacidad de red global de al menos 9 Tbps
- Como respuesta a un ataque, deberá ofrecer la opción de únicamente alertar o de bloquear al usuario o la dirección IP origen por un periodo de tiempo
- Deberá permitir la creación de reglas personalizadas basadas en al menos URL, tasa de peticiones, existencia de algún parámetro o header HTTP, si el cliente es humano o bot, y el contenido del header REFERER.
- El servicio debe contar con un equipo de especialistas del fabricante que desde un SOC realicen el afinamiento y monitoreo continuo de las reglas de seguridad gestionadas

Web application Firewall (WAF)

- La solución deberá permitir la creación de políticas de seguridad personalizadas, mediante la configuración de una variedad de factores que las desencadenen, además de tener múltiples acciones como bloquear Usuario, Bloquear petición, Bloquear Usuario o poner en cuarenta la URL.
- La solución deberá entregar un análisis detallado de las amenazas, incluyendo:
 - Dirección IP
 - User Agent
 - Locación geográfica
 - Información relevante de la sesión
- La solución deberá contar con un mecanismo de perfilado, dicho mecanismo debe diferenciar entre usuarios humanos, bots legítimos (google, bing) y robots maliciosos como gusanos.
- La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
- La solución deberá contar con una clasificación de bots basada en reputación para la distinción de Bots buenos, malos y sospechosos. Permitiendo el bloqueo de ataques como comment spam, scraping y escaneo de vulnerabilidades, y asegurando el acceso de bots como Google, Facebook y Pingdom.
- La solución deberá detectar y bloquear los intentos de instalar y/o operar backdoors en los Aplicativos Web.
- La solución deberá hacer bloqueos a partir del País de Origen (GeoBlocking)
- La solución deberá contar con un sistema de Seguridad Colaborativa para evitar ataques que han sufrido otros sitios web. (Crowdsourcing)
- La solución deberá incluir un servicio de Inteligencia Artificial y Machine Learning para la investigación, correlación de eventos de seguridad y alertas originados por el firewall de aplicaciones web independientemente donde resida ya sea en sitio, en la nube o híbrido.
- La solución deberá permitir la creación de reglas personalizadas para reescribir peticiones (URL Rewrite)

- La solución deberá permitir crear reglas personalizadas para agregar/quitar encabezados en los paquetes HTTP, como, por ejemplo, X-Forward-For, País, Ciudad, Coordenadas de geolocalización y contar con una mayor visibilidad del origen de las conexiones.

Protección DDoS

- La solución deberá proporcionar los mecanismos necesarios para la mitigación de todos los tipos de ataques DDoS, ya sean basados en la Red (Capa 3, 4) o ataques de nivel aplicativo (Capa 7). Teniendo en cuenta la siguiente lista:
 - TCP SYN+ACK
 - TCP FIN
 - TCP RESET
 - TCP ACK
 - TCP ACK+PSH
 - TCP Fragment
 - UDP
 - ICMP
 - IGMP
 - HTTP Flood
 - Brute Force
 - Connection Flood
 - Slowloris
 - Spoofing
 - DNS Flood
 - Mixed SYN+UDP or ICMP+UDP Flood
 - TCP SYN+ACK
 - Ping Of Death
 - Smurf
 - Reflected ICMP and UDP
 - Teardrop
 - Zero-day DDoS attacks
 - Ataques comunes a plataformas Web (Apache, IIS)
- La solución deberá proporcionar conocimiento de la situación en tiempo real para la detección temprana de ataques de DDoS para que el tiempo entre el ataque y la mitigación sea reducido.
- Para la mitigación de ataques DDoS al servicio DNS, la plataforma de nube deberá tomar el rol de NS (Nameserver), designado a través del sistema DNS global, para que sea la primera instancia que reciba peticiones de DNS provenientes de Internet y destinadas a la infraestructura; y las reenvíe después de la inspección de seguridad.
- Deberá de tener la capacidad de definir los queries de DNS válidos, en cuanto a tipo y dominio, que habrá de dejar pasar a los servidores DNS reales, bloqueando el resto de las peticiones.

Optimización y Disponibilidad

- La solución deberá contar con una consola en tiempo real en la cual se podrá monitorear y verificar que el tráfico se está optimizando de forma correcta.
- La solución deberá ser capaz de proveer la capacidad de hacer compresión y almacenamiento en cache.
- La solución deberá soportar las siguientes capacidades para el almacenamiento en cache
 - Contenido Estático
 - Contenido Dinámico
 - Servir Paginas desde Memoria

- Almacenamiento cache desde el lado del Usuario
- La solución deberá tener la opción de generar reglas personalizadas para el almacenamiento en cache.

Gestión SSL

- La solución debe incluir el despliegue de certificados SSL entregados por el fabricante (la misma cantidad de las aplicaciones ofrecidas). Estos certificados deben ser válidos y firmados.
- La solución debe permitir la carga de certificados SSL de la entidad ya sea para validación de los sitios o para autenticaciones avanzadas como MTLS
- La solución debe soportar autenticación MTLS

Servicio DNS

- La solución deberá contar con la capacidad de proteger el servicio de DNS contra ataques, y a su vez realizar la optimización del servicio de DNS.
- La solución deberá ser capaz de funcionar como DNS Proxy.
- La solución deberá ser capaz de funcionar como Managed DNS.

SERVICIO DE TELEFONIA MOVIL

- Brindar 06 líneas nuevas de telefonía móvil (incluye equipo celular)
- Las líneas deberán contar con cobertura a nivel nacional y un plan de Datos de como mínimo 100GB
- Las líneas deben permitir llamadas ilimitadas a cualquier operador fijo y móvil local y nacional
- Las líneas deberán permitir:
 - SMS ilimitados
 - Apps ilimitadas (FACEBOOK MESSENGER, WHATSAPP, WAZE)
 - El POSTOR asignará un Ejecutivo Comercial que atenderá tanto la parte de servicios móviles como servicios fijos.
 - Las líneas de telefonía móvil serán según la siguiente distribución

CATEGORIA	CANTIDAD	Internet /GB alta velocidad
A	06	ILIMITADO/100 GB

- Como parte del servicio móvil deberán entregarse dispositivos móviles con características técnicas que faculden el aprovechamiento de los servicios contratados de acuerdo a cada categoría.
- Especificaciones técnicas de los equipos

CATEGORIA A

- **Sistema operativo:** ANDROID
- **Procesador:** QUALCOMM SD 685
- **Tamaño de Pantalla:** 6.67"
- **WIFI:** Si
- **Peso:** mínimo 188g.
- **Bluetooth:** Si V5.1
- **Cámara de fotos Principal:** 108+8+2 Mpx

- **Cámara de fotos Frontal:** 16Mpx
- **Radio FM:** Si
- **Grabadora de Voz:** Si
- **Tipo de Batería:** Li-Po / Interna / 5000mAh
- **Capacidad Memoria Interna:** 256GB
- **Capacidad Memoria RAM:** 8GB
- **Reconocimiento Facial:** Si
- **Lector de Huella:** Si
- **Dimensión:** 162.24*75.55*7.97MM
- **Carga rápida:** Si

CAPACITACION

- Debe brindarse una capacitación para cuatro (04) personas, como mínimo. El número total de horas de la capacitación no deberá ser menos de 08 horas. Las 8 horas de Capacitación serán por cada tecnología de seguridad ofrecida por el postor por los siguientes temas indicados:
 - Solución de Seguridad Perimetral (Next Generation Firewall)
 - Solución de Protección de ampliación web (WAF)
 - Solución de Seguridad de Filtro de Correo.
- Debe brindarse un curso no menor a Setenta (70) horas en Seguridad en Redes para 2 participantes. Debe incluir laboratorios con entornos virtuales para cada alumno. El Centro de Enseñanza debe contar con el respaldo de un fabricante de equipos de Seguridad en Redes de preferencia CURSO DE ESPECIALIZACIÓN EN CCNP ENTERPRISE.
- Debe brindarse un curso Oficial de CERTIFIED BUSINESS PROCESS MANAGEMENT PROFESSIONAL (ISO19510), un curso de CERTIFIED CLOUD COMPUTING PROFESSIONAL, un curso de CERTIFIED BUSINESS CONTINUITY MANAGEMENT PROFESSIONAL (ISO22301) y un curso de CERTIFIED IT CORPORATE GOVERNANCE PROFESSIONAL (ISO 38500) que incluya examen y certificación internacional (es responsabilidad de INSTITUTO NACIONAL MATERNO PERINATAL la aprobación del examen de certificación)
- Las capacitaciones podrán ser brindadas de manera virtual.

SOPORTE TÉCNICO

- Durante el período de garantía comercial, debe contar con un Centro de Operaciones de Seguridad **propio y/o tercerizado** para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.
- El postor deberá contar con un Centro de Operaciones de Seguridad (SOC certificado con ISO 27001) para el servicio de Soporte Técnico, con la finalidad de garantizar que se cuente con procesos de atención óptimos que asegure el cumplimiento de los tiempos de respuesta, la calidad de su atención, así como el aseguramiento de la confidencialidad e integridad del manejo de los datos y de la información de la entidad.
- El Proveedor deberá ofrecer una solución de monitoreo de tráfico, eventos, detección y orquestación de respuestas con enfoque contra las amenazas cibernéticas en el ambiente heterogéneo de las redes modernas, donde las fronteras cada vez son más difusas. Es por ello que se requiere de una solución para proteger, asegurar y defender la infraestructura, así como los datos de posibles daños, acceso no autorizado y uso indebido de recursos de TI. La solución deberá ser abierta, agnóstica y capaz de integrar cualquier fuente de información de las diferentes marcas que operan la ciberseguridad en la entidad (no open source) aplicando los conceptos de Open XDR (Extended Detection and Response).
- La solución de monitoreo de tráfico, eventos, detección y orquestación de respuestas busca un enfoque proactivo para el manejo de ciber amenazas dentro de la infraestructura de La entidad, el cual brindará visibilidad de los datos a través de redes, nubes y puntos finales, mientras se aplica análisis y automatización para abordar las ciber amenazas cada vez más sofisticadas de la actualidad.

- La solución deberá incluir y abarcar en una sola licencia y plataforma las siguientes características:
- Módulo de UEBA (análisis de comportamiento de usuarios y entidades)
- Módulo de Detección de Phishing.
- Módulo de Caza de Amenazas (Threat Hunting)
- Módulo de Automatización de Respuesta.
- Módulo de Sistema de información y gestión de eventos de seguridad (SIEM)
- Módulo de Sandbox de Red.
- Módulo de Inteligencia de Amenazas
- Módulo de Monitoreo de Integridad de Archivos
- Se deberá considerar dentro de la solución y como parte de la misma, estas actividades de entrega:
- Deberá de implementarse de manera transparente a través de sensores y/o sondas virtuales **y/o colectores**, para proporcionar telemetría. La entidad proporcionara los recursos necesarios para el despliegue.
- Deberá de rastrear las amenazas en cualquier fuente o ubicación dentro de la entidad, incluyendo y no limitado a: redes, servidores (físicos y virtuales), aplicaciones, contenedores, nubes pública y privada.
- Deberá de identificar amenazas ocultas, sigilosas y sofisticadas, en archivos o en el tráfico de red de forma pro-activa y rápida en la infraestructura tecnológica.
- Deberá de realizar análisis de patrones de tráfico este-oeste (tráfico en el mismo segmento de LAN) a través de un puerto espejo o port mirror **o envío a través de Netflow**.
- Deberá de correlacionar los eventos, anomalías e incidentes identificados de manera automática.
- Deberá permitir la caza de amenazas en todos los ambientes de La entidad.
- Deberá Integrarse a la infraestructura de firewalls de la entidad para enriquecer la información colectada, independientemente de la marca.
- Deberá tener la capacidad de responder cada evento de ataques de ciberseguridad de manera orquestada y automatizada integrándose con la infraestructura tecnológica de ciberseguridad y redes presente en la Institución para tal fin.
- Debe estar considerada para la cantidad de 1000 usuarios, 100 dispositivos informáticos y/o **mínimo 1500 EPS 400 EPS**.
- El Proveedor deberá considerar todo el equipamiento, licencias, implementación, puesta a punto, memoria técnica y entrenamiento de los componentes tecnológicos que componen el servicio de Orquestación de Red y respuesta a Incidentes.
- El proveedor deberá proporcionar el servicio para la continuidad operativa con capacidades de analizar en el tráfico de la red: eventos de seguridad anómalos y críticos, en internet, la comunicación Este-Oeste y Norte-Sur la red interna, perimetral, las aplicaciones, contenedores, servidores, usuarios, entre estos elementos que representen un riesgo para la entidad, y que sea capaz de recolectar información de datos que cursen hacia y desde la MPLS, Internet, LAN to LAN, LAN, servidores u otros, con una amplia variedad de patrones de uso.
- Para este Servicio, el sistema deberá contar con al menos las siguientes funcionalidades:
- Proveer la habilidad de escuchar el tráfico de la red de manera transparente y descubrir elementos nuevos de infraestructura automática.
- Visibilidad en toda la red (extremo a extremo), logrando identificar, eventos de Ciberseguridad, las anomalías críticas, correlaciones, conexiones y segmentos. Mostrando la distribución de las amenazas presentes, intentos de infiltración y riesgo, de acuerdo con los estados de MITRE ATT&CK para mejorar la postura de seguridad dlla entidad.
- Esta solución deberá tener la capacidad de integrar las diferentes plataformas que integran la red de La entidad, para correlacionar de manera automática.
- Contar con Inteligencia Artificial para correlacionar todos los eventos de manera automática y cercano a tiempo real.
- La solución debe de contar con diversas funcionalidades que permitan maximizar la capacidad de detección a través MITRE ATT&ACK de manera automática, como mínimo:
- IDS basado en Machine Learning
- Sandbox
- Analítica de comportamiento de Usuarios y entidades (UEBA)
- Detección de Phishing
- Network Detection and Response

- Caza de Amenazas (Threat Hunting) empoderado con Graph Machine Learning
- Módulo de Automatización de Respuesta
- Sistema de información y gestión de eventos (SIEM)
- Threat Intelligence Platform (TIP) Herramienta de enriquecimiento de información automática de cada evento. Mínimo 30 listas de proveedores de Inteligencia de información.
- Monitoreo de Integridad de Archivos
- La solución podrá estar basada en equipos colectores que puedan conectarse vía puerto espejo, por medio de TAP's o packet brokers o envió a través de Netflow, que le hagan llegar paquetes en crudo. Los colectores reportarán a un servidor central o bien, el proveedor podrá llevar a cabo la configuración remota de los paquetes de red de cada localidad y envío de los mismos a un servidor central cuidando que este tráfico no represente un consumo dentro del ancho de banda de los enlaces solicitados por La entidad.
- El sistema deberá ser capaz de integrar al monitoreo aplicaciones y desarrollos propios de La entidad al menos por:
 - Identificador de aplicaciones no limitado al puerto TCP/UDP
 - Direcciones IP de los servidores.
 - IP Origen y Destino.
- La recolección de datos de la solución no deberá afectar el rendimiento de la red de La entidad. Por lo que no deberá ser una solución exclusivamente basada en agentes.
- La solución deberá generar información detallada de los eventos detectados, incluyendo amenazas, anomalías, comportamientos y tendencias de la red asociadas al riesgo en la red.
- El sistema deberá ofrecer una solución de almacenamiento para datos históricos de seguridad que concentre todos los sitios de La entidad durante la vigencia del contrato.
- Datos de eventos de seguridad
- Datos de aplicación
- Datos de Sistemas operativos
- Datos de la nube pública y privada
- Datos de Trafico de Red
- Datos de fuentes de Inteligencia de amenazas
- Datos de geolocalización
- Trafico de registros (syslog)
- La solución propuesta deberá ser capaz de crear reportes que permitan seleccionar el periodo (por hora, día, semana, mes, año, y personalizada es decir por fechas específicas) y/o por grupo de nodos manteniendo disponible en línea la información por lo menos 1 año. Este sistema almacenará los eventos de seguridad, hasta la conclusión del contrato. Toda la información deberá estar disponible, en los diversos tableros de reportes, disponibles en la plataforma, así como en el sistema de reportes, para el envío de estos de manera automatizada.
- Analizar el tráfico TCP/UDP en la red de La entidad para detectar comportamiento y posibles amenazas, generando eventos accionables de acuerdo con el tipo de tráfico.
- La solución deberá ser capaz de realizar desgloses sobre las gráficas para mostrar el detalle de la información (proceso conocido en inglés como Drill Down).
- La solución deberá estar disponible con los datos en gráficas que podrá filtrarse, al menos: por minutos, horas, días o meses.
- Se deberán emitir alertas cuando se detecten eventos críticos de seguridad en la red, se desvíe de los patrones establecidos (anomalías), mediante el análisis detallado de todas y cada una de las aplicaciones que corran en la red de manera nativa.
- La solución deberá incluir mecanismos de sincronización como NTP (Network Time Protocol) o PTP (Precision Time Protocol) y así garantizar la correcta sincronización de la información.
- La solución deberá poder integrar con métodos de autenticación vía Directorio Activo y LDAP, asimismo para identificar patrones de comportamientos anómalos de usuarios y poder deshabilitar usuarios del domino en caso de estar comprometidos o asociados a una amenaza.
- La solución deberá contar con una aplicación que permita la caza de amenazas (Threat Hunting), para identificar las amenazas presentes en la red y automatizar los subsecuentes eventos de seguridad presentes en la red.
- El sistema deberá contar con un visor de eventos que al menos de una vista retrospectiva de las mismas.

- La herramienta deberá tener la capacidad de obtener mediciones de amenazas presentes en el tráfico y monitoreo pro activo cercano a tiempo real de todo el tráfico cursando por la red dla entidad, por lo menos, bajo las siguientes métricas:
- Utilización de ancho de banda.
- Intentos de penetración y escaneos de IPs y puertos
- Autenticaciones fallidas
- Ataques de autenticación de fuerza bruta exitosos
- Presencia de tráfico malicioso, como Ransomware, movimiento lateral, Cryptojacking, Mimikatz, etc
- Análisis de archivos benignos y maliciosos y sus respectivas categorías.
- Ataques de negación de servicio
- Conexiones de Comando y Control Presentes, internamente o hacia/desde Internet
- Hosts que representan el mayor riesgo
- Tiempos de respuesta, tráfico de entrada y de salida (inbytes/outbytes)
- Aplicaciones que más consumen recursos de red
- Análisis de DNS (tiempos de respuesta, time-out, errores y desempeño).
- Distribución de las conexiones y su riesgo asociado
- Utilización de los servidores de Bases de Datos presentes (Top queries, usuarios, origen y destino y el detalle de uso
- Distribución de aplicaciones de capa 7
- Top de los eventos de seguridad críticos
- Tiempo de respuesta de aplicaciones.
- En los sistemas virtuales cuyo tráfico atravesase la red física monitoreada, se deberán obtener al menos las siguientes métricas: Eventos de seguridad más críticos identificados en los servidores virtualizados.
- Las aplicaciones que más se usan.
- Top de eventos de seguridad entre las máquinas virtuales.
- Riesgo asociado entre las máquinas virtuales.
- Deberá ser capaz de realizar análisis retrospectivo basado en el análisis de la ingesta del tráfico TCP/UDP (análisis forense).
- Deberá contar con una Plataforma de Inteligencia de Amenazas (TIP) integrada directamente en la solución.
- Deberá proveer una capacidad de detección de ataques novedosos, conocidos como Zero Day
- Deberá proveer un mecanismo para la clasificación de alertas de acuerdo al sentido del ataque (Interno o Externo)
- Las capturas de paquetes que sean obtenidas por la solución, deberán poder ser convertidas en metadatos para su análisis posterior.
- Deberá permitir generar diagramas de las conexiones TCP mostrando cómo las amenazas asociadas, así como la comunicación entre el servidor y el cliente. Esto basado en capturas de tráfico, clasificado y normalizado de manera automática.
- La solución deberá mostrar los eventos críticos y anomalías en las conversaciones TCP/UDP., así como en aplicaciones, servicios, servidores (físico y virtuales) y nubes públicas y privadas
- Deberá permitir usar los paquetes almacenados en las sondas de monitoreo para crear gráficas de los eventos de seguridad entre 2 hosts que muestren dichas amenazas presentes en la conexión, con detalles que incluyan: el origen y destino, la geolocalización, reputación, evidencia de todos los eventos y que permitan una respuesta de estos.
- La solución de análisis y tráfico deberá graficar las anomalías de las aplicaciones dentro de la red, entregando resultados Top de al menos las siguientes variables:
- Movimientos laterales.
- Crónica de eventos.
- Anomalías de tráfico malicioso.
- Anomalías en las políticas y negaciones de los firewalls de la infraestructura del La entidad.
- Top Aplicaciones.
- Top Servidores.
- Top Clientes.
- Estados de las sesiones presentes.
- Orígenes y destinos de países con mala reputación

- La plataforma deberá de generar KRI, tales como la cantidad de eventos generados en un día, semana o mes y compararlo con periodo similar, lo mismo, con la criticidad promedio de los eventos.
- La solución de análisis de tráfico deberá integrarse con los elementos de IT presentes en la red, como FW, EDR, para enriquecer la información recopilada para su análisis
- Deberá permitir inventariar los activos presentes en la red por direcciones IP y el nivel de riesgo de estos activos, con detalles y evidencia de esto sin necesidad de ejecutar análisis activos en la red para este fin.
- Deberá ser capaz de monitorear el comportamiento de la red de ancho de banda por aplicación y así mismo identificar tendencias de crecimiento para poder tomar decisiones proactivas.
- Deberá contar con mecanismos de control de acceso y autenticación basado en rol, para que únicamente el personal autorizado por La entidad, a través de la DSI tenga acceso a la información.
- La plataforma deberá proporcionar tableros configurables que podrán contener diferentes paneles o gráficas de información, mostrando al menos la siguiente información:
 - Eventos anómalos y críticos, los cuales incluyan:
 - Detecciones de seguridad.
 - IP Origen y Destino.
 - Panorámica de la actividad de los equipos (servidores e infraestructura, física y virtualizada).
 - Las tácticas y técnicas asociadas al marco de MITRE ATT&ACK
 - Aplicación presentes o históricas en total y desglosado por:
 - Riesgo asociado.
 - IP Origen y Destino.
 - Información de geolocalización
 - Información de fuentes de inteligencia de amenazas
 - Anomalías detectadas.
 - Calificación de riesgo.
 - Conversaciones entre Hosts.
- ~~Deberán permitir visualizar para un Host:~~
- ~~Aplicaciones presentes.~~
 - Conversaciones hacia y desde el Host basadas en detecciones de seguridad y anomalías.
 - Deberá observar el estado de las aplicaciones y servicios que están corriendo en el centro de datos, como:
 - Indicar el número y severidad de las anomalías en indicadores clave de desempeño.
 - Indicar posibles problemas de seguridad en el centro de datos.
 - Deberá proveer la capacidad de hacer zoom sobre la información, conocido como drill-down hacia métricas específicas que hayan causado el problema.
- La Solución deberá ser capaz de obtener datos disponibles para cada intervalo de tiempo seleccionado mostrando al menos las siguientes variables:
 - Ingesta recibida.
 - Tipos de eventos y anomalías de la ingesta recibida y normalizada.
 - Tráfico por dirección IP asociado con el puerto, aplicación.
 - Tráfico por puerto asociado con el protocolo IP.
 - Conversaciones entre estaciones IP.
 - Mostrar eventos de alta fidelidad.
- El tiempo máximo de respuesta a problemas de comunicación y/o averías dependientes de los equipos instalados por el proveedor en el INMP, no debe exceder las 04 horas, desde la comunicación de la falla por parte del INMP, al centro de soporte del Postor (vía telefónica, correo electrónico), hasta la solución del problema, incluyendo cambio de equipos y la restauración del servicio.
- El tiempo máximo de respuesta a fallas del servicio, debido a problemas de configuración, enlace y/o comunicación, plazo máximo será de 04 horas de incidentes crítico, a partir del reporte de la falla por el usuario (INMP), al centro de soporte del Postor (vía telefónica, correo electrónico), hasta la solución del problema y restauración del servicio.
- Todos los recursos que se requieran para solucionar la avería serán sin costo alguno para el INMP.

GARANTÍA COMERCIAL

- Se requiere que se brinde una garantía comercial de doce (12) meses del sistema / plataforma adquirida. La garantía debe ser otorgada por el ~~poster~~ **contratista** y confirmada por el fabricante o el representante de

la marca en el país, de las siguientes tecnologías incluidas en el proceso, Esta garantía proporcionará una garantía formal de que la solución de seguridad cumple con los estándares de calidad y que el fabricante ofrece soporte técnico y actualizaciones durante el periodo solicitado:

- SERVICIO DE INTERNET IP
- SEGURIDAD INFORMATICA PERIMETRAL (NEXT GENERATION FIREWALL)
- FILTRO DE SEGURIDAD PARA CORREO ELECTRONICO (ANTISPAM)
- SOLUCIÓN DE PROTECCION DE APLICACIONES WEB
- SERVICIO DE TELEFONIA MOVIL

Esta garantía proporcionará una garantía formal de que la solución de seguridad cumple con los estándares de calidad y que el fabricante ofrece soporte técnico y actualizaciones durante el periodo solicitado.

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

ESPECIALISTAS EN CIBERSEGURIDAD

- Dos (02) ingenieros titulados ~~y/o bachiller~~ en Ingeniería Electrónica, o en Telecomunicaciones, ~~Ingeniería de Seguridad y Auditoría Informática, Ingeniería de Sistemas y/o Computación, Ingeniería de Sistemas e Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones y/o Redes, Ingeniería de Ciencias de la Computación y/o Redes, Ingeniería de Computación y/o Sistemas, Ingeniería Informática y de Sistemas, Ingeniería de Seguridad Informática, e Ingeniería de Computación e Informática en cada solución ofertada para el total de la solución propuesta.~~
- Deberá contar con ~~al menos dos (02) certificaciones técnicas~~ del fabricante de la solución ofertada (NGFW o PROTECCION DE APLICACIONES WEB o FILTRO DE SEGURIDAD DE CORREO ELECTRONICO)
- Deberá contar con certificación técnica de solución de CYBERSOC ofertada.
- Deberá contar con experiencia mínima de ~~tres (03) años~~ ~~dos (02) años~~ en la implementación y/o soporte de soluciones ofertada.

PLAN DE IMPLEMENTACION, PLAZO DE ENTREGA DE EQUIPOS E IMPLEMENTACION DEL SERVICIO.

- El ~~Postor~~ ~~contratista~~ deberá presentar formalmente un plan de implementación del servicio a la Oficina de Estadística e Informática como máximo 10 días calendarios después de realizada la firma de contrato; el mismo que estará sujeto a revisión y aprobación por parte de la Oficina de Estadística e Informática en el plazo no mayor a dos (02) días hábiles, contemplando el total de actividades de la implementación del servicio.
- El plazo de entrega de equipos e implementación del servicio será de hasta (60) días calendario, contados a partir del día siguiente de la firma del contrato.
- El CONTRATISTA deberá habilitar uno de los enlaces principal o respaldo hasta el día 60 de la prestación del servicio a fin de que la entidad no vea afectada su operación por la transición de operadores.
- El inicio formal del servicio de Internet se contabilizará una vez realizado la Implementación y emitida la conformidad de implementación por parte de la Oficina de Estadística e Informática.
- El postor debe incluir en su oferta todo lo necesario para la correcta provisión del servicio, ~~incluyendo las mejoras de los términos de referencia.~~
- El postor podrá realizar una visita previa para verificar el ambiente o ambientes donde estarán implementados los equipos.
- El postor deberá considerar en su propuesta; ductos, canalización, picado, resane y otras obras civiles que deberán ser realizadas por el proveedor del servicio.

MECANISMOS DE SUPERVISIÓN

- El **Postor contratista** y el personal responsable del INMP, verificarán el cumplimiento de los términos de referencia, la instalación y configuración de los equipos, plan de trabajo y pruebas del servicio para el otorgamiento y firma del Acta de Conformidad de Implementación correspondiente.
- La omisión de algún recurso que se requiera para la instalación del servicio o pruebas, según lo ofertado, será provisto por el postor sin cargo alguno para el INMP.
- Cualquier incumplimiento de los términos de referencia notificado por el personal del INMP al postor, durante la implementación, deberá ser subsanado por éste, sin cargo alguno, teniendo como plazo mínimo de dos (2) ni mayor de ocho (8) días para subsanar las Observaciones durante la implementación a partir de su notificación.

ENTREGABLES DEL SERVICIO E IMPLEMENTACIÓN.

- Información y documentación descriptiva de las configuraciones y políticas de acceso referidas al servicio provisto.
- Diseño del diagrama de flujo del servicio de soporte definido entre el INMP y el POSTOR.
- El soporte Off Site será 7 x 24 y con un tiempo de tolerancia máxima para averías críticas por parte del proveedor de 04 horas luego de efectuado el registro del incidente de acuerdo al Diagrama de Flujo del servicio de soporte.
- Matriz de escalamiento indicando el soporte que estará a cargo de captar las atenciones por avería y/o requerimientos del INMP.
- El proveedor deberá garantizar en toda circunstancia la posibilidad de escalamiento del servicio con el fabricante para una oportuna solución de los eventos presentados de 06 horas luego de efectuado el registro.
- La administración de la solución instalada es por parte del postor el cual debe realizar todos los cambios en las configuraciones y/o reglas que el INMP solicite de lunes a viernes de 8:00 a.m. a 6:30 p.m. y sábados de 8:00 a 2:00 pm sin costo adicional y sin límite de solicitudes por el plazo del contrato.

DEL PROVEEDOR.

- El contratista deberá proveer, instalar y configurar los equipos y/o software de seguridad informática necesarios para la prestación de los servicios con óptima calidad.
- Proporcionar, con el correspondiente respaldo del fabricante, los servicios de garantía de hardware, mantenimiento software y soporte técnico remoto para la solución propuesta de seguridad perimetral – firewalls por el periodo de un (01) año (se adjuntará carta del fabricante y/o distribuidor autorizado, certificando el requerimiento), se acreditará como parte de los entregables de implementación).
- El contratista deberá trabajar de manera conjunta con el personal técnico de la Oficina de Sistemas del instituto nacional materno perinatal que supervisarán la implementación de los servicios correspondientes. La Oficina de Sistemas nombrará un responsable Técnico del proyecto, quien será el encargado de las coordinaciones con el Personal técnico del contratista, de modo que la implementación se ejecute en forma coordinada.
- El contratista deberá proveer, instalar y configurar los equipos y/o software de seguridad informática necesarios para la prestación del servicio con óptima calidad. La entidad facilitará entregará al contratista la arquitectura de la red para la implementación de la solución, así como proveer las facilidades siguientes:
 - Espacio en el rack del centro de datos, necesarios para la implementación de todos los equipos que formarán parte del servicio, incluyendo los dos (02) equipos para seguridad perimetral y los dos (02) routers.
 - Mínimo 2 puertos Ethernet
 - Energía eléctrica estabilizada (pozo a tierra a menos de 5 Ohmios)
 - Bandejas
 - Patch Cord
 - Switch (de ser el caso)
 - Facilidad de acceso al área de trabajo, así como las facilidades técnicas para la instalación.
 - Otros necesarios para la operación del equipamiento
- El tiempo de entrega e implementación no será mayor a sesenta (60) días calendarios posteriores a la firma del contrato.

- Si al momento de la implementación, los equipos ofertados por el contratista en su propuesta técnica no se encuentren disponibles en el mercado, deberá reemplazarlos con equipos de iguales o mayores prestaciones, adjuntando el correspondiente sustento técnico documentado.
- Presentar para la etapa de implementación una relación descriptiva de los componentes proporcionados, incluyendo sus códigos comerciales (Sku).
- El contratista deberá considerar un equipo tipo spare (de repuesto) igual o de mejores características que el equipamiento ROUTER implementado en la red del instituto materno perinatal, el que servirá para reemplazar el equipo principal en caso este presente fallas que impliquen la pérdida de servicio. Esto será validado a través de una declaración jurada.
- El Postor deberá contar con el siguiente personal para el desarrollo del presente proyecto:

CONFIDENCIALIDAD DE LA INFORMACIÓN

- Toda información del Instituto Materno Nacional Perinatal a la que tenga acceso el contratista, y su personal, es estrictamente confidencial, debiendo mantener las reservas del caso y no transmitirla bajo ninguna circunstancia.
- El Contratista se compromete a mantener en reserva, y no revelar a terceros sin previa conformidad escrita de la Municipalidad de Piura, toda información que le sea suministrada por este último, excepto en cuanto resulte estrictamente necesario para el cumplimiento del Contrato, y que restringirá la revelación de dicha información sólo a sus empleados y subcontratistas, sobre la base de "necesidad de conocer".
- La Entidad identificará la información que deba ser tratada como confidencial al momento de su revelación al contratista, ya que no toda la documentación entregada tiene dicha naturaleza.
- La información que sea pública o conocida por el contratista, sin obligación de confidencialidad, no estará sujeta a la obligación de confidencialidad.
- La obligación de confidencialidad se mantendrá vigente durante todo el tiempo de contrato, lo que guarda relación con la Ley de transparencia y acceso a la información pública

7. Plazo de duración del servicio:

- EL PROVEEDOR deberá proporcionar el **Servicio de Internet IP**, por el período de un (01) año, dicho inicio será contabilizado desde el día que se firma el acta de conformidad.

8. Forma de Pago.

- El pago se realizara de forma mensual, previo informe del proveedor del servicio indicando el cumplimiento del servicio y la conformidad emitida por el Director de la Oficina de Estadística e Informática y responsable del Equipo Funcional de Informática del INMP.

9. Penalidades.

PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

- 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:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;

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

OTRAS PENALIDADES

La Entidad puede establecer penalidades distintas a la precedente, siempre y cuando sean objetivas, razonables, congruentes y proporcionales con el objeto de la contratación.

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.

10. Supervisión y Conformidad de la Contratación.

- Dr. Juan Torres Osorio – jefe de la Oficina de Estadística e Informática.
- Ing. Noe Rodriguez Hilario – jefe de Equipo Funcional de Informática.

3.2. 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 por la Ley general de telecomunicaciones, como empresa proveedora de telecomunicaciones. El Postor deberá pertenecer al NAP (NETWORK Access Point) — Peru activo y operativo. <p><u>Acreditación:</u></p> <ul style="list-style-type: none"> Copia simple de la resolución del ministerio de transportes y comunicaciones; o copia del certificado de registro de empresas prestadoras de servicios de valor añadido expedido por dirección general de concesiones en comunicaciones del MTC; o impresión simple del registro de empresas prestadoras de servicios de valor añadido publicadas en la página web MTC. Constancia expedida por el mismo NAP PERU o la captura de pantalla de la página web del NAP PERU, donde se indique que el postor es asociado de la referida institución.

B	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	CALIFICACIONES DEL PERSONAL CLAVE
B.1.1	FORMACIÓN ACADÉMICA
	<p><u>Requisitos:</u></p> <p>UN (01) JEFE DE PROYECTO</p> <p>Ingeniero de Telecomunicaciones o Electrónico o Sistemas o Ingeniería Informática o Ingeniería de Sistemas o Computación y Sistemas o Industrial o y Computación e Informática titulado, colegiado y habilitado al momento de la generación de la propuesta.</p> <p>DOS (02) ESPECIALISTAS EN CIBERSEGURIDAD</p> <p>Dos (02) ingenieros titulados y/o bachiller en Ingeniería Electrónica, o en Telecomunicaciones, Ingeniería de Seguridad y Auditoría Informática, Ingeniería de Sistemas y/o Computación, Ingeniería de Sistemas e Informática, Ingeniería Electrónica, Ingeniería de Telecomunicaciones y/o Redes, Ingeniería de Ciencias de la Computación y/o Redes, Ingeniería de Computación y/o Sistemas, Ingeniería Informática y de Sistemas, Ingeniería de Seguridad Informática, e Ingeniería de Computación e Informática en cada solución ofertada para el total de la solución propuesta.</p> <p><u>Acreditación:</u></p>

	<p>El CONSIGNAR EL GRADO O TÍTULO PROFESIONAL REQUERIDO 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: https://titulosinstitutos.minedu.gob.pe/, según corresponda.</p> <p>En caso CONSIGNAR EL GRADO O 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>
B.1.2	CAPACITACIÓN
	<p><u>Requisitos:</u></p> <p>UN (01) JEFE DE PROYECTO</p> <ul style="list-style-type: none"> – Deberá contar con capacitación mínima de 24 horas en gestión de proyectos y/o certificación en gestión de proyectos (PMP) – Certificación ITIL (opcional) <p>DOS (02) ESPECIALISTAS EN CIBERSEGURIDAD</p> <ul style="list-style-type: none"> – Deberá contar con certificación técnica del fabricante en las soluciones ofertadas (NGFW, Protección de Aplicaciones Web y Filtro de Seguridad de Correo Electrónico). <p><u>Acreditación:</u></p> <p>Se acreditará con copia simple de certificados emitidos por el fabricante. No se aceptarán documentos emitidos por el postor.</p>
B.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>UN (01) JEFE DE PROYECTO</p> <ul style="list-style-type: none"> – Experiencia de más de dos (02) años como Jefe de Proyectos en Seguridad Perimetral y/o Protección de Correo Electrónico y/o Prevención de Fuga de Información y/o implementación de proyectos de internet. <p>DOS (02) ESPECIALISTAS EN CIBERSEGURIDAD</p> <ul style="list-style-type: none"> – Experiencia mínima de tres (03) años dos (02) años en la implementación y/o soporte de soluciones ofertada. <p><u>Acreditación:</u></p> <p>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.</p>
C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 500,000.00 (QUINIENTOS MIL CON 00/100 SOLES), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/. 119,000.00 (CIENTO DIECINUEVE MIL CON 00/100 SOLES), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores</p>

	<p>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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran servicios similares a los siguientes SERVICIO DE INTERNET Y/O INTERCONEXIÓN Y/O COMUNICACIÓN MEDIANTE FIBRA ÓPTICA, SERVICIO DE ANCHO DE BANDA, SERVICIO DE INTERNET, SERVICIO DE ENLACE DEDICADO, ACCESO A INTERNET, SERVICIO DE INTERNET DE BANDA ANCHA.</p> <p>Se consideran servicios similares a los siguientes SERVICIO DE ANCHO DE BANDA, SERVICIO DE INTERNET, SERVICIO DE ENLACE DEDICADO, ACCESO A INTERNET, SERVICIO DE INTERNET DE BANDA ANCHA, servicio de acceso a internet y/o servicio de internet a nivel nacional y/o servicio de Internet Dedicado y Enlace de Datos</p> <p><u>Acreditación:</u></p> <p>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^[1], correspondientes a un máximo de veinte (20) contrataciones.</p> <p>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 según bases referido a la Experiencia del Postor en la Especialidad</p> <p>En 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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo según bases.</p>
--	--

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

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".

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 según bases 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".*

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></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>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= Oferta P_i= Puntaje de la oferta a evaluar O_i=Precio i O_m= Precio de la oferta más baja PMP=Puntaje máximo del precio</p> <p style="text-align: right;">100 puntos</p>
PUNTAJE TOTAL	100 puntos¹³

¹³ 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA 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 PAGO¹⁴

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 dentro de los diez (10) días calendario siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el

¹⁴ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

contrato para ello, bajo responsabilidad del funcionario competente.

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE 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.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

De conformidad con el artículo 152 del Reglamento, no se constituirá garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias, en contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00). Dicha excepción también aplica a 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 no supere el monto señalado anteriormente.

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD puede solicitar la ejecución de las garantías cuando EL CONTRATISTA no las hubiere renovado antes de la fecha de su vencimiento, conforme a lo dispuesto en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

Importante para la Entidad

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

CLÁUSULA NOVENA: ADELANTO DIRECTO

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

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

LA ENTIDAD debe entregar el monto solicitado dentro de [CONSIGNAR EL PLAZO] siguientes a la presentación de la solicitud del contratista."

Incorporar a las bases o eliminar, según corresponda.

CLÁUSULA DÉCIMA: 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 CONTROVERSIAS¹⁵

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

¹⁵ 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).

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 Digitales¹⁶.

¹⁶ 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 ¹⁷	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 servicios¹⁸

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.

¹⁷ 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. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹⁸ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 ¹⁹		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²⁰		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²¹		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:

¹⁹ 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. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

²⁰ Ibidem.

²¹ Ibidem.

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 servicios²²

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.

²² Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 EL 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 N° 4**DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO**

Señores

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]**ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP**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 de [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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **ADJUDICACIÓN SIMPLIFICADA 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] [%]²³

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁴

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²⁵

²³ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁴ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁵ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

[CONSIGNAR CIUDAD Y FECHA]

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

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

Importante

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

Importante para la Entidad

En caso de la prestación de servicios bajo el sistema a precios unitarios 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

Presente.-

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

CONCEPTO	CANTIDAD	PRECIO UNITARIO	PRECIO TOTAL
TOTAL			

El precio de la oferta **[CONSIGNAR LA MONEDA DE LA CONVOCATORIA]** incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del 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

- En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- 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

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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del 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.*
- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *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

En caso de la prestación de servicios bajo el esquema mixto de suma alzada y precios unitarios 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

Presente.-

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

OFERTA A PRECIOS UNITARIOS DE LOS COMPONENTES SIGUIENTES:

CONCEPTO	CANTIDAD	PRECIO UNITARIO	COSTO
Monto del componente a precios unitarios			

OFERTA A SUMA ALZADA DE LOS COMPONENTES SIGUIENTES:

CONCEPTO	PRECIO TOTAL
Monto del componente a suma alzada	

Monto total de la oferta	
--------------------------	--

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 en su oferta los precios unitarios de los componentes previstos para este sistema en el presente anexo y por un monto fijo integral de los componentes previstos a suma alzada.*
- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas

Importante para la Entidad

En caso de la prestación de servicios bajo el sistema en base a porcentajes 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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

CONCEPTO	OFERTA
Porcentaje ofertado ²⁶	%
Monto Total Ofertado	

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

- En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- 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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas

²⁶ De conformidad con la Opinión N° 202-2016/DTN, corresponde al porcentaje del monto total a cobrar o recuperar.

Importante para la Entidad

En caso de la prestación de servicios bajo el sistema en base a honorario fijo y comisión de éxito 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

Presente.-

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

CONCEPTO	MONTO
(A) Honorario Fijo	
(B) Comisión de éxito ²⁷	
Precio de la Oferta (A) + (B)	

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

- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- *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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas

²⁷ De conformidad con la Opinión N° 011-2017/DTN "El postor formula su oferta contemplando un monto fijo y un monto adicional como incentivo que debe pagársele en caso consiga el resultado esperado".

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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 empresa²⁸ 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.

²⁸ En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquéllas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]
ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP
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 ²⁹	FECHA DE LA CONFORMIDAD DE SER EL CASO ³⁰	EXPERIENCIA PROVENIENTE ³¹ DE:	MONEDA	IMPORTE ³²	TIPO DE CAMBIO VENTA ³³	MONTO FACTURADO ACUMULADO ³⁴
1										
2										
3										
4										

²⁹ 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.

³⁰ 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.

³¹ 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".

³² Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

³³ 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.

³⁴ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²⁹	FECHA DE LA CONFORMIDAD DE SER EL CASO ³⁰	EXPERIENCIA PROVENIENTE ³¹ DE:	MONEDA	IMPORTE ³²	TIPO DE CAMBIO VENTA ³³	MONTO FACTURADO ACUMULADO ³⁴
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

**[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN,
SEGÚN CORRESPONDA]**

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>.

También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

Importante para la Entidad

En el caso de contratación de servicios en general que se presten fuera de la provincia de Lima y Callao cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00) o el procedimiento de selección según relación de ítem no supere dicho monto, se debe considerar 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 órgano encargado de las contrataciones o comité de selección, según corresponda, 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 órgano encargado de las contrataciones o comité de selección, según corresponda, 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.*

ANEXO N° 11

SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA

Señores

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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 órgano encargado de las contrataciones o 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

[CONSIGNAR ÓRGANO ENCARGADO DE LAS CONTRATACIONES O COMITÉ DE SELECCIÓN, SEGÚN CORRESPONDA]

ADJUDICACIÓN SIMPLIFICADA N° 008-2024-INMP

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.