

BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE BIENES

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



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

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el 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 2019, junio 2019, diciembre 2019, julio 2020, julio y diciembre 2021, junio y octubre de 2022

**BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA
PARA LA CONTRATACIÓN DE BIENES**

**ADJUDICACIÓN SIMPLIFICADA N°
ADJUDICACIÓN SIMPLIFICADA N° 06-2023-SIMA
SEGUNDA CONVOCATORIA**

**CONTRATACIÓN DE BIENES
ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL
NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN
ALTA DISPONIBILIDAD**

PAC 15

2023

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.mp.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 funcionales y condiciones de las Especificaciones Técnicas, 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.

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.

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 compra, 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 compra, 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 compra. En caso la Entidad perfeccione el contrato con la recepción de la orden de compra 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 accesorio, 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.

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

- 1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).*
- 2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.*
- 3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.*
- 4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.*

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

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

Advertencia

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

Advertencia

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : Servicios Industriales de la Marina
RUC N° : 20100003351
Domicilio legal : Av. Contralmirante Mora 1102 Callao
Teléfono: : 413-1100 anexo 8029
Correo electrónico: : rcondemarin@simacom.pe; rmeregildo@simacom.pe; alburqueque@simacom.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de Adquisición de Solución de Seguridad perimetral Next Generation firewall y filtro de contenido en alta disponibilidad,

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Solicitud de Aprobación de expediente de Contratación Desarrollo Propio N° 001-AS-06-2023 SIMA - Primera Convocatoria del 22 de septiembre del 2023, aprobado con fecha 22 de septiembre del 2023.

1.4. FUENTE DE FINANCIAMIENTO

Recursos propios

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. MODALIDAD DE EJECUCIÓN

Llave en mano, en concordancia con lo establecido en el expediente de contratación.

1.7. DISTRIBUCIÓN DE LA BUENA PRO

No es posible distribuir la buena pro, de acuerdo con lo establecido en el expediente de contratación respectivo.

1.8. ALCANCES DEL REQUERIMIENTO

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

1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán en el plazo en el siguiente plazo:

a. PLAZO ENTREGA DEL BIEN:

Los bienes materia de la presente convocatoria se entregarán en el plazo en el siguiente plazo:

b.1 Plazo de entrega de los bienes.

Los bienes y/o licenciamiento serán entregados en un plazo no mayor a TREINTA (30) días calendario, contados a partir del día siguiente del perfeccionamiento del contrato.

b.2 Plazo de instalación, configuración y puesta en funcionamiento.

La instalación, configuración y puesta en producción será en un plazo no mayor a CINCO (5) días calendario, contados a partir de la entrega de los bienes y/o licencias.

En concordancia con lo establecido en el expediente de contratación.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar el monto de OCHO CON 40/100 SOLES (S/. 8.00) en la Cta. Cte. N° 0661-61-100000584 del Banco Continental y con el voucher recabar un ejemplar de las bases en la mesa de partes del Departamento de Contrataciones, sito en Av. Contralmirante Mora N° 1102 Callao.

Importante

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

1.11. BASE LEGAL

- Ley N° 31638 Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública, aprobado por D.S. N° 043-2003-PCM.
- Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General, aprobado por D.S. N° 004-2019-JUS.
- Texto Único Ordenado de la Ley N° 30225 - Ley de Contrataciones del Estado, aprobado por D.S. N° 082-2019-EF, en adelante la Ley.
- Ley de Contrataciones del Estado N° 30225, aprobado por D.S. N° 082-2019-EF

- Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado, aprobado mediante Decreto Supremo N° 344-2018-EF, y dictan otras disposiciones DECRETO SUPREMO N° 162-2021-EF
- Ley N° 27073 Ley de Servicios Industriales de la Marina S.A. SIMA-PERÚ S.A., cualquier otra disposición vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado.
- D.S. N° 103-2020-EF "Decreto Supremo que establece disposiciones reglamentarias para la tramitación de los procedimientos de selección que se reinicien en el marco del Texto Único Ordenado de la Ley N° 30225".
- 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.
- Directivas y Opiniones del OSCE.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos², la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

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

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

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

- e) Deberá indicar marca y modelo de los equipos propuestos, así como presentar la documentación oficial del fabricante (hoja técnica, brochure, datasheet) en el cual deberá de indicar el numero de folio que sustente las características técnicas en el numeral 5.3 de las Especificaciones Técnicas, de acuerdo al Anexo N° 12 de las bases.

DESCRIPCIÓN	MARCA	MODELO
SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD		

- f) El postor deberá acreditar para admisión de la oferta, ser representante o distribuidor autorizado de la marca ofertada con la presentación de la carta del fabricante.
- g) Declaración jurada de plazo de entrega. (Anexo N° 4)⁴
- h) 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)
- i) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el **Anexo N° 6**.

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

Importante

El 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.

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 Discapacidad⁵.
- b) Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa (Anexo N° 10).

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

⁵ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

- c) Incorporar en la oferta los documentos que acreditan los **"Factores de Evaluación"** establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.

Advertencia

El órgano encargado de las contrataciones o el comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".

2.3. 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 : 0661-61-100000584
Banco : Continental
N° CCI⁶ : 0011-0661-0100000584-61

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 – PIDE⁷ 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

⁷ 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/>

- plazo mediante medios electrónicos de comunicación⁸ (**Anexo N° 11**).
- i) Detalle de los precios unitarios del precio ofertado⁹.
- j) Detalle del precio de la oferta de cada uno de los bienes que conforman el paquete¹⁰.

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 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 Haya¹¹.
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

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 Mesa de Partes del Departamento de Contrataciones – Av. Contralmirante Mora N° 1102 – Callao

⁸ En tanto se implemente la funcionalidad en el SEACE, de conformidad con la Primera Disposición Complementaria Transitoria del Decreto Supremo N° 234-2022-EF.

⁹ Incluir solo en caso de la contratación bajo el sistema a suma alzada.

¹⁰ Incluir solo en caso de contrataciones por paquete.

¹¹ Según lo previsto en la Opinión N° 009-2016/DTN.

Importante para la Entidad

- *En el caso de procedimientos de selección cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), siempre que se haya optado por perfeccionar el contrato con la recepción de una orden de compra, debe sustituirse por esta disposición:*

"El contrato se perfecciona con la notificación de la orden de compra. 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 [INDICAR LUGAR Y DIRECCIÓN EXACTA DONDE DEBE DIRIGIRSE EL POSTOR GANADOR]."

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

2.6. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en ÚNICO PAGO.

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

- Garantía Comercial (De acuerdo al punto 5.5 de las EE.TT. en las Bases)
- Informe del funcionario responsable de la Oficina de Tecnología de la Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada;
- Comprobante de pago.

Dicha documentación se debe presentar en la Oficina de Gestión Integrada, sito en Av. Contralmirante Mora 1102 Callao.

CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. ESPECIFICACIONES TÉCNICAS



ESPECIFICACIONES TÉCNICAS PARA LAS ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD

1 DENOMINACIÓN DE LA CONTRATACIÓN.

Adquisición de solución de seguridad perimetral next generation firewall y filtro de contenido en alta disponibilidad.

2 FINALIDAD PÚBLICA.

Realizar la adquisición de una solución de seguridad para la protección del perímetro de red ante posibles ataques cibernéticos, controlando el tráfico saliente y entrante no autorizado a la red informática del SIMA PERÚ.

3 ANTECEDENTES.

El SIMA PERÚ S.A. como parte de su infraestructura de red, posee un parque informático compuesto por:

- Servidores los cuales soportan los principales servicios y sistemas de informáticos.
- Estaciones de trabajo de usuarios finales.

En ese escenario, el servicio de acceso a internet es imprescindible para el cumplimiento de las funciones y correcto funcionamiento de los sistemas de información, sin embargo, también es una fuente de amenazas informáticas que ponen en riesgo la red corporativa del SIMA PERÚ S.A.

Actualmente el SIMA PERÚ, para mantener dicha funcionalidad, cuenta con un equipo de seguridad informática firewall y filtro de contenido, ubicado físicamente en el centro de datos, el cual se encuentra conectado después del módem router del proveedor de servicio de internet (ISP), con la finalidad de cumplir las siguientes funciones:

- Filtrar todo el tráfico entrante y saliente de red, bloqueando accesos no autorizados de acuerdo con las políticas de seguridad preestablecidas.
- Controlar el tráfico de navegación desde la red privada LAN hacia internet.

Cabe mencionar que, según lo indicado por el fabricante, el equipo de seguridad con el que cuenta actualmente el SIMA PERÚ S.A. se encuentra discontinuado, por lo cual ya no cuenta con renovación de licenciamiento y soporte especializado, así mismo dicha suscripción vence 13/12/2023, por lo que requiere adquirir una nueva solución de seguridad, el mismo que incluya equipos con mejores prestaciones y funcionalidades. Así mismo se requiere contar con un centro de servicio de soporte local que realice un constante seguimiento, análisis, monitoreo y efectúe acciones correctivas ante estas nuevas amenazas de acceso a internet.

4 OBJETIVOS DE LA CONTRATACIÓN.

4.1. OBJETIVO GENERAL.

Contar con una solución de seguridad perimetral de filtro de contenido y control de navegación web de forma segura, controlada y monitoreada,



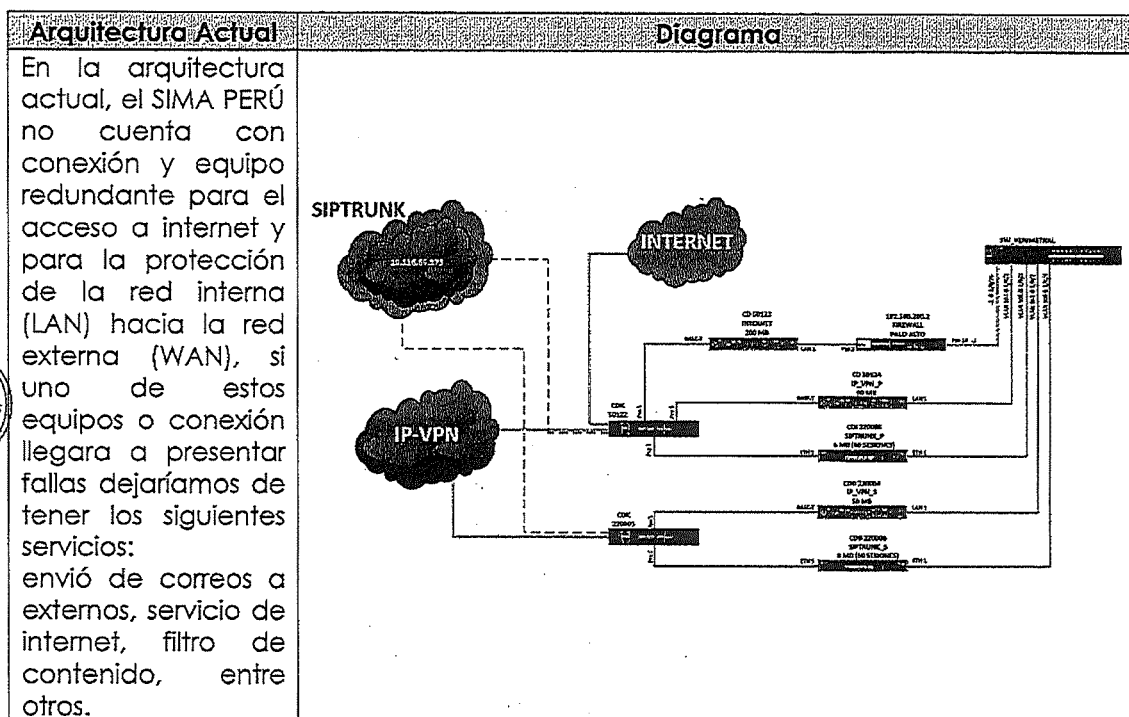
de manera que se reduzca el riesgo de ataques informáticos que impacten en la disponibilidad, confidencialidad e integridad de la información y los sistemas informáticos.

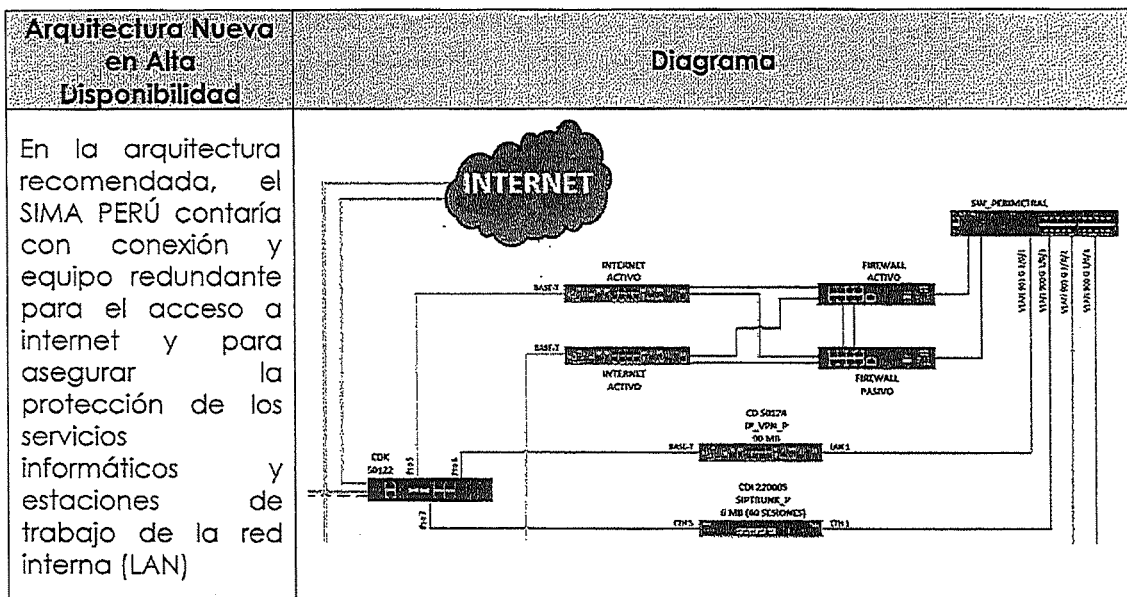
4.2. OBJETIVOS ESPECÍFICOS.

- Proteger el perímetro de red antes posibles ataques cibernéticos desde la red WAN (Internet).
- Filtrar y monitorear todo el tráfico de red entrante y saliente no autorizado.
- Mantener la disponibilidad de los sistemas de informáticos.
- Minimizar los riesgos de seguridad informática del SIMA PERÚ S.A.
- Contar con el soporte de un centro de operaciones de seguridad (SOC) el cual mantenga una constante vigilancia ante nuevas amenazas de acceso a internet.

5 ALCANCE Y DESCRIPCIÓN DE LOS BIENES A CONTRATAR.

5.1 DESCRIPCIÓN DE LOS BIENES A CONTRATAR.





N°	DESCRIPCION
1	SOLUCIÓN DE SEGURIDAD PERIMETRAL NEXT GENERATION FIREWALL Y FILTRO DE CONTENIDO EN ALTA DISPONIBILIDAD

5.2 CARACTERISTICAS GENERALES.

5.2.1 NEXT GENERATION FIREWALL PARA LA SEDE PRINCIPAL EN ALTA DISPONIBILIDAD.

- Se requiere de una solución de protección de redes con características de Next Generation Firewall (NGFW) en alta disponibilidad para la seguridad de la red empresarial.
- La solución tiene que ser ofrecida en alta disponibilidad, es decir por lo menos DOS (02) equipos appliances con las mismas características mínimas mencionadas en estas especificaciones.
- El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes.
- El fabricante debe poseer todos los componentes necesarios para adoptar una arquitectura de Zero Trust.
- El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
- La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante



como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.

- h. Los equipos Next Generation Firewall (NGFW) deberán tener soporte vigente de fábrica durante la ejecución del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware. (documento de compromiso).
- i. Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde el SIMA PERÚ tendrá la potestad de dar seguimiento a los casos abiertos por el proveedor.
- j. El soporte del fabricante deberá incluir el servicio de investigación de amenazas en caso exista una sospecha de ataque.
- k. No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde.

5.3 CARACTERISTICAS TÉCNICAS.

5.3.1 CARACTERISTICAS DE RENDIMIENTO PARA FIREWALL.

- a. Throughput de Next Generation Firewall de 4.3 Gbps (mínimo) medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.
- b. Throughput de Prevención de Amenazas de 2 Gbps (mínimo) medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: control de aplicaciones, sistema de prevención de intrusos (IPS), seguridad del tráfico DNS, antivirus/antimalware de red, antispymware/antiBot, sandboxing, filtro de archivos y logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.





- c. El equipo debe soportar como mínimo 390.000 sesiones simultáneas y 70.000 sesiones por segundo, medidos con paquetes HTTP de 1 byte.
- d. Debe contar con fuente de poder redundante.
- e. Disco interno de 120 GB o superior.
- f. Mínimo OCHO (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red.
- g. La plataforma deberá contar con al menos UN (01) puerto de gestión fuera de banda dedicada para la gestión del equipo.
- h. Deberá tener CPU dedicado para tareas de gestión del equipo, de manera independiente a los recursos de CPU para el procesamiento del tráfico. Esta arquitectura podrá estar integrada dentro del NGFW, o en caso no lo soporte, se podrán incluir consolas de gestión externas al NGFW.
- i. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- j. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- k. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPsec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.
- l. 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.
- m. 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.
- n. La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de firewall, IDS e IPS.
- o. 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).
- p. 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.
- q. 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.



- r. Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.

5.3.2 FUNCIONALIDADES DE FIREWALL.

- a. 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).
- b. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- c. 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).
- d. Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- e. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- f. 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.
- g. Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.
- h. 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.

5.3.3 DESCIFRADO DE TRÁFICO SSL/TLS.

- a. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
- b. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
- c. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- d. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
- e. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS.



- f. Debe soportar certificados que utilice subject alternative name (SAN) y Server Name Indication (SNI).
- g. Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio.
- h. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
- i. Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.
- j. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

5.3.4 CONTROL DE APLICACIONES.

- a. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- b. Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.
- c. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- d. 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.
- e. Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.
- f. 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.
- g. Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.
 - h. 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.
 - i. El módulo de aprendizaje deberá ser específico por cada política de seguridad.
 - j. 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.
 - k. 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.

5.3.5 PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS).

- a. 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.
- b. Debe ser posible utilizar SYN Cookies como medida de defensa.
- c. 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).
- d. 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.
- e. Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route.
- f. 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.



5.3.6 PREVENCION DE AMENAZAS.

- a. La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- b. 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.
- c. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- d. La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.
- e. 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.
- f. Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS.
- g. El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.
- h. El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.
- i. 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.
- j. 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.
- k. 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.
- l. 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.



5.3.7 ANALISIS DE MALWARE DE DÍA CERO.

- a. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- b. La plataforma de Sandboxing debe ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.
- c. También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.
- d. 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.
- e. 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.
- f. Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines).
- g. Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- h. El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.
- i. 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.
- j. El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.
- k. 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.
- l. Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- m. Debe permitir al administrador la descarga del archivo original analizado por el sandbox.



- n. 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.
- o. Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.
- p. 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.
- q. La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

5.3.8 PROTECCION AVANZADA DE DNS.

- a. 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.
- b. 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.
- c. 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.
- d. Deberá soportar el manejo excepciones para poder mitigar los falsos positivos.
- e. 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.
- f. 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.
- g. En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA.

5.3.9 IDENTIFICACION DE USUARIOS.

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



- b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- c. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
- d. Debe disponer de un servicio en nube o onpremise que extraiga automáticamente la información del usuario grupos de usuario de varios IDPs y proveedores de SSO como Azure AD, okta, Google identity y PingID y la ponga a disposición de los NGFW para ser incluidos en la política de seguridad.
- e. Debe disponer de un servicio en nube o onpremise que simplifique la autenticación SAML de usuarios, que actúe como Service Provider único frente a IDPs o proveedores de SSO.
- f. Debe disponer de un servicio en nube o onpremise que almacene todos los grupos disponibles del Active Directory, los filtre y ponga a disposición únicamente los grupos necesarios que el NGFW utilice en la política de seguridad.
- g. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- h. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
- i. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- j. Debe permitir la definición de grupos dinámicos de usuarios.

5.3.10 FILTRO DE CONTENIDO WEB.

- a. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.
- b. Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs.
- c. 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.
- d. 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.



- e. Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.
- f. Debe permitir la creación de categorías personalizadas.
- g. Debe permitir la personalización de la página de bloqueo.
- h. Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.
- i. Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet.
- j. Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.
- k. 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.

5.3.11 FUNCIONALIDADES DE OPTIMIZACIÓN.

- a. Se debe proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Firewall implementado.
- b. Esta herramienta debe funcionar en línea y de manera automática. Es decir, luego de cada configuración realizada en el Firewall, debe mostrar los cambios realizados.
- c. Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.
- d. Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.
- e. Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio.
- f. La herramienta de evaluación de buenas prácticas debe mostrar al menos lo siguiente: nivel de adopción del control de aplicaciones, visibilidad de usuarios, configuraciones correctas de los perfiles de seguridad (antivirus, IPS, sandboxing), hardening de la plataforma.
- g. La herramienta de evaluación de buenas prácticas debe ser específica para la configuración de firewall implementado, no se aceptarán guías de usuarios genéricas.
- h. Debe contar con un dashboard que muestre la salud del equipo. Asimismo, si apareciera una falla debe enviar un correo de manera automática.



5.3.12 CONSOLA DE ADMINISTRACIÓN Y MONITOREO.

- a. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del NGFW, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante.
- b. Permitir exportar las reglas de seguridad en formato CSV y PDF.
- c. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- d. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- e. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino).
- f. Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de sólo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- g. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- h. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- i. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
- j. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- k. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- l. Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración.



- m. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- n. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- o. Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL.
- p. Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS.
- q. La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.

5.4 SOPORTE TÉCNICO.

- a. Durante el período de garantía comercial, debe contar con un centro de operaciones de seguridad (SOC) 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.
- b. 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.
- c. El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio en SIMA, así como a la pérdida de la calidad o degradación de este. A todo ello se le denominará "falla".
- d. El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará "requerimiento".
- e. El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.
- f. Deberá brindar soporte técnico in situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ





se dará en caso de fallas que no puedan ser solucionados de manera remota.

- g. El postor deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca.
- h. El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del postor, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.

5.5 GARANTIA COMERCIAL.

Deberá brindar una garantía comercial de DOCE (12) meses por el hardware de la solución adquirida. La garantía debe ser otorgada por el postor y confirmada por el fabricante o el representante de la marca en el país por cada solución ofertada.

La vigencia de la garantía iniciará en el momento que se otorgue la conformidad de la puesta en marcha de la solución de seguridad, contados a partir del día siguiente de la firma del acta de conformidad de la instalación.

5.6 INSTALACIÓN Y CONFIGURACIÓN DE LOS EQUIPOS.

Nº	ACTIVIDADES
1	Sesión remota para el levantamiento de información relacionada a la solución existente.
2	Instalación y montaje físico del firewall.
3	Actualización de firmware y licenciamiento firewall.
4	Configuración de políticas críticas para los firewalls.
5	Habilitación de túnel a proveedor.
6	Pruebas de funcionamiento de la VPN de SIMA a proveedor.
7	Configuración de políticas secundarias para firewall.
8	Habilitación del HA en la solución de firewall.
9	Habilitación del tenant de SIMA.
10	Vinculación de los dispositivos de SIMA mediante túnel VPN hacia proveedor.
11	Pruebas finales de las configuraciones y solución HA del firewall.



12	<p>Migración de la solución actual firewall Palo Alto 3020 a la solución HA firewall adquirida, en caso de no sea posible la migración, el contratista deberá realizar todas configuraciones más relevantes ya establecidas en el actual equipo firewall en producción, el cual se indica a continuación:</p> <ul style="list-style-type: none"> • Reglas de entrada y salida. • Enrutamiento. • Filtro de contenido. • Plantillas de políticas de seguridad. • Publicación de servicios (NAT). • Configuración en HA de zonas (Wan, Lan). • Configuración en HA de los enlaces Wan de Internet. • Configuración del portal de autenticación para usuarios fuera del Dominio SIMA. • Configuración de grupos y objetos (Equipos, Redes, Rangos). • Configuración de puertos y servicios. • Integración de dominio SIMA PERU, para autenticación de usuarios a internet. • Configuración de acceso VPN a usuarios. • Y otras que personal de OTIC indique.
----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5.7 CAPACITACIÓN.

El postor deberá considerar una capacitación de la solución por un mínimo de CUATRO (04) horas para un grupo de TRES (03) personas. La capacitación debe comprender lo relacionado a la administración, gestión, resolución de problemas y buenas prácticas de la solución de las soluciones de seguridad ofertadas.

6 RECURSOS Y FACILIDADES A SER PROVISTOS POR LA ENTIDAD.

La OTIC designará el personal técnico que será responsable de coordinar la entrega de los equipos y el soporte técnico requerido.

7 REQUISITOS DEL POSTOR y/o PERSONAL.

7.1. REQUISITOS DEL POSTOR.

a. Requisitos:

1. El postor deberá acreditar para admisión de la oferta ser representante o distribuidor autorizado de la marca ofertada, adjuntando una carta del fabricante haciendo referencia al proceso.¹²
2. Contar con un centro de operaciones de seguridad (SOC) propia para brindar el soporte 24x7x365 incluidos domingos y feriados. El SOC debe contar con certificación ISO27001.

b. Acreditación:

¹² En concordancia con la absolución a la consulta N° 1 del Pliego de consultas y observaciones



1. Para el literal a, numeral 1, el postor deberá demostrar mediante carta de fabricante o enlace de página web oficial del fabricante, que es partner autorizado de la solución ofertada.
2. Para el literal a, numeral 2, el postor deberá de enviar una copia de la certificación, el cual valida que su SOC (Security Operations Center) está de acuerdo con la norma ISO 27001.

7.2. PERSONAL CLAVE.

7.2.1. JEFE DEL PROYECTO.

Funciones:

Encargado de la gestión de la solución, su implementación y configuración hasta su operatividad.

Deberá gestionar las actividades de la contratación con un enfoque de proyecto bajo estándar PMI o metodologías ágiles.

a. Formación académica:

1. UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.
2. Deberá contar con certificación PMP vigente y/o especialización o diplomado en gestión de proyectos con base en el enfoque del Project Management Institute – PMI, con una duración mínima de 160 horas.
3. Deberá contar con experiencia mínima de DOS (02) años en gestión de proyectos de TI y/o proyectos de seguridad de la información.

b. Acreditación:

1. Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.
2. El título profesional podrá ser verificado por el comité de selección 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 según corresponda.
3. Deberá demostrar estar colegiado y estar habilitado en el CIP.
4. Copia simple de certificado oficial PMP
5. Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos.



7.2.2.SUPERVISOR DE PROYECTO.

Funciones:

Deberá supervisar las actividades del proyecto y participar en la implementación

Deberá asegurar el posterior soporte técnico de la solución ofertada.

a. Formación académica:

1. UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.
2. Deberá contar con certificación services desk leader o IT service management (ITSM)
3. Deberá contar con certificación ITIL y Lead Cybersecurity Professional Certificate (LCSPC)
4. Deberá contar con experiencia mínima de DOS (02) años en supervisión de proyectos de seguridad informática y/o soluciones de seguridad y/o soluciones de seguridad de la información.

b. Acreditación:

1. Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.
2. El título profesional podrá ser verificado por el comité de selección 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 según corresponda.
3. Deberá demostrar estar colegiado y estar habilitado en el CIP.
4. Copia simple de certificado oficial services desk leader o IT service management (ITSM).
5. Copia simple de certificado oficial ITIL y Lead Cybersecurity Professional Certificate (LCSPC).
6. Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos.

7.2.3.ESPECIALISTA DE SEGURIDAD PERIMETRAL.

Funciones:

Encargado de la implementación y configuración de la solución.



a. Formación académica:

1. UN (01) técnico titulado, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.
2. Certificado en la marca ofertada.
3. Deberá contar con experiencia mínima de DOS (02) años en implementaciones, soporte técnico y mantenimiento de soluciones de firewall de seguridad perimetral e interno.

b. Acreditación:

1. Copia simple de, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.
2. El título profesional podrá ser verificado por el comité de selección 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 según corresponda.
3. Copia simple de certificado en la marca ofertada.
4. Deberá acreditar experiencia por medio de constancias, certificados, contratos y/u otros documentos.

8 LUGAR Y PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN.

8.1. LUGAR.

El lugar de ejecución del servicio será en la OTIC del SIMA PERÚ, ubicado en Av. Contralmirante Mora 1102, Base Naval del Callao.

8.2. PLAZO.

8.2.1. DE LA PRESTACIÓN PRINCIPAL.

8.2.1.1. Plazo de entrega de los bienes.

Los bienes y/o licenciamiento serán entregados en un plazo no mayor a TREINTA (30) días calendario, contados a partir del día siguiente del perfeccionamiento del contrato.

8.2.1.2. Plazo de instalación, configuración y puesta en producción.

La instalación, configuración y puesta en producción será en un plazo no mayor a CINCO (05) días calendario, contados a partir de la entrega de los bienes y/o licencias.

9 DE LA ENTREGA DEL BIEN.





- a. El internamiento se realizará empacado en un medio seguro que garantice el buen estado del producto, el cual deberá estar identificado con la razón social del fabricante, cantidad, y tipo de bien debidamente sellada para protegerla del almacenamiento, transporte y manipuleo.
- b. Los bienes deben ser transportados en vehículo acondicionado para su traslado y evitar el contacto con superficies contaminadas.

10 MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL.

10.1 ÁREAS QUE COORDINARÁN CON EL CONTRATISTA.

El personal técnico dispuesto en el numeral 6 será responsable de efectuar las coordinaciones con el PROVEEDOR.

10.2 ÁREAS RESPONSABLES DE LAS MEDIDAS DE CONTROL.

La OTIC es responsable de las medidas de control previstas durante la ejecución de la entrega del bien.

10.3 ÁREA QUE BRINDARÁ LA CONFORMIDAD.

El Almacén del SIMA CALLAO emitirá el acta de conformidad de recepción correspondiente, luego de la verificación de los siguientes entregables:

- a. Revisión de la guía de remisión del proveedor y verificación de productos, por el personal designado en el numeral 6, validando que los equipos corresponden a lo requerido en las especificaciones técnicas.

11 FORMA DE PAGO.

Será un único pago posterior a la firma del acta de conformidad respectiva.

I. REQUISITOS DE CALIFICACIÓN



A.	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a DOSCIENTOS VEINTE MIL CON 00/100 SOLES (S/ 220,000.00), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</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 VEINTICUATRO MIL CIENTO OCHENTA Y 00/100 SOLES (S/ 24,180.00), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los OCHO (08) años anteriores a la fecha de la presentación de ofertas que se computarán desde</p>



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.

Se consideran venta de bienes similares a los siguientes: venta de equipos de seguridad firewall y/o venta de equipos de seguridad anti spam y/o venta de equipos de seguridad ips y/o venta de servidores de datos y/o venta de sistema de almacenamiento y/o venta de soluciones de infraestructura.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad

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

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

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la



documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

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

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

Importante

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

Importante para la Entidad

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

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases, así como el requisito de calificación, si este no ha sido incluido.

B. CAPACIDAD TÉCNICA Y PROFESIONAL

B.1 FORMACIÓN ACADÉMICA

DEL JEFE DE PROYECTO

Requisitos:

UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.

Deberá contar con certificación PMP vigente y/o especialización o diplomado en gestión de proyectos con base en el enfoque del Project Management Institute – PMI, con una duración mínima de 160 horas.

Acreditación:

Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.

El título profesional podrá ser verificado por el comité de selección 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 según corresponda.

Deberá demostrar estar colegiado y estar habilitado en el CIP.

Copia simple de certificado oficial PMP

DEL SUPERVISOR DE PROYECTO

Requisitos:

UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.

Deberá contar con certificación services desk leader o IT service management (ITSM).

Deberá contar con certificación ITIL y Lead Cybersecurity Professional Certificate (LCSPC).

Acreditación:

Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.

El título profesional podrá ser verificado por el comité de selección 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 según corresponda.

Deberá demostrar estar colegiado y estar habilitado en el CIP.

Copia simple de certificado oficial services desk leader o IT service management (ITSM).

Copia simple de certificado oficial ITIL y Lead Cybersecurity Professional Certificate (LCSPC).

DEL ESPECIALISTA DE SEGURIDAD PERIMETRAL

Requisitos:

UN (01) técnico titulado, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.

Certificado en la marca ofertada.

Acreditación:

Copia simple de, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.

El título profesional podrá ser verificado por el comité de selección 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 según corresponda.

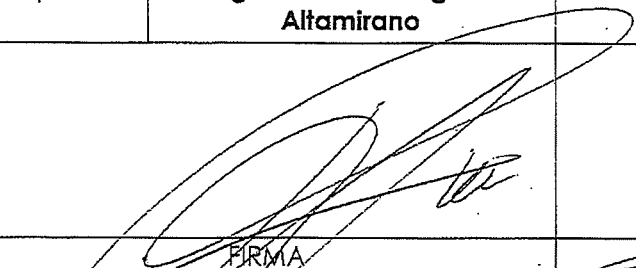
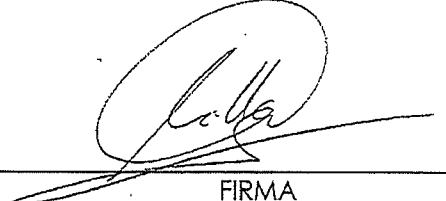


	Copia simple de certificado en la marca ofertada.
B.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>DEL JEFE DE PROYECTO</u></p> <p><u>Requisitos:</u> Deberá contar con experiencia mínima de DOS (02) años en gestión de proyectos de TI y/o proyectos de seguridad de la información.</p> <p><u>DEL SUPERVISOR DE PROYECTO</u></p> <p><u>Requisitos:</u> Deberá contar con experiencia mínima de DOS (02) años en supervisión de proyectos de seguridad informática y/o soluciones de seguridad y/o soluciones de seguridad de la información.</p> <p><u>DEL ESPECIALISTA DE SEGURIDAD PERIMETRAL</u></p> <p><u>Requisitos:</u> Deberá contar con experiencia mínima de DOS (02) años en implementaciones, soporte técnico y mantenimiento de soluciones de firewall de seguridad perimetral e interno</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> <div><p>Importante</p><ul style="list-style-type: none">• El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.• Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento y la fecha de emisión y nombres y apellidos de quien suscribe el documento.• En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.• Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</div>



Importante

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

Fecha	04/09/2023	Fecha:	04/09/2023
Elaborado por:	Especialista en Redes y Comunicaciones Ing. Manuel Meregildo Altamirano	Revisado por:	Experto en Infraestructura y Servicios Informáticos (e) Ing. Luis MILLA Mostacero
			
FIRMA		FIRMA	

3.2 REQUISITOS DE CALIFICACIÓN

A.	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a DOSCIENTOS VEINTE MIL CON 00/100 SOLES (S/ 220,000.00), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</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 VEINTICUATRO MIL CIENTO OCHENTA Y 00/100 SOLES (S/ 24,180.00), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los OCHO (08) 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran venta de bienes similares a los siguientes: venta de equipos de seguridad firewall y/o venta de equipos de seguridad anti spam y/o venta de equipos de seguridad ips y/o venta de servidores de datos y/o venta de sistema de almacenamiento y/o venta de soluciones de infraestructura.</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, 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 N° 8 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 a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes</p>

de pago cancelados.

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

Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9**.

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

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

Importante

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

B.	CAPACIDAD TÉCNICA Y PROFESIONAL
B.1	FORMACIÓN ACADÉMICA
	<u>DEL JEFE DE PROYECTO</u>
	<u>Requisitos:</u> UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas,

ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.

Deberá contar con certificación PMP vigente y/o especialización o diplomado en gestión de proyectos con base en el enfoque del Project Management Institute – PMI, con una duración mínima de 160 horas.

Acreditación:

Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.

El título profesional podrá ser verificado por el comité de selección 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 según corresponda.

Deberá demostrar estar colegiado y estar habilitado en el CIP.

Copia simple de certificado oficial PMP

DEL SUPERVISOR DE PROYECTO

Requisitos:

UN (01) profesional titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, Informática y sistemas. Deberá estar colegiado y habilitado al momento de la presentación de la oferta.

Deberá contar con certificación services desk leader o IT service management (ITSM).

Deberá contar con certificación ITIL y Lead Cybersecurity Professional Certificate (LCSPC).

Acreditación:

Copia simple de título en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.

El título profesional podrá ser verificado por el comité de selección en el

	<p>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 según corresponda.</p> <p>Deberá demostrar estar colegiado y estar habilitado en el CIP.</p> <p>Copia simple de certificado oficial services desk leader o IT service management (ITSM).</p> <p>Copia simple de certificado oficial ITIL y Lead Cybersecurity Professional Certificate (LCSPC).</p> <p><u>DEL ESPECIALISTA DE SEGURIDAD PERIMETRAL</u></p> <p><u>Requisitos:</u> UN (01) técnico titulado, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>Certificado en la marca ofertada.</p> <p><u>Acreditación:</u> Copia simple de, profesional, bachiller o titulado en ingeniería electrónica, ingeniería de sistemas, ingeniería de seguridad y auditoría informática, ingeniería de telecomunicaciones, redes y comunicaciones o redes y comunicaciones de datos, informática y sistemas.</p> <p>El título profesional podrá ser verificado por el comité de selección 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 según corresponda.</p> <p>Copia simple de certificado en la marca ofertada.</p>
B.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>DEL JEFE DE PROYECTO</u></p> <p><u>Requisitos:</u> Deberá contar con experiencia mínima de DOS (02) años en gestión de proyectos de TI y/o proyectos de seguridad de la información.</p> <p><u>DEL SUPERVISOR DE PROYECTO</u></p> <p><u>Requisitos:</u> Deberá contar con experiencia mínima de DOS (02) años en supervisión de proyectos de seguridad informática y/o soluciones de seguridad y/o soluciones de seguridad de la información.</p>

DEL ESPECIALISTA DE SEGURIDAD PERIMETRAL

Requisitos:

Deberá contar con experiencia mínima de DOS (02) años en implementaciones, soporte técnico y mantenimiento de soluciones de firewall de seguridad perimetral e interno

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

Importante

- El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.
- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento y la fecha de emisión y nombres y apellidos de quien suscribe el documento.
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.

Importante

- Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.
- El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral

2.2.1.1 de esta sección de las bases.

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

**CAPÍTULO IV
FACTORES DE EVALUACIÓN**

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
<p><u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u> Se acreditará mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>	<p>La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i = 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;">90 puntos</p>
B. MEJORAS A LOS TÉRMINOS DE REFERENCIA	
<p><u>ANÁLISIS DE VULNERABILIDADES</u></p> <p>El contratista deberá realizar un servicio análisis de vulnerabilidades a 10 direcciones IP por el periodo mínimo de 10 días que cumpla con las siguientes características:</p> <ul style="list-style-type: none"> • El servicio debe incluir una capacidad integrada de exploración activa / pasiva para una visibilidad total de las vulnerabilidades y la configuración. • El servicio debe poder utilizar grupos de escáneres en una sola tarea. • El servicio debe ser capaz de escanear activos en las redes internas de los clientes, así como activos externos / disponibles públicamente. • Los escáneres deben ser gestionados por la plataforma, actualizaciones de firmas de vulnerabilidad y código. • El servicio debe cifrar los datos en reposo y en tránsito. • El servicio debe admitir múltiples motores de escaneo distribuidos geográficamente. • El servicio debe ser capaz de escanear hosts muertos (dispositivos que no responden al ping). • El servicio debe detectar y clasificar problemas, riesgos y vulnerabilidades. 	<p style="text-align: right;">10 puntos</p>

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<ul style="list-style-type: none"> • El servicio debe incluir resultados detallados de los resultados del análisis para incluir información como las versiones de DLL esperadas y encontradas. • El servicio debe ser compatible con CVE y proporcionar al menos 10 años de cobertura de CVE. • El análisis debe considerar la búsqueda de información confidencial de diseño y configuración de la aplicación web expuesta de manera directa o indirecta, a través de distintos de motores de búsqueda. • Debe identificar la versión y el tipo del servidor web donde esta alojada la aplicación, para explorar las distintas vulnerabilidades y exploits a los que se encuentra expuesto. • Se debe detectar la fuga de información en metadatos de archivos y/o página web. • Análisis de fuga de información sobre el código de programación público del servicio web. • Debe identificar el tipo de framework de la aplicación a través de su fingerprint para la revisión de vulnerabilidades conocidas. • Detección de archivos de configuración que puedan exponer el código del lado del servidor. • El análisis debe contemplar las pruebas de credenciales por defecto sobre la aplicación web a través de distintos diccionarios. • Debe considerar las pruebas de mecanismo de bloqueo débil para la mitigación de ataques de fuerza bruta. 	
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 de Adquisición de Solución de Seguridad perimetral Next Generation firewall y filtro de contenido en alta disponibilidad, 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 bien, todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre la ejecución de la prestación materia del presente contrato.

CLÁUSULA CUARTA: DEL PAGO¹⁴

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR EL DETALLE DEL PAGO UNICO O PAGOS A CUENTA, SEGÚN CORRESPONDA], luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

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

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

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. EN LA MODALIDAD DE LLAVE EN MANO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].

Importante para la Entidad

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

CLÁUSULA: PRESTACIONES ACCESORIAS¹⁵

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

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

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

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

Incorporar a las bases o eliminar, según corresponda

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

- 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.

En el caso que corresponda, consignar lo siguiente:

- Garantía fiel cumplimiento por prestaciones accesorias: [CONSIGNAR EL MONTO], a través

¹⁵ De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesorias, pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

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

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: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA DE ALMACÉN O LA QUE HAGA SUS VECES] y la conformidad será otorgada por [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para subsanar no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

El plazo máximo de responsabilidad del contratista es de **[CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO]** año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

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

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

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

Importante

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

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

Lo señalado precedentemente no exime a ninguna de las partes del cumplimiento de las demás obligaciones previstas en el presente contrato.

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

Asimismo, el CONTRATISTA se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

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

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹⁶

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

¹⁶ 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 Digitales¹⁷.

¹⁷ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA-SEGUNDA CONVOCATORIA
Presente.-

El que se suscribe, [...], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento N° [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ¹⁸		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 compra¹⁹

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.

¹⁸ 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 cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹⁹ 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 compra.

Importante

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA-SEGUNDA CONVOCATORIA
Presente.-

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

Datos del consorciado 1				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ²⁰		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ²¹		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :		Teléfono(s) :		
MYPE ²²		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:

²⁰ 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 cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

²¹ Ibídem.

²² Ibídem.

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 compra²³

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.

²³ 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 compra.

ANEXO N° 2

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA-SEGUNDA CONVOCATORIA
Presente.-

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

- i. No haber incurrido y me obligo a no incurrir en actos de corrupción, así como a respetar el principio de integridad.
- ii. No tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 11 de la Ley de Contrataciones del Estado.
- iii. Conocer las sanciones contenidas en la Ley de Contrataciones del Estado y su Reglamento, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iv. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- v. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- vi. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vii. Comprometerme a mantener la oferta presentada durante el procedimiento de selección y a perfeccionar el contrato, en caso de resultar favorecido con la buena pro.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA-SEGUNDA CONVOCATORIA
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023- SIMA- SEGUNDA CONVOCATORIA
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **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] [%]²⁴

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁵

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

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

²⁵ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

TOTAL OBLIGACIONES

100%²⁶

[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.

²⁶ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

Importante para la Entidad

En caso de la contratación de bienes 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

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA

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 bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *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 conlleven 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 contratación de bienes bajo el sistema a suma alzada incluir el siguiente anexo:

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

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA

Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

Importante para la Entidad

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

Incluir o eliminar, según corresponda

Importante para la Entidad

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

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

ANEXO N° 7

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA
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 empresa²⁷ se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);
- 2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);
- 3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y
- 4.- Que la empresa no tiene producción fuera de la Amazonía.²⁸

[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.

²⁷ En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquellas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

²⁸ En caso de empresas de comercialización, no consignar esta condición.

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / 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										

²⁹ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

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 Compra o de cancelación del comprobante de pago, según corresponda.

³⁴ Consignar en la moneda establecida en las bases.

SERVICIOS INDUSTRIALES DE LA MARINA
ADJUDICACIÓN SIMPLIFICADA AS-06-2023-SIMA-SEGUNDA CONVOCATORIA

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/C / 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
4										
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

**DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)**

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA Nº AS-06-2023-SIMA- SEGUNDA CONVOCATORIA
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 10

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA
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° 11

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° AS-06-2023-SIMA- SEGUNDA CONVOCATORIA
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 12

DEBERÁ INDICAR EL NÚMERO DE FOLIO QUE SUSTENTE LAS CARACTERÍSTICAS TÉCNICAS DETALLADAS EN EL NUMERAL 5.3 DE LAS ESPECIFICACIONES TÉCNICAS, DE ACUERDO A LA DOCUMENTACIÓN OFICIAL DEL FABRICANTE (HOJA TÉCNICA, BROCHURE, DATASHEET).

5.3 CARACTERÍSTICAS TÉCNICAS	
5.3.1 CARACTERÍSTICAS DE RENDIMIENTO PARA FIREWALL.	N° FOLIO DE SUSTENTO
a. Throughput de Next Generation Firewall de 4.3 Gbps (mínimo) medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.	
b. Throughput de Prevención de Amenazas de 2 Gbps (mínimo) medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: control de aplicaciones, sistema de prevención de intrusos (IPS), seguridad del tráfico DNS, antivirus/antimalware de red, antispymware/antiBot, sandboxing, filtro de archivos y logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido al habilitar los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242.	
c. El equipo debe soportar como mínimo 390.000 sesiones simultaneas y 70.000 sesiones por segundo, medidos con paquetes HTTP de 1 byte.	
d. Debe contar con fuente de poder redundante.	
e. Disco interno de 120 GB o superior.	
f. Mínimo OCHO (08) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red.	
g. La plataforma deberá contar con al menos UN (01) puerto de gestión fuera de banda dedicada para la gestión del equipo.	
h. Deberá tener CPU dedicado para tareas de gestión del equipo, de manera independiente a los recursos de CPU para el procesamiento del tráfico. Esta arquitectura podrá estar integrada dentro del NGFW, o en caso no lo soporte, se podrán incluir consolas de gestión externas al NGFW.	
i. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.	
j. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).	
k. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPsec no cifrado, sin necesidad de que el NGFW sea el punto final del túnel.	
l. 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.	
m. 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.	

n. La plataforma propuesta por el fabricante debe contar con certificación USGv6-r1 para las pruebas de firewall, IDS e IPS.	
o. 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).	
p. 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.	
q. 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.	
r. Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.	
5.3.2 FUNCIONALIDADES DE FIREWALL.	N° FOLIO DE SUSTENTO
a. 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).	
b. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.	
c. 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).	
d. Debe mostrar la primera y última vez que se utilizó una regla de seguridad.	
e. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.	
f. 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.	
g. Debe permitir tener un registro de auditoría en cada política que permita conocer que cambios se realizó con anterioridad.	
h. 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.	
5.3.3 DESCIFRADO DE TRÁFICO SSL/TLS.	N° FOLIO DE SUSTENTO
a. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.	
b. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.	
c. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.	
d. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.	
e. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS.	
f. Debe soportar certificados que utilice subject alternative name (SAN) y Server Name Indication (SNI).	
g. Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio.	
h. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.	
i. Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.	

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

5.3.4 CONTROL DE APLICACIONES.

N° FOLIO DE
SUSTENTO

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

b. Las aplicaciones deberán estar clasificadas en al menos 30 tipos, de tal manera que se puedan configurar políticas en base al tipo de aplicación.

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

d. 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.

e. Las políticas de seguridad deben poder definirse netamente en base a aplicaciones, sin necesidad de especificar puertos.

f. 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.

g. Con el objetivo de controlar aplicaciones propietarias en capa 7, la solución debe permitir la creación de aplicaciones personalizadas desde la interfaz de gestión.

h. 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.

i. El módulo de aprendizaje deberá ser específico por cada política de seguridad.

j. 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.

k. 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.

5.3.5 PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (DoS).

N° FOLIO DE
SUSTENTO

a. 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.

b. Debe ser posible utilizar SYN Cookies como medida de defensa.

c. 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).

d. 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.

e. Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route.	
f. 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.	
5.3.6 PREVENCIÓN DE AMENAZAS.	N° FOLIO DE SUSTENTO
a. La solución propuesta deberá contar con capacidades de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.	
b. 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.	
c. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.	
d. La solución deberá identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que se pueda bloquear dichas consultas DNS.	
e. 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.	
f. Deberá ser capaz de identificar amenazas sobre el tráfico DNS encriptado camuflado sobre HTTPS (DNS over HTTPS – DoH), y también DNS sobre TLS.	
g. El módulo de IPS debe ser capaz de bloquear ataques en base a firmas, heurística y anomalías en el protocolo.	
h. El módulo de IPS debe permitir personalizar firmas directamente desde la consola gráfica.	
i. 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.	
j. 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.	
k. 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.	
l. 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	
5.3.7 ANALISIS DE MALWARE DE DÍA CERO.	N° FOLIO DE SUSTENTO
a. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.	
b. La plataforma de Sandboxing debe ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.	
c. También se aceptará soluciones sandbox terceras de otro fabricante distinto al NGFW.	
d. 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.	

e. 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.	
f. Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines).	
g. Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.	
h. El Next Generation Firewall deberá ser capaz de actualizar las firmas de malware en tiempo real, con el objetivo de tener información de malware detectado a nivel global por el fabricante.	
i. 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.	
j. El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.	
k. 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 ser extraída en un reporte PDF.	
l. Deberá generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.	
m. Debe permitir al administrador la descarga del archivo original analizado por el sandbox.	
n. 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.	
o. Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico.	
p. 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.	
q. La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.	
5.3.8 PROTECCION AVANZADA DE DNS.	N° FOLIO DE SUSTENTO
a. 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.	
b. 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.	
c. Deberá ser capaz de prevenir ataques como DGA (Domain Generation Algoritim) Random y de Diccionario, DNS Tunneling, Fast Flux Domains, NXNS Attack, DNS Rebinding, abuso de wildcards, CNAME cloaking, infiltración de DNS.	
d. Deberá soportar el manejo excepciones para poder mitigar los falsos positivos.	
e. 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.	
f. 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.	
g. En caso de ser una plataforma en nube deberá estar certificado en SOC2 Tipo II de AICPA.	
5.3.9 IDENTIFICACION DE USUARIOS.	N° FOLIO DE SUSTENTO

a. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.	
b. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.	
c. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.	
d. Debe disponer de un servicio en nube o onpremise que extraiga automáticamente la información del usuario grupos de usuario de varios IDPs y proveedores de SSO como Azure AD, okta, Google identity y PingID y la ponga a disposición de los NGFW para ser incluidos en la política de seguridad.	
e. Debe disponer de un servicio en nube o onpremise que simplifique la autenticación SAML de usuarios, que actue como Service Provider único frente a IDPs o proveedores de SSO.	
f. Debe disponer de un servicio en nube o onpremise que almacene todos los grupos disponibles del Active Directoy, los filtre y ponga a disposicion unicamnte los grupos necesarios que el NGFW utilice en la política de seguridad.	
g. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.	
h. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.	
i. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.	
j. Debe permitir la definición de grupos dinámicos de usuarios.	
5.3.10 FILTRO DE CONTENIDO WEB.	Nº FOLIO DE SUSTENTO
a. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing, redes sociales, páginas de adultos.	
b. Debe soportar un cache local de URLs en el dispositivo, evitando el delay de comunicación/validación de las URLs.	
c. 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.	
d. 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.	
e. Debe contar con medidas de antievasión como Cloaking, Captcha falsos, codificación de caracteres HTML, entre otros.	
f. Debe permitir la creación de categorías personalizadas.	
g. Debe permitir la personalización de la página de bloqueo.	
h. Debe permitir notificar al usuario, mostrándole solo una página de alerta personalizable, pero permitiéndole continuar la navegación al site.	
i. Debe ser capaz de registrar el User-agent, Referer, XFF de cada sesión hacia internet.	
j. Debe ser capaz de forzar la navegación de los usuarios en el modo Safe Search Enforcement.	
k. 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	

5.3.11 FUNCIONALIDADES DE OPTIMIZACIÓN.	N° FOLIO DE SUSTENTO
a. Se debe proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Firewall implementado.	
b. Esta herramienta debe funcionar en línea y de manera automática. Es decir, luego de cada configuración realizada en el Firewall, debe mostrar los cambios realizados.	
c. Debe contar con gráficos ejecutivos que permitan mostrar el nivel de adopción de los módulos de seguridad del NGFW en las políticas de seguridad.	
d. Debe contar con un módulo que permita filtrar y depurar las políticas de NGFW sin uso en la red.	
e. Debe identificar automáticamente las políticas abiertas que no tengan restricciones de puertos y/o aplicaciones (ANY o ALL), con el objetivo de corregirlas y hacer cumplir el principio de mínimo privilegio.	
f. La herramienta de evaluación de buenas prácticas debe mostrar al menos lo siguiente: nivel de adopción del control de aplicaciones, visibilidad de usuarios, configuraciones correctas de los perfiles de seguridad (antivirus, IPS, sandboxing), hardening de la plataforma.	
g. La herramienta de evaluación de buenas prácticas debe ser específica para la configuración de firewall implementado, no se aceptarán guías de usuarios genéricas.	
h. Debe contar con un dashboard que muestre la salud del equipo. Asimismo, si apareciera una falla debe enviar un correo de manera automática.	
5.3.12 CONSOLA DE ADMINISTRACIÓN Y MONITOREO.	N° FOLIO DE SUSTENTO
a. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del NGFW, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante.	
b. Permitir exportar las reglas de seguridad en formato CSV y PDF.	
c. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.	
d. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.	
e. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino).	
f. Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de sólo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.	
g. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.	
h. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).	
i. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).	
j. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.	

k.	Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).	
l.	Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración.	
m.	Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.	
n.	Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispysware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.	
o.	Debe permitir configurar reportes para ver el tiempo de navegación de los usuarios en internet, clasificado por tipo de página web y URL.	
p.	Debe contar con reportes predeterminados que muestren información y diversas estadísticas sobre el uso de aplicaciones SaaS.	
q.	La gestión de NGFW debe permitir realizar tareas de gestión a través del API basado en XML.	

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