

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 sombread.
- 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° 0006-2023-SINEACE

BASES INTEGRADAS

CONTRATACIÓN DE BIENES

**ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD
PERIMETRAL**

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I

ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento, así como el literal a) del artículo 89 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada. Las consultas y observaciones que se formulen sobre el particular, se tienen como no presentadas.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 del Reglamento.

Importante

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

1.6. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

Importante

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

1.7. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

¹ Para mayor información sobre la normativa de firmas y certificados digitales ingresar a: <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>

En la apertura electrónica de la oferta, el órgano encargado de las contrataciones o el comité de selección, según corresponda, verifica la presentación de lo exigido en la sección específica de las bases de conformidad con el numeral 73.2 del artículo 73 del Reglamento y determina si las ofertas responden a las características y/o requisitos 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-emitir-cartas-fianza>).

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

Advertencia

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre : SISTEMA NACIONAL DE EVALUACIÓN, ACREDITACIÓN Y CERTIFICACIÓN DE LA CALIDAD EDUCATIVA – SINEACE.

RUC N° : 20551178294

Domicilio legal : AV. REPÚBLICA DE PANAMÁ N° 3659 – SAN ISIDRO.

Teléfono: : 6371122 ANEXO 156, 158

Correo electrónico: : apoyo-logistica14@sineace.gob.pe; jsancheza@sineace.gob.pe; jportales@sineace.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la Adquisición de una Solución de Seguridad Perimetral.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante la Resolución Jefatural N° 030-2023-SINEACE/P-GG-OA, de fecha 13 de junio de 2023.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

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.

1.7. DISTRIBUCIÓN DE LA BUENA PRO

No corresponde.

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

El plazo de entrega de los bienes materia de la presente convocatoria, instalación, configuración y puesta en producción del equipamiento es de hasta sesenta (60) días calendario, en concordancia con lo establecido en el expediente de contratación.

1.10. PLAZO DE PRESTACIONES ACCESORIAS:

El plazo de ejecución total del mantenimiento preventivo y soporte técnico es de un (01) año (365 días calendario), contados a partir del día siguiente de la firma del Acta de implementación de la solución y garantía, en concordancia con lo establecido en el expediente de contratación.

1.11. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, la cual se le será expedida de forma gratuita. La solicitud de la misma podrá realizarla de forma electrónica a través de la mesa de partes virtual de la Entidad, a través del siguiente link: <https://www.gob.pe/20416-acceder-a-mesa-de-partes?child=9385>

1.12. BASE LEGAL

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

- Ley N° 31640 - Ley de Endeudamiento del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 - Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Ley N° 31638 de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 28411 - Ley General del Sistema Nacional del Presupuesto.
- Ley 27815 Ley de Código de Ética de la Función Pública.
- Decreto Legislativo N° 1440 - Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado - Aprobado mediante Decreto Supremo N° 082-2019-EF, (en adelante, la Ley).
- Texto Único Ordenado de la Ley 27444, Ley del Procedimiento Administrativo General, aprobado con Decreto Supremo N° 004-2019-JUS.
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, aprobado con Decreto Supremo N° 021-2019-JUS.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado, y modificatorias, (en adelante, el Reglamento).
- Directivas del OSCE. - Resolución Jefatural N° 003-2023-SINEACE/P-ST-OA, Plan Anual de Contrataciones del Pliego 117: Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa - Sineace, correspondiente al Ejercicio Fiscal 2023.
- Directivas del OSCE.
- Código Civil
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la presente convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado y su Reglamento.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de 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.
- 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)**
- e) Reporte del fabricante donde se acredite que los modelos ofertados no se encuentren discontinuados, listados ni anunciados en el sitio web del fabricante como fin de vida (end-of-life), no deberán estar en el fin de venta (end-of-sale) y no deberán estar en el fin de soporte (end-of-support).
- f) Reporte obtenido desde el portal oficial de “Gartner” y el enlace correspondiente, en el cual el fabricante debe pertenecer al cuadrante de líderes de Gartner para “Network Firewall” o “Firewall de Redes” en los últimos 5 reportes.
- g) Reporte obtenido desde el portal oficial de “Forrester” y el enlace correspondiente, en el cual el fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls.
- h) **Certificación del Centro de Operaciones de Seguridad – SOC, certificado con la norma ISO 27001.³**
- i) Declaración jurada de plazo de entrega. **(Anexo N° 4)⁴**

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

³ De acuerdo a la consulta N° 02

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.

- j) 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**)
- k) 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.

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**).

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- a) Garantía de fiel cumplimiento del contrato (Carta Fianza)
- b) Garantía de fiel cumplimiento por prestaciones accesorias. (Carta Fianza)
- 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.
- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación ⁶ (**Anexo N° 11**).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) Documentos que acrediten la formación académica del personal clave.
- k) Carta del fabricante que acredite que los equipos deben ser comercializados de última vigencia tecnológica, conforme a las características generales del numeral 5.1. "Características técnicas mínimas".
- l) Seguros complementarios de trabajo de riesgo (SCTR) vigentes.

Importante

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente

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

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

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

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.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida a través de mesa de partes física o a través de mesa de partes virtual, de acuerdo a lo siguiente:

Mesa de partes física:

De lunes a viernes de 08:30 a 16:30 horas, en la Av. República de Panamá N° 3659 – distrito de San Isidro, provincia y departamento de Lima.

Mesa de partes virtual:

En cualquier horario ingresando al link: <https://www.gob.pe/20416-acceder-a-mesa-departes?child=9385>

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS A CUENTA, en tres (03) armadas, de acuerdo a lo siguiente:

Pago N° 01: Por la presentación del entregable 1 y 2, correspondiente al 95%, del monto total de la contratación, el monto incluye los impuestos de ley, previa conformidad otorgada por el área usuaria.

Pago N° 02: Por la presentación con del entregable 3, correspondiente al 2%, del monto total de la contratación, el monto incluye los impuestos de ley, previa conformidad otorgada por el área usuaria.

Pago N° 03: Por la presentación con del entregable 4, correspondiente al 3%, del monto total de la contratación, el monto incluye los impuestos de ley, previa conformidad otorgada por el área usuaria.

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

- Documento que acredite la recepción por parte del Almacén del Sineace.
- Conformidad de Ingreso de bienes.
- Informe de supervisión del coordinador o especialista o analista de la Oficina de Tecnologías de la Información y Comunicaciones.
- Conformidad de la prestación emitida por el Jefe de Oficina de Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en mesa de partes física o a través de mesa de partes virtual, de acuerdo a lo siguiente:

Mesa de partes física:

De lunes a viernes de 08:30 a 16:30 horas, en la Av. República de Panamá N° 3659 – distrito de San Isidro, provincia y departamento de Lima.

Mesa de partes virtual:

En cualquier horario ingresando al link: <https://www.gob.pe/20416-acceder-a-mesa-departes?child=9385>.

CAPÍTULO III REQUERIMIENTO

3.1. ESPECIFICACIONES TÉCNICAS

1. DENOMINACIÓN:

Adquisición de una Solución de Seguridad Perimetral.

2. FINALIDAD PÚBLICA:

A través de la presente contratación se busca menguar los riesgos ante ataques informáticos externos, accesos no autorizados y otras amenazas que afecten el normal funcionamiento de los servicios informáticos, con la finalidad de elevar los niveles de eficiencia y satisfacción de los usuarios, en apoyo a las actividades que coadyuvan al cumplimiento de objetivos institucionales.

3. ANTECEDENTES:

Actualmente la Entidad cuenta con una solución de seguridad perimetral adquirido en el año 2017, cuyo soporte del fabricante solo estará disponible hasta el 08/05/2023, generando un riesgo alto de indisponibilidad de servicios para casos de fallas a nivel de hardware, además de no permitir aceptar las nuevas actualizaciones y/o parches de seguridad del sistema y versiones de software; limitando su capacidad operativa, funcionalidad y tiempo de respuesta. Asimismo, el soporte y licencia de la solución de seguridad perimetral vencieron el 27/12/2022, esta condición limita su uso y funcionalidades como antivirus, filtrado web, IPS, entre otros.

En ese sentido, se necesita seguir contando con una solución de seguridad perimetral con tecnología y soporte vigente, que proteja la infraestructura de redes y plataforma tecnológica de la Entidad, con esta solución se busca minimizar los riesgos de ataques informáticos externos, accesos no autorizados, y otras amenazas que afecten el normal funcionamiento de los servicios informáticos, salvaguardando los activos de la información y evitar riesgos que impacten en la disponibilidad de los servicios ofrecidos por la Entidad.

A razón de lo anteriormente expuesto, la Oficina de Tecnologías de la Información y Comunicaciones – OTIC, a través del Memorandum N° 000031-2023-SINEACE/P-GG-OTIC (de fecha 06/03/2023) y el Memorandum N° 000039-2023-SINEACE/P-GG-OTIC (de fecha 13/03/2023), presenta el sustento técnico para la adquisición de activos por reposición a través de Inversiones de Optimización, de Ampliación Marginal, de Rehabilitación y de Reposición (IOARR). Al respecto, la Oficina de Planificación y Presupuesto, a través del Memorandum N° 000139-2023-SINEACE/P-GG-OPP (de fecha 14/03/2023), comunica la aprobación de la IOARR con CUI N° 2577398 "Adquisición de sistema de seguridad perimetral (firewall), servidor y switch; en el(la) Oficina de Tecnologías de Información y Comunicaciones, distrito de San Isidro, provincia Lima, departamento Lima". La presente, proviene de un proyecto de inversión, el cual se encuentra aprobado en el Banco de Inversiones del Invierte.pe con fecha 13/03/2023.

4. OBJETIVO DE LA CONTRATACIÓN:

a. OBJETIVO GENERAL:

Contar con una solución de seguridad perimetral (tipo appliance) en alta disponibilidad, debidamente configurado y puesto en producción bajo la modalidad LLAVE EN MANO, para garantizar la operatividad, continuidad y disponibilidad de la misma, en apoyo al logro de los objetivos institucionales.

b. OBJETIVO ESPECÍFICO:

- *Proteger la red con características de nueva generación para la prevención de amenazas mediante visibilidad completa de todo el tráfico en la red perimetral, permitiendo la detección de comportamientos maliciosos o sospechosos de aplicaciones y amenazas que vulneran la seguridad de los sistemas informáticos de la Entidad.*
- *Adquirir e implementar una solución de seguridad perimetral (firewall de siguiente generación) en el perímetro de la red hacia internet, para filtrar el tráfico proveniente de internet, filtrar URLs, controlar el uso de las aplicaciones, identificar los usuarios, monitorear los archivos que ingresan y salen de la Entidad, prevenir ataques informáticos de botnets/spywares, malware, prevenir intrusiones; permitiendo solo el tráfico válido y seguro; aislar y controlar los servicios publicados a internet en una zona DMZ.*
- *Contar con soporte técnico especializado, que garantice la atención y/o solución de incidentes y requerimientos (cambios en el sistema), solicitados por la Oficina de Tecnologías de la Información y Comunicaciones – OTIC.*
- *Contar con una garantía vigente para los equipos y servicios asociados activos, que forman parte de la solución de seguridad perimetral, durante el periodo de la ejecución del servicio.*
- *Garantizar la operatividad de los equipos que forman parte de la solución de seguridad perimetral a nivel de hardware, a través de los mantenimientos preventivos programados.*

5. ALCANCE Y DESCRIPCIÓN DE LOS BIENES A CONTRATAR:

5.1. Características técnicas mínimas:

CARACTERÍSTICA	ESPECIFICACIONES TÉCNICAS MÍNIMAS DE LA SOLUCIÓN DE SEGURIDAD PERIMETRAL
CANTIDAD	Dos (2) equipos de seguridad perimetral (tipo appliance) con características de Next Generation Firewall (NGFW) configurados en alta disponibilidad con consola de administración y monitoreo. Se entiende por alta disponibilidad, es decir por lo menos dos (2) equipos con las mismas características mínimas mencionadas en estas especificaciones.
CARACTERÍSTICAS GENERALES	<ul style="list-style-type: none"> - El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Network Firewall" o "Firewall de Redes" en los últimos 5 reportes, lo cual el postor debe acreditar en su oferta, adjuntando el reporte obtenido desde el portal oficial de "Gartner" y el enlace correspondiente. - El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls, lo cual el postor debe acreditar en su oferta, adjuntando el reporte obtenido desde el portal oficial de "Forrester". - Para efectos de la propuesta, los bienes que conformen la solución, deben estar vigentes en el mercado y posicionarse dentro de la familia de equipos de última generación en tecnologías publicadas por el fabricante, asimismo, ninguno de los modelos ofertados deberá estar discontinuados, listados ni anunciados en el sitio web del fabricante como fin de vida (end-of-life), no deberán estar en el fin de venta (end-of-sale) y no deberán estar en el fin de soporte (end-of-support), lo cual el postor debe acreditar en su oferta, adjuntando el reporte del fabricante. - Los equipos deben ser nuevos. No se aceptarán equipos o materiales reciclados, reensamblados o reacondicionados, tampoco se aceptarán aquellos que tenga la denominación "refurbished", "remarketing" o su equivalente. - El postor deberá ofertar equipos de última vigencia tecnológica; igualmente no se podrá ofertar versiones beta o que no sean de venta comercial por parte del fabricante. Dichas condiciones deberán ser acreditadas al momento de la suscripción del contrato. - No serán aceptadas soluciones basadas en software o equipos de propósito genérico (servidores o computadoras personales) sobre los cuales pueda instalarse y/o ejecutarse un sistema operativo regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X o cualquiera de las distribuciones basadas en GNU/Linux. - Para uso en rack (debe incluir todos los accesorios necesarios para instalación, incluyendo patch-cords de fibra y/o cobre y ópticos conectados hacia los switches core en redundancia y router), no se aceptarán equipos de tipo escritorio. La oferta incluye los accesorios y todos lo necesario para su funcionamiento. - El equipo solicitado debe tener el firmware en su versión más estable (actualizado). - El contratista deberá considerar el software del mismo fabricante del equipo firewall. - No se va implementar soluciones virtuales, todas serán de forma física en los gabinetes de la Entidad. - En ningún caso, se deben presentar soluciones con equipos que dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la instalación de los equipos a ser propuestos. Esto deberá ser respaldado oficialmente con una carta del mismo fabricante en el Entregable N° 1. - Debe incluir activación de los siguientes servicios como mínimo por el tiempo que dure el servicio: Protección de amenazas, Control de aplicaciones, IPS, Antivirus, VPN, Filtrado web, Optimización WAN, Traffic Shapping y Anti Spam (opcional), asegurando la disponibilidad vigente de todos los servicios que forme parte de los equipos de Seguridad Perimetral en alta disponibilidad.

	<ul style="list-style-type: none"> - La solución de seguridad perimetral debe permitir configuración en alta disponibilidad, tanto para IPv4 como para IPv6.
RENDIMIENTO	<ul style="list-style-type: none"> - Throughput de Next Generation Firewall de 2.2 Gbps 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. - Throughput de Prevención de Amenazas de 1 Gbps 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), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes. - Para el cumplimiento de performance, se deberá comprobar el cumplimiento de requerimiento de throughput a 1 Gbps, con documentación pública del fabricante, para lo cual el postor debe adjuntar en su oferta el reporte que acredite el performance y el enlace requerido. - El equipo debe soportar como mínimo 200 000 sesiones simultaneas y 37 500 sesiones por segundo.
CAPACIDADES	<ul style="list-style-type: none"> - El dispositivo de seguridad debe soportar VLAN Tags 802.1Q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. - Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). - Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/Active Directory, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones. - Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP. - La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red. - Debe permitir cifrar la comunicación entre dos Firewall de alta disponibilidad durante la sincronización de las configuraciones. - La solución propuesta debe permitir utilizar las capacidades de Firewall e IPs en IPv4 e IPv6.
ARQUITECTURA DEL EQUIPO	<p>Cada equipo appliance deberá poseer:</p> <ul style="list-style-type: none"> - Mínimo 08 interfaces de red 10/100/1000 Base T, formato RJ45 para tráfico de datos de la red - Mínimo 01 interfaz de red 1G en formato SFP. - Mínimo 01 interfaz de red de 1G Base T, formato RJ45 para la gestión del equipo. - Capacidad de almacenamiento mínimo de 120 GB - Debe contar con fuente de poder redundante. - La solución deberá contar con al menos una interfaz en formato SFP para la sincronización de alta disponibilidad.
FIREWALL	<ul style="list-style-type: none"> - Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.

	<ul style="list-style-type: none"> - Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención. - Permitir el agendamiento de las políticas de seguridad. - Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa. - Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. - Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría. - Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules). - Debe mostrar la primera y última vez que se utilizó una regla de seguridad. - Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad. - Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall. - Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
CONTROL DE APLICACIONES	<ul style="list-style-type: none"> - Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, video, proxy, mensajería instantánea, email. - Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2. - Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada. - Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389. - Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación. - Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.
PREVENCIÓN DE AMENAZAS	<ul style="list-style-type: none"> - Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot. - Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante. - Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia. - Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad. - Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems. - Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad. - Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS. - Los eventos deben identificar el país que origino la amenaza.

	<ul style="list-style-type: none"> - Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto. - Debe soportar la creación de firmas de IPS basadas en el formato de Snort. - Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
ANÁLISIS DE MALWARE	<ul style="list-style-type: none"> - La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing. - La plataforma de Sandboxing podrá ser ofrecido en Nube (Cloud), On-premise o ambos y 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. - En caso la plataforma Sandboxing sea cloud minimamente deberá garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, FedRAMP. - El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red. - Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante. - Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. - Debe permitir al administrador la descarga del archivo original analizado por el Sandbox. - Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. - Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado. - Permitir la subida de archivos al sandbox de forma manual y vía API.
FILTRO DE CONTENIDO WEB	<ul style="list-style-type: none"> - Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora). - Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local. - Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs. - Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing. - Debe permitir la creación de categorías personalizadas. - Debe soportar la categorización o crawling de URLs hasta en 40 idiomas. - Debe utilizar machine learning para analizar URL en tiempo real y clasificarlas en categorías benignas o maliciosas. - Debe ser capaz de bloquear URLs maliciosas no vistas con anterioridad, es decir, URLs que no hayan sido categorizadas previamente por el fabricante. - Debe poseer algoritmos que evalúen URLs en tiempo real para bloquear URLs no categorizadas por crawlers, inclusive URLs resistentes a técnicas de cloaking. - Debe incluir escaneo en línea basado en machine learning para detectar ataques de phishing no vistos antes. - Debe poseer capacidades anti evasivas para contener evasiones de cloaking, Captchas y codificación de caracteres. - Debe emplear modelos de aprendizaje automático para analizar imágenes en páginas web y determinar si están imitando marcas conocidas, previniendo intentos de phishing.

	<ul style="list-style-type: none"> - Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad perimetral. - Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site. - Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo ataques de phishing.
IDENTIFICACION DE USUARIOS	<ul style="list-style-type: none"> - Debe incluir la capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E-Novell Directory, Exchange y base de datos local. - Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente. - Soportar autenticación vía Active Directory/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
PROTECCIÓN ANTE ATAQUES DE DENEGACIÓN DE SERVICIO (QoS)	<ul style="list-style-type: none"> - Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood. - Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies/Proxy como medidas de defensa. - La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor). - Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo. - La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección. - Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route. - Debe 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.
VPN	<ul style="list-style-type: none"> - Debe incluir y configurar la opción de crear conexiones VPN hacia la red interna mediante IPsec y SSL. - No debe requerir ningún tipo de licencia para el establecimiento de VPN IPsec y SSL, deben ser ilimitados o se debe considerar la licencia para 500 usuarios. - Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPsec y SSL, para permitir el acceso remoto seguro para un mínimo de 500 usuarios las cuales serán autenticadas mediante sincronización con el Directorio Activo del Sineace, debiendo soportarse dispositivos Android, MacOS, iOS y Windows. - Las VPN client-to-site deben poder operar usando el protocolo IPsec y SSL, y permitir la conexión por medio de agente instalado en el sistema operativo. - El agente de VPN SSL o IPSEC client-to-site debe permitir ser instalado al menos en Windows, Mac OS, Linux, Android e IOS. De ser requerido, se debe incluir el licenciamiento necesario para permitir esta capacidad. - Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN. - La VPN IPsec debe soportar como mínimo: <ul style="list-style-type: none"> • DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard). • Autenticación MD5, SHA-1, SHA-2. • Diffie-Hellman Group 1, Group 2, Group 5 y Group 14. • Algoritmo Internet Key Exchange (IKEv1 & IKEv2). - Debe permitir los siguientes tipos de conexión del cliente al túnel VPN: <ul style="list-style-type: none"> • Antes del usuario se autentique en la estación. • Después de la autenticación del usuario en la estación usando Single Sign On (SSO). • Bajo demanda del usuario.

ADMINISTRACION Y CONSOLA	<ul style="list-style-type: none"> - La solución ofertada deberá contar con una consola centralizada para su administración. - Debe soportar y tener habilitado diferentes perfiles de administrador, incluyendo al menos los siguientes: read/write y/o read/only. - El equipo debe ser administrable tanto por CLI (Command Line Interface, Interfaz de línea de comando) como por GUI (Graphical User Interface, Interfaz Gráfica de Usuario). - La solución debe contar con interfaz gráfica de usuario (GUI), vía web por HTTP y/o HTTPS, compatible al menos con Windows, Linux y Mac OS. - 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. - La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML. - Acceso concurrente de administradores. - Debe permitir la definición de perfiles de acceso. - Debe permitir realizar backup de las configuraciones y rollback de configuración para la última configuración salvada. - Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política. - Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas.
MONITOREO	<ul style="list-style-type: none"> - Soporte SNMP. - 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. - La solución debe incluir la capacidad de poder monitorear la salud de los enlaces en términos de jitter, latencia y pérdida de paquetes, tomando decisiones inteligentes de enrutamiento basado en la condición de los enlaces de manera dinámica. - 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. - La solución debe contar con la posibilidad de hacer reportes del estado de los enlaces y aplicaciones, indicando volúmenes de datos con respecto a las veces que fueron degradados o afectados. - Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante. - Permitir exportar las reglas de seguridad en formato CSV y PDF.
CARACTERÍSTICAS SECUNDARIAS	<ul style="list-style-type: none"> - La solución debe ser alimentada por un servicio de inteligencia global capaz de identificar decenas de millones de dominios maliciosos con análisis en tiempo real sin depender de firmas estáticas. - Debe permitir la gestión del ancho de banda de los protocolos TCP y VoIP, permitiendo la definición de niveles mínimos y máximos. - Debe poseer políticas para bloquear dominios DGA o interrumpir las consultas de DNS a dichos dominios. - Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI. - Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.

	<ul style="list-style-type: none"> - Capacidad de poder cambiar dinámicamente de camino al detectar alguna degradación del enlace sin afectar o cortar la sesión establecida de la aplicación, es decir, que el usuario no perciba corte en la aplicación o tener que reiniciar la sesión. - Soportar de algoritmo de corrección de errores (FEC - Forward Error Correction) con el objetivo de poder garantizar una experiencia alta en el uso de aplicaciones de voz y video a través de la red de SD-WAN. - 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). - Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el contratista. - Se deberá proporcionar como mínimo dos cuentas de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante, así como exámenes y certificaciones. - El contratista deberá ejecutar la evaluación de buenas prácticas de forma semestral por el tiempo que dure la garantía, con el objetivo de proporcionar un servicio de mejora continua sobre las configuraciones de la solución de seguridad perimetral. En base a la evaluación realizada, se deberá coordinar la implementación de las configuraciones recomendadas por el fabricante, previa coordinación entre el contratista y la OTIC.
LICENCIA Y SUSCRIPCION	<ul style="list-style-type: none"> - Toda licencia que sea requerida por la solución deberá estar cubierta por el proveedor, sin incurrir costo o gasto alguno para la Entidad. - La licencia debe ser para usuarios ilimitados de firewall.
CABLES Y ACCESORIOS	<ul style="list-style-type: none"> - Incluir el material necesario (cables de conectividad, conectores de red y fibra, cable de consola, ópticos, otros) requeridos para la implementación y configuración de la solución de seguridad perimetral ofertada.

Otras consideraciones:

- El Contratista debe cumplir con lo señalado en el "Plan para la Vigilancia, Prevención y Control de la Salud de los trabajadores con riesgo a exposición a SARS-Cov-2, versión 3" vigente en la Entidad, el mismo que se encuentra disponible en el siguiente enlace: <https://www.gob.pe/institucion/sineace/normas-legales/2752157-000005-2022-sineace-p-gg>

5.2. Visita técnica:

La visita a las instalaciones del Sineace será facultativa para el contratista y podrán realizarse previa coordinación, teniendo en cuenta lo siguiente:

Área Encargada: Oficina de Tecnologías de la Información y Comunicaciones

Cargo: Coordinador de Proyectos de TIC, Especialista en Infraestructura Tecnológica y Analista de Servicios de TI

Teléfono: 637 1122 anexo 143

Correo electrónico: jsancheza@sineace.gob.pe, jportales@sineace.gob.pe y jpinto@sineace.gob.pe

5.3. Acondicionamiento, montaje o instalación:

Instalación e implementación de la solución:

Generalidades:

- La solución se instalará en el gabinete del Centro de Datos de la Entidad (ubicado en la Av. República de Panamá 3659 San Isidro), previa coordinación con personal de la Oficina Tecnologías de la Información y Comunicaciones de la Entidad, además el contratista deberá asignar a un jefe de proyecto o supervisor quien estará a cargo de la implementación de la solución ofertada y en constante coordinación con el Jefe de Proyecto del Sineace.
- Todos los servicios a los que está obligado el Contratista a cumplir con lo indicado en las especificaciones técnicas, serán sin costo adicional para la Entidad.
- A la firma de contrato, el contratista deberá presentar los seguros complementarios de trabajo de riesgo (SCTR) vigentes del personal técnico y durante la ejecución de trabajos, el personal técnico del contratista deberá presentarse con los equipos de protección personal (EPP).

- La Entidad no se responsabiliza por accidentes que pudieran sufrir el personal técnico o profesional del Contratista durante la ejecución de los trabajos en el Sineace.
- El contratista deberá subsanar en forma inmediata los daños ocasionados a los bienes (deterioro, daño, degradación) o responder civilmente a personas (golpes, heridas, otros traumas o perjuicios), que hayan sido ocasionados voluntaria o involuntariamente, durante implementación de la solución.
- La Oficina de Tecnologías de la Información y Comunicaciones de la Entidad asignará a su Jefe de Proyecto, quien será el encargado de las coordinaciones con el Jefe de Proyecto del Contratista, de modo que la implementación se ejecute en forma coordinada.
- El Contratista deberá trabajar de manera conjunta con el personal técnico de la Oficina de Tecnologías de la Información y Comunicaciones, el mismo que será asignado por el Jefe de Proyecto de la Entidad.
- El Contratista deberá de realizar la implementación, configuración, instalación y puesta en producción de la solución ofertada, previa coordinación con el Jefe de Proyecto de la Oficina de Tecnologías de la Información y Comunicaciones de la Entidad.
- El contratista es responsable del desmontaje de firewall actual (de ser necesario), ejecutar la configuración del firewall propuesto manteniendo todas las reglas y políticas de la plataforma de seguridad actual instalada, realizar la adecuación física, traslado, cableado estructurado y cableado eléctrico necesario para la instalación, integración y puesta en servicio de la solución ofertada con la infraestructura de la red de la Entidad, sin desestabilizar la red existente, sin afectar la continuidad del servicio y con protección adecuada de la red.
- Los equipos que requiera instalar el contratista para cumplir con la implementación de la solución ofertada, deben ser nuevos sin uso y deben llegar a las oficinas de la Entidad sin señales de uso anterior.
- Todos los drivers y software que formarán parte de la solución a instalar, deberán ser entregados a nombre del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa - Sineace, con su correspondiente licenciamiento.
- El contratista 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.
- Una vez terminados los trabajos de instalación, se realizarán los trabajos de puesta en marcha y puesta en producción de la solución a satisfacción de la Entidad.
- El Contratista se compromete a no efectuar cualquier tipo de cambio, transacción, modificación y adición de información a los archivos, programas y sistemas de aplicación, sin la respectiva autorización por escrito y por adelantado del Sineace. Asimismo, el Contratista se compromete a no facilitar a terceros, bajo ningún concepto, información alguna.
- El Contratista debe entregar el hardware, software y licencias necesarios para habilitar todas las características solicitadas, de tal manera que se puedan utilizar en cualquier momento durante la garantía y soporte la solución. La modalidad de ejecución es llave en mano, es decir el Contratista deberá dotar a la Entidad de todos los equipos, accesorios y componentes necesarios para la implementación de la solución ofertada, sin que esto ocasione un gasto adicional a la Entidad.
- Las licencias y/o suscripciones de software deben ser enviadas al correo: soporte@sineace.gob.pe

Solución de servicios de Hardware

Se deberá considerar las siguientes tareas como mínimas y adicionar todas las tareas que fueran necesarias para completar la instalación, implementación y puesta en producción de la solución ofertada, según especificaciones técnicas.

- Verificar la compatibilidad, conectividad e interoperabilidad de los recursos de hardware a todo nivel del equipamiento que comprenden la solución ofertada.
- Instalación y acondicionamiento de los equipos eléctricos necesarios para la puesta en marcha de la solución.
- Encendido y testeo global de la solución ofertada.
- Realizar el cableado respectivo entre los equipos: switches core en redundancia y router.
- Instalación y configuración de la solución de seguridad perimetral ofertada.
- Verificación de conectividad entre la solución de seguridad perimetral y los switches core en redundancia y router.
- Actualización de firmware a la última versión estable.
- El Contratista deberá dejar configurada la consola de administración para que esta sea accedida desde una IP de la Red del Sineace, se deberá realizar las pruebas respectivas.

Pruebas de la solución de seguridad perimetral

- Pruebas de redundancia de fuentes de poder.
- Pruebas de alta disponibilidad físicas y lógica de los equipos.
- Pruebas de failover.
- Pruebas de operatividad de la solución implementada.

Otros

- La instalación debe cumplir con las instrucciones y normas que demandan las marcas de los equipos que llenen los requisitos.

- Todos los materiales requeridos serán suministrados y transportados por el contratista. El Sineace no proporcionará material alguno para este requerimiento.
- Antes de iniciar el trabajo de implementación, todos los equipos y accesorios que ingresen para la ejecución de los trabajos de las instalaciones del Sineace serán revisados por el área usuaria, quienes verificarán la calidad y el estado del material.
- El Sineace no asumirá ninguna responsabilidad por las obligaciones que contraiga el contratista con su personal para la ejecución del requerimiento. Asimismo, el personal a cargo del contratista no tendrá dependencia de ninguna naturaleza con el Sineace.
- Es de absoluta responsabilidad del contratista mantener la continuidad del servicio, evitando conflictos laborales, por concepto de remuneraciones.
- El contratista tiene la obligación de entregar los ambientes, después de la culminación de los trabajos, totalmente limpios y sin ningún material de desecho, de lo contrario se aplicarán las penalidades correspondientes.
- El contratista deberá tomar las precauciones necesarias para evitar daños a terceros y/o a las propias instalaciones. En caso de presentarse éstos, las reparaciones correspondientes serán por cuenta del contratista, sin tener derecho a retribución por dichos trabajos.
- El contratista es responsable del suministro de materiales y demás accesorios puestos en el sitio para su utilización en la sede, su resguardo y preservación, será responsabilidad del contratista.
- El contratista es responsable de que los equipos y accesorios no sufran ningún daño o desperfecto durante la labor de instalación y puesta en producción, de igual manera de no producir daños en el lugar donde sea instalado, asumiendo el costo de la reparación en caso de producirse algún daño.

5.4. Garantía:

El contratista deberá otorgar una garantía mínima 1095 días calendario (equivalente a 3 años), la cual se contabilizará desde el día siguiente de firmada el acta de implementación de la solución y garantía. Dicha garantía cubre entre otros, la reparación y/o reposición del equipamiento y/o componentes ofertados que forman parte de la solución, en caso corresponda.

6. RECURSOS Y FACILIDADES A SER PROVISTOS POR LA ENTIDAD:

El Sineace para efectos de la instalación brindará los accesos necesarios al contratista:

- Espacio para la instalación del equipamiento.
- Energía Estabilizada en el gabinete del Centro de Datos.
- Acceso a los ambientes necesarios para la implementación.

7. FACILIDADES A SER PROVISTOS POR EL CONTRATISTA:

El Contratista deberá considerar el uso de sus propios recursos humanos, herramientas, útiles, materiales de trabajo y equipos para la ejecución de la adquisición en mención; por lo que la adquisición deberá ser presupuestado a todo costo, es decir sin ocasionar un costo adicional al propuesto de la Entidad.

8. PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL:

8.1. Mantenimiento preventivo

- El contratista deberá realizar 01 mantenimiento preventivo anual.
- El contratista deberá elaborar y entregar un plan de mantenimiento preventivo de los equipos que forman parte de la solución de seguridad perimetral, en el Entregable N° 2, de acuerdo al siguiente cronograma:

2. CRONOGRAMA DE MANTENIMIENTO											
Mes	1	2	3	4	5	6	7	8	9	10	11
Ejecución											X

- Los trabajos de mantenimiento serán realizados por un técnico especialista del contratista.
- El contratista se encuentra obligado a realizar un (1) mantenimiento anual, de acuerdo al cronograma a fin de asegurar el correcto funcionamiento del equipo, durante el tiempo de garantía, previa coordinación con la Oficina de Tecnologías de Información y comunicaciones, además, los servicios se realizarán fuera del horario laboral.
- El contratista deberá realizar el servicio contratado con materiales adecuados, siguiendo las recomendaciones del fabricante. También deberá emplear herramientas especializadas idóneas para la ejecución del servicio.
- Todos los materiales necesarios para llevar a cabo íntegramente las actividades consideradas como parte del mantenimiento preventivo deberán ser asumidos por el contratista.
- Antes de la ejecución de los trabajos de cada uno de los mantenimientos preventivos, el contratista deberá presentar los seguros complementarios de trabajo de riesgo (SCTR) vigentes del personal técnico y durante la ejecución de trabajos el personal técnico del contratista deberá presentarse con los equipos de protección personal (EPP).
- El mantenimiento debe incluir la actualización del firmware en el equipo, incluyendo el suministro de nuevas versiones (releases) y reparaciones (denominadas comercialmente como patches y/o updates), el cual se realizaría una vez al año.
- El servicio de mantenimiento preventivo deberá incluir necesariamente lo siguiente:

- La limpieza general externa de los equipos que forman parte de la solución de seguridad perimetral.
- Backup de la configuración del sistema
- Revisión y evaluación para diagnosticar el estado de los equipos para hardware y software.
- Aplicación de actualizaciones de firmware (nuevas versiones y patches).
- Pruebas de funcionamiento de los equipos que forman parte de la solución de seguridad perimetral como un sistema.
- El contratista de detectar un imperfecto o anomalía deberá realizar cualquier ajuste necesario para su corrección a nivel de hardware y/o software de acuerdo a los tiempos y plazos establecidos en los acuerdos de niveles de servicios - SLA.
- El contratista después de cada mantenimiento deberá presentar un Informe dirigido a la Oficina de tecnologías de la información y comunicaciones - OTIC, el cual debe describir:
 - Tareas realizadas por cada mantenimiento preventivo del equipamiento ofertado.
 - Observaciones y recomendaciones para la buena operatividad del equipamiento ofertado.
- Será presentado en Mesa de Partes del Sineace, ubicado en Av. República de Panamá N° 3659 - San Isidro, en horario corrido de lunes a viernes de 8:30 a.m. a 4:30 p.m., o en Mesa de Partes Virtual desde el siguiente enlace <https://app.sineace.gob.pe/portal-ciudadano/mesa-partes>.

8.2. Soporte técnico, acuerdos de niveles de servicios – SLA.

El soporte técnico se brindará durante los 365 días posteriores a la implementación de la solución, de acuerdo a lo siguiente:

- 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 la incidencia (avería) o requerimiento del servicio y proporcionará un número de ticket.
- El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.
- Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá al Sineace 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.
- Reparación de cualquier equipo o componente, incluye hardware y software, para su correcto funcionamiento.
- Reemplazo de cualquier equipo o componente, incluye hardware y software, que formen parte de la solución, cuando éstos no puedan ser reparados. Los reemplazos serán por equipos de iguales o mejores características, los mismos que quedarán en propiedad definitiva de la Entidad. Se considerará la marca, modelo y número de parte para efectos de compatibilidad.
- Cuando se realice un reemplazo en forma definitiva, el Contratista deberá informar a la Oficina de Tecnologías de Información y Comunicaciones, presentando un informe técnico que describa los motivos por el cual no puede ser reparado el activo; este informe deberá contener datos completos del equipo o componente instalado. Los equipos reemplazados deberán ser entregados a la Unidad de Logística - Control Patrimonial en presencia de personal de la Oficina de Tecnologías de Información y Comunicaciones para su validación técnica.
- La cobertura de atención del soporte técnico deberá ser del tipo 24x7 de lunes a domingo (24 horas, los 7 días de la semana y los 365 días del año por el tiempo que dure la garantía).
- Soporte técnico deberá ser especializado y realizarse vía asistencia remota y/o presencial.
- Durante el período de garantía comercial, debe contar con un Centro de Operaciones de Seguridad para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets.
- En cualquier caso, que se necesite retirar el equipo defectuoso, el contratista están en la obligación de entregar un equipo (backup o respaldo temporal) de su propiedad de características similares o superiores, e instalarlo dentro del tiempo máximo para solucionar el problema definido el "Acuerdos de nivel de servicio - SLA"; y por un tiempo máximo de cuarenta y cinco (45) días calendario, tiempo en el cual se dará solución definitiva entregando el equipo reparado o caso contrario reemplazándolo por otro equipo nuevo, sin uso, de características iguales o superiores. El equipo entregado debe quedar con el software que tenía instalado a tiempo de iniciar el servicio, debidamente configurado y puesto en operación.
- El postor deberá contar con un Centro de Operaciones de Seguridad (SOC certificado con ISO 27001) para el servicio de Soporte Técnico, con la finalidad de garantizar que se cuente con procesos de atención óptimos que asegure el cumplimiento de los tiempos de respuesta, la calidad de su atención, así como el aseguramiento de la confidencialidad e integridad del manejo de los datos y de la información de la Entidad.
- El servicio de soporte técnico incluirá un servicio de monitoreo y gestión de incidencias sobre la plataforma de seguridad perimetral, el cual deberá cumplir con los siguientes requisitos mínimamente:
 - El servicio de Centro de Operaciones de Seguridad (SOC) debe contar personal calificado propio del contratista para las labores de gestión y soporte técnico de la solución ofertada. No se aceptará SOC tercerizado.
 - Brindar una capa de SIEM para la retención de log, mínimo de 90 días.

- Brindar capas adicionales al SIEM como analítica de comportamiento de usuarios (UBA y/o UEBA⁸), orquestación, automatización y respuesta de seguridad (SOAR), Data Lake para procesar múltiples eventos de seguridad y mecanismos de detección propietarios basados en Inteligencia artificial totalmente integrados al servicio, sin costo adicional.
 - Con el objetivo de validar y dar seguimiento a las investigaciones de ciberseguridad, el postor deberá entregar un Portal web seguro con doble factor de autenticación para revisar las investigaciones.
 - El portal debe actuar como un front-end independiente de la capa tecnológica descrita en los puntos anteriores (SIEM, UBA y/o UEBA⁹, SOAR, data lake, I.A.).
 - El portal deberá mostrar investigaciones por el periodo de contrato para efectos de historial y permitir consultas como: fecha de creación, fecha de resolución, fuentes datos, estados, por lo menos 3 niveles de condición de defensa o DEFCON (normal, intermedio y crítica) asociado a las investigaciones y misiones pendientes de revisar.
 - Las investigaciones presentadas en el portal deberán incluir información del estado, tipo, analista asignado, fuente de datos asociada y si existen misiones (debe permitir notificar cualquier modificación del estado). Deberá también mostrar un resumen de la investigación detallando lo ocurrido, magnitud, conclusión y una sección donde se deberá incluir evidencia como archivos o indicadores. Finalmente, deberá mostrar una línea de tiempo con actividades asociadas a la investigación, así como las interacciones entre analistas de seguridad.
 - Monitoreo 24x7 identificando amenazas cibernéticas que puedan afectar la operación.
 - Inteligencia de amenazas mediante actualizaciones de indicadores de compromiso (IOC) de múltiples fuentes, CERT y Dark Web. Las fuentes de inteligencia de amenazas deberán ser enviadas al SIEM para correlacionar y generar detecciones. El postor deberá adjuntar a su propuesta técnica un listado de fuentes de inteligencia (mínimo 10) con las que operan.
 - Caza de amenazas sobre el SIEM, identificando, evaluando y mejorando la capacidad de detección mediante búsqueda exhaustiva de ciber-amenazas y actividades maliciosas.
 - Respuesta y mitigación de incidentes en tiempo real ante ciber-amenazas.
 - Optimización de procesos consistentes de desarrollo y aprendizaje que incluyan optimización de reglas, actualizaciones y sugerencias de implementación de nuevas tecnologías de detección de amenazas cibernéticas.
 - Investigación forense de procesos en curso de presuntas actividades maliciosas y amenazas cibernéticas incluyendo el análisis post mortem de incidentes verificados. Mínimo de 4 horas mensuales de ser requerido.
 - La solución deberá procesar logs de por lo menos 700 fuentes de datos en nube y/o¹⁰ locales. En caso no exista una integración, sin costo adicional, se deberá poder crear una personalización en no más de 90 días desde la solicitud y dentro del alcance del requerimiento.
 - Envío periódico de IOC del tipo email, dominio, URL, sha3-256, IP, MD5, SHA1 y SHA256 en formato STIX.
 - Brindar una llave API y/o¹¹ URL para digerir los IOC de forma automática
- También como parte del soporte, el postor deberá realizar una prueba de penetración continua, incluido el descubrimiento automático de activos, la identificación de la superficie de ataque, la minería y explotación de vulnerabilidades, que cumpla mínimamente con lo siguiente:
- Debe realizar pruebas de caja negra y gris, formando automáticamente rutas de ataque basadas en el aprendizaje de la red y los sistemas.
 - Las pruebas de penetración continua se deben realizar de 10 Host IP.
 - Debe admitir un proceso completamente automatizado que pueda minimizar el comportamiento de un pirata informático real para escanear/descubrir las exposiciones de la superficie de ataque de la máquina objetivo, las vulnerabilidades del sistema y luego explotar automáticamente las vulnerabilidades del sistema para validar el riesgo real de las máquinas objetivo.
 - Debe tener una base de conocimiento de complementos de vulnerabilidad/explotación con más de 36,000 complementos; cada complemento deberá incluir puntaje CVSS, vector CVSS, información de número CVE si está disponible; cada complemento tendrá un nivel de gravedad de vulnerabilidad y un nivel de control de riesgo de explotación asociado con él; el nivel de severidad del complemento debe tener Alto, Medio, Bajo e Informativo.
 - Debe admitir la explotación automática de vulnerabilidades y debe ser capaz de mostrar el progreso del exploit en tiempo real en su interfaz de usuario web.
 - Debe proporcionar información detallada para cada vulnerabilidad descubierta, incluidos, entre otros, el tipo de vulnerabilidad, la gravedad, la puntuación CVSS (Common Vulnerability Scoring System), el vector CVSS, la descripción, la solución, el enlace de referencia, así como la máquina objetivo vulnerable, la superficie de ataque y ruta de ataque para esta vulnerabilidad. La solución también debe proporcionar una herramienta de

⁸ De acuerdo a la consulta N° 27

⁹ De acuerdo a la consulta N° 28

¹⁰ De acuerdo a la consulta N° 33

¹¹ De acuerdo a la consulta N° 34

validación de vulnerabilidades que ayude al usuario a volver a validar la vulnerabilidad después de parchear el software.

- El servicio debe ejecutarse mínimamente durante 10 días calendarios, emitir el informe de las remediaciones que deben ser solucionadas por parte de la entidad; y posteriormente a ello realizar un segundo escaneo durante el mismo periodo y emitir un informe final del servicio.
- Los tiempos de atención y subsanación ante una incidencia (avería) o requerimiento reportada por personal de la Oficina de Tecnologías de la Información y Comunicaciones de la Entidad, se deberá realizar de acuerdo con los tiempos indicados en el SLA (Acuerdos de Nivel de Servicio) que se detalla a continuación:

Tiempo de atención:

Se entiende por tiempo de atención y/o respuesta máxima, al tiempo transcurrido que inicia con la notificación que la Entidad efectúa a través de los canales de comunicación (llamada telefónica y/o correo electrónico) para reportar un incidente (avería) o requerimiento y culmina con la asignación de un ticket de atención (registrado en el sistema de mesa de servicio o ayuda) a un técnico del contratista. Dicho tiempo no deberá exceder los treinta (30) minutos.

Tiempo de subsanación:

Se entiende por tiempo de subsanación y/o solución máxima, al tiempo transcurrido que inicia desde que se le asigna el ticket de atención (registrado en el sistema de mesa de servicio o ayuda) al técnico del contratista hasta la solución de la incidencia (avería) o atención del requerimiento, en base a los siguientes niveles de servicio:

1. **Baja:** La solución es operable, pero se requiere alguna funcionalidad o procedimiento o se tiene una consulta técnica o requerimiento o consultas sobre el funcionamiento de la solución, modos de uso, buenas prácticas, actualización de firmware del equipamiento, dudas en general; el tiempo de solución máximo es de noventa y seis (96) horas
2. **Normal:** La solución está operando de manera inadecuada, generando una alerta desde el mismo equipo o detectada por el personal técnico. Una alternativa de solución está disponible y es aceptable o correcciones técnicas/funcionales no críticas, es decir que el estado actual no perjudica el funcionamiento general de la solución; el tiempo de solución máximo es de cuarenta y ocho (48) horas.
3. **Alta:** La solución es operacional, pero su funcionalidad es inadecuada, impidiendo que las aplicaciones y/o servicios operen de forma correcta; el tiempo de solución máximo es de seis (6) horas.
4. **Urgente:** Algún servicio crítico que brinda la solución no es operacional, la producción está detenida, imposibilidad absoluta de acceso o el problema está causando un impacto en producción o en la continuidad del servicio; el tiempo de solución máximo es de cuatro (4) horas.

8.3. Capacitación y/o entrenamiento

Hasta 10 días calendario posterior a la firma del Acta de implementación de la solución y garantía¹², el contratista deberá brindar capacitación al personal del Sineace y emitir la respectiva constancia o certificado de dicha capacitación. El contratista deberá de realizar la capacitación; se debe considerar los siguientes cursos de forma obligatoria y para seis (6) participantes para el personal de la Oficina de Tecnologías de la Información y Comunicaciones:

- Capacitación teórica/práctico en instalación, administración, configuración, resolución de problemas y buenas prácticas de la Solución de Seguridad Perimetral ofertada, como mínimo de 24 horas lectivas.

La capacitación solicitada deberá ser dictada en formar presencial y/o virtual y por los especialistas técnicos que realizarán la implementación de la solución ofertada, en horarios especiales y en 02 grupos (03 personas por grupo), de manera que no afecte la continuidad del servicio de la Entidad. El contratista deberá facilitar los medios didácticos y materiales que se requieran para cumplir con los objetivos de la capacitación, incluir el material en digital para cada participante. Las capacitaciones deberán ser dictadas fuera de las instalaciones de la Entidad, en caso se realicen de forma presencial, en un lugar de entrenamiento que el contratista indique, dicho lugar deberá contar con las facilidades necesarias para el desarrollo del curso para todos los participantes.

El horario para la capacitación será establecido en coordinación con la Entidad. El contratista deberá otorgar certificados de participación para cada uno de los cursos indicando en el certificado el nombre completo del participante, nombre del curso, fechas en las que se realizó la capacitación y número de horas.

9. PERSONAL CLAVE:

¹² De acuerdo a la consulta N° 18

Un Jefe de proyecto: Responsable de la gestión integral de la implementación de la solución.

FORMACIÓN ACADÉMICA:

Requisito:

- Título universitario de la carrera de Ingeniería informática o electrónica o sistemas o computación y sistemas o telecomunicaciones.
- Colegiado.
- Certificación del Project Management Professional (PMP) vigente.

Acreditación:

- El Título Universitario será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/>. En caso el Título Universitario no se encuentre inscrito en el referido registro, se debe presentar la copia simple del diploma respectivo a fin de acreditar la formación académica requerida.
- Copia simple del certificado de habilidad profesional.
- Copia simple de la certificación del Project Management Professional (PMP)

Un Supervisor de servicio: Responsable de la Supervisión del servicio para las prestaciones accesorias.

FORMACIÓN ACADÉMICA:

Requisito:

- **Grado de bachiller¹³** o Título universitario de la carrera de Ingeniería informática o electrónica o sistemas o computación y sistemas o telecomunicaciones o técnico titulado en informática o electrónica o computación o telecomunicaciones o redes y comunicaciones de datos.
- Colegiado (de corresponder).
- Contar con dos (2) de las siguientes certificaciones: "ITIL Foundation Certificate" y/o "Lead Cybersecurity Professional Certificate" y/o "Service Desk Leader Professional Certificate" y/o "NSE 4 Network Security Professional" y/o "Remote Work Professional Certification – RWPC".

Acreditación:

- El Título Universitario será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: <http://www.titulosinstitutos.pe/>, según corresponda. En caso el Título universitario o Título Técnico no se encuentre inscrito en el referido registro, se debe presentar la copia simple del diploma respectivo a fin de acreditar la formación académica requerida.
- Copia simple del certificado de habilidad profesional.
- Copia simple de la certificación ITIL Foundation Certificate, Lead Cybersecurity Professional Certificate y Service Desk Leader Professional Certificate.

Un Especialista técnico de servicio: Responsable de la revisión, afinamiento, implementación, configuración y soporte técnico de la solución de seguridad perimetral.

FORMACIÓN ACADÉMICA:

Requisito:

- Bachiller de la carrera de Ingeniería informática o electrónica o sistemas o computación y sistemas o telecomunicaciones o técnico titulado en informática o electrónica o computación o telecomunicaciones o redes **y comunicaciones de datos¹⁴** o seguridad informática.
- Certificación vigente del fabricante de la solución ofertada.

Acreditación:

- El Grado de Bachiller o Título Técnico será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web

¹³ De acuerdo a la consulta N° 20

¹⁴ De acuerdo a la consulta N° 22

de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: <https://enlinea.sunedu.gob.pe/> o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : <http://www.titulosinstitutos.pe/>, según corresponda. En caso el Grado de Bachiller o Título Técnico no se encuentre inscrito en el referido registro, se debe presentar la copia simple del diploma respectivo a fin de acreditar la formación académica requerida.

- Copia simple de la certificación vigente del fabricante de la solución ofertada.

10. REQUISITOS DE CALIFICACIÓN:

10.1. Experiencia en la especialidad

Requisito:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 360,000.00 (Trescientos Sesenta Mil con 00/100 Soles) por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 37,000.00 (Treinta y Siete Mil con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.

Se consideran bienes similares a los siguientes: Firewall, UTM, Switches Administrables, Equipos de seguridad perimetral.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹⁵ correspondientes a un máximo de veinte (20) contrataciones.

10.2. Capacidad técnica y profesional.

Experiencia del Personal Clave:

UN JEFE DE PROYECTO:

Requisito:

- Tres (3) años de experiencia específica en lo siguiente: Gestión de proyectos de TI y/o proyectos de seguridad perimetral y/o jefe de proyectos de implementación de soluciones de seguridad perimetral y/o soluciones de seguridad gestionada y/o soluciones de seguridad de infraestructura de red y/o servicios de tecnología y/o proyectos de seguridad gestionada y/o perimetral y/o seguridad informática.

Acreditación:

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

UN SUPERVISOR DE SERVICIO:

Requisito:

¹⁵ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

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

(...)

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

- Tres (3) años de experiencia específica a lo siguiente: Supervisor de proyectos de seguridad informática y/o coordinador de servicio y/o soluciones de seguridad gestionada y/o soluciones de seguridad de infraestructura de red y/o servicios de tecnología y/o proyectos de seguridad gestionada y/o perimetral y/o seguridad informática y/o soporte técnico de soluciones de seguridad informática y/o perimetral.

Acreditación:

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

UN ESPECIALISTA TÉCNICO DE SERVICIO:

Requisito:

- Dos (2) años de experiencia específica a lo siguiente: Implementador o responsable de instalación y/o configuración de soluciones de seguridad perimetral y/o soluciones de seguridad gestionada y/o soluciones de seguridad de infraestructura de red y/o proyectos de seguridad gestionada y/o perimetral y/o seguridad informática.

Acreditación:

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

11. LUGAR DE ENTREGA:

La entrega se realizará en el almacén del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa - Sineace, sitio en Av. República de Panamá 3659-3663, Distrito de San Isidro, de lunes a viernes de 08:30 a 16:30 horas. Asimismo, la implementación se realizará en el Centro de Datos del Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa - Sineace, sitio en Av. República de Panamá 3659-3663, Distrito de San Isidro, previa coordinación con la Oficina de Tecnologías de la Información y Comunicaciones – OTIC.

12. PLAZO DE ENTREGA:

Plazo de ejecución de la prestación principal

El plazo de entrega, instalación, configuración y puesta en producción del equipamiento es hasta sesenta (60) días calendario, de acuerdo a lo siguiente:

- **Entregable N° 1:** El Plan de Trabajo deberá ser entregado hasta los cinco (05) días calendario, contados desde el día siguiente de suscrito el contrato, el mismo que deberá ser aprobado por la Oficina de Tecnologías de la Información y Comunicaciones (OTIC) hasta dos (02) días hábiles posterior a la entrega de dicho plan, a través de una comunicación vía correo electrónico o un documento formal.
- **Entregable N° 2:** Los documentos que forman parte del entregable N° 2 deberán ser entregados hasta los cincuenta y cinco (55) días calendarios, contabilizados desde el día siguiente de la aprobación del Plan de Trabajo.

Plazo de ejecución de la prestación accesoria

El plazo de ejecución total del mantenimiento preventivo y soporte técnico es de un (1) año (365 días calendario), contados a partir del día siguiente de la firma del Acta de implementación de la solución y garantía, de acuerdo con lo siguiente:

- **Entregable N° 3:** Será presentado como máximo hasta ciento ochenta y uno (181) días calendarios, contabilizados a partir del día siguiente de suscrito el Acta de implementación de la solución y garantía.
- **Entregable N° 4:** Será presentado como máximo hasta ciento ochenta y cuatro (184) días calendarios, contabilizados a partir de la fecha máxima de vencimiento del Entregable N° 3.

13. ENTREGABLE:

El contratista deberá presentar cuatro (4) entregables:

Entregable N° 1:

El contratista deberá presentar una carta, adjuntado los siguientes documentos:

- Plan de trabajo para la instalación, configuración, migración y puesta en producción de la solución ofertada, deberá incluir como mínimo:
 - Carta de fabricante en la cual se acredite que los equipos que forman parte de la solución no dejen de ser fabricadas, comercializadas y/o soportadas durante los 5 años siguientes a la implementación de los equipos.
 - Detalle del desglose de tareas, asunciones y requisitos para el inicio del proyecto.

- Describir los procesos/actividades requeridos para cumplir con el alcance y los tiempos del proyecto respecto a instalación, configuración, migración y puesta en producción.
- Cronograma de trabajo, con el detalle las actividades generales y específicas, el cual debe contemplar la fecha, tiempo en minutos y horas por cada actividad. Dentro del cronograma se debe incluir como actividad la entrega del SCTR.
- Presentación del equipo de trabajo que formará parte de la ejecución del servicio.
- Relación de materiales y herramientas a utilizar.
- Diseño y situación de red actual.
- Diagrama de red lógica y física.

Entregable N° 2:

El contratista deberá presentar una carta al terminar la etapa de instalación, configuración y puesta en producción de la solución ofertada, adjuntando los siguientes documentos:

- Documento que acredite la entrega de los equipos que forman parte de la solución.
- Documento que acredite la garantía de los equipos que forman parte de la solución.
- Plan de Mantenimiento Preventivo del equipamiento que forma parte de la solución ofertada.
- Informe técnico final de Instalación, configuración y puesta en producción de la solución ofertada que el contratista deberá entregar al finalizar la implementación y antes de emitir el acta de implementación de la solución y garantía, con el siguiente detalle:
 - Diagrama topológico de interconexión de la solución.
 - Configuración y puesta en operación de la solución.
 - Informe de diseño de arquitectura (diagramas de componentes, red, topología física y lógica de la solución)
 - Plan de aceptación de funcionalidades: Estará conformado por un formato de aceptación que incluye las pruebas realizadas sobre las funcionalidades de la solución ofertada, verificando:
 - Pruebas de rendimiento
 - Pruebas de tiempo de respuesta
 - Pruebas de accesibilidad
 - Pruebas de monitoreo
 - Pruebas de reportes
 - Pruebas de conectividad de red.
 - Pruebas de alta disponibilidad.
 - Manual de Administración de la solución implementada.
 - Compromiso de la ejecución del mantenimiento preventivo de la solución ofertada (Deberá presentar una Declaración Jurada).
- Lista de contactos para el soporte técnico, con los niveles de escalamiento para las atenciones por parte del contratista, durante el periodo de garantía, de acuerdo a lo indicado en las especificaciones técnicas del presente documento.
- Acta de implementación de la solución y garantía, firmada por el contratista y el Sineace, luego de culminada la instalación, implementación y puestas en producción de la solución ofertada, posterior a la elaboración del informe técnico final.
- Documento que acredite la capacitación brindada para la solución ofertada, según especificidades técnicas.
- Compromiso de confidencialidad suscrita previa a la implementación (Deberá presentar Declaración Jurada)

Entregable N° 3:

El contratista deberá presentar una carta, adjuntando el siguiente documento:

- Documento que acredite la capacitación brindada para la solución ofertada, según especificidades técnicas¹⁶.
- Informe con el reporte de incidentes y/o requerimientos de la solución implementada del primer semestre de servicio de soporte técnico, el cual debe contener el detalle de cada incidente y/o requerimiento, estado, solución y/o atención y tiempo de atención, con sus conclusiones y recomendaciones.

Entregable N° 4:

El contratista deberá presentar una carta, adjuntando los siguientes documentos:

- Informe con el reporte de incidentes y/o requerimientos de la solución implementada del segundo semestre de servicio de soporte técnico, el cual debe contener el detalle de cada incidente y/o requerimiento, estado, solución y/o atención y tiempo de atención, con sus conclusiones y recomendaciones.
- Informe con las tareas realizadas en el mantenimiento preventivo de equipamiento de la solución ofertada, que incluya observaciones y recomendaciones para la buena operatividad de la solución.

Los entregables serán dirigidos a la Oficina de Tecnologías de la Información y Comunicaciones (OTIC), y deberán ser entregados a través de la Mesa de Partes física o Virtual, de acuerdo a lo siguiente:

Mesa de partes física:

¹⁶ De acuerdo a la consulta N° 18

De lunes a viernes de 08:30 a 16:30 horas, en la Av. República de Panamá N° 3659 – distrito de San Isidro, provincia y departamento de Lima.

Mesa de partes virtual:

A través del siguiente enlace: <https://www.gob.pe/20416-acceder-a-mesa-de-partes?child=9385>

14. CONFIDENCIALIDAD:

La confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros. El contratado, debe dar cumplimiento a todas las políticas y estándares definidos por el Sineace, en materia de seguridad de la información.

Esta obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, diagnósticos, documentos, cuadros comparativos y demás datos compilados o recibidos por el contratado.

15. RESPONSABILIDAD POR VICIOS OCULTOS

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de tres (3) años, contado a partir de la conformidad otorgada por la Entidad.

16. COORDINACIONES:

Las coordinaciones sobre las especificaciones técnicas, la ejecución u otros respecto a la prestación solicitada, podrá realizarla teniendo en cuenta lo siguiente:

- Área Encargada: Oficina de Tecnologías de la Información y Comunicaciones (OTIC).
- Cargo: Coordinador o especialista o analista.
- Teléfono: 637-1123 (Anexo 143).
- Correo electrónico: jsancheza@sineace.gob.pe / jportales@sineace.gob.pe / jpinto@sineace.gob.pe

17. SUPERVISIÓN:

La supervisión estará a cargo del siguiente personal:

- Área Encargada: Oficina de Tecnologías de la Información y Comunicaciones – OTIC.
- Cargo: Coordinador o especialista o analista.

18. CONFORMIDAD:

La conformidad de la prestación la otorgará el Jefe de Oficina de Tecnologías de la Información y Comunicaciones, previo informe de supervisión del coordinador o especialista o analista de la Oficina de Tecnologías de la Información y Comunicaciones. Asimismo, dicha conformidad estará acompañada por la "Conformidad de Ingreso de bienes".

19. FORMA DE PAGO:

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en pagos parciales, en tres (03) armadas, de acuerdo a lo siguiente:

Pago N° 01: Por la presentación del entregable 1 y 2, correspondiente al 95%, del monto total de la contratación, el monto incluye los impuestos de ley, previa conformidad otorgada por el área usuaria.

Pago N° 02: Por la presentación con del entregable 3, correspondiente al 2%, del monto total de la contratación, el monto incluye los impuestos de ley, previa conformidad otorgada por el área usuaria.

Pago N° 03: Por la presentación con del entregable 4, correspondiente al 3%, del monto total de la contratación, el monto incluye los impuestos de ley, previa conformidad otorgada por el área usuaria.

20. PENALIDAD POR MORA EN LA EJECUCIÓN:

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. La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = (0.10 \times \text{monto}) / (F \times \text{plazo en días})$$

Donde F tiene los siguientes valores:

- Para plazos menores o iguales a sesenta (60) días: F=0.40
- Para plazos mayores a sesenta (60) días: F=0.25

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

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

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

Cuando se llegue a cubrir el monto máximo de la penalidad, la Entidad podrá resolver el contrato por incumplimiento.

21. OTRAS PENALIDADES

Se aplicarán penalidades en caso que el contratista incurra en deficiencias en la ejecución del soporte técnico, los parámetros establecidos para ello serán de acuerdo a los niveles de servicio tipificados en el numeral "8.2. Soporte técnico, acuerdos de niveles de servicios - SLA", se ha establecido las siguientes penalidades frente a la infracción de algún nivel servicio.

ITEM	Plazo máximo (horas)	Nivel de Servicio	Incumplimiento	Penalidad	Procedimiento
1	96	BAJA: La solución es operable, pero se requiere alguna funcionalidad o procedimiento o se tiene una consulta técnica o requerimiento o consultas sobre el funcionamiento de la solución, modos de uso, buenas prácticas, actualización de firmware del equipamiento, dudas en general.	Superar el plazo máximo de atención para Nivel de Servicio BAJA.	Se aplicará una penalidad de 1 % de la UIT vigente por cada ticket que no ha sido subsanado en el mes del servicio, dentro de los plazos indicados en los Acuerdos de Niveles de Servicio (SLA).	Revisión del Informe semestral de reporte de incidentes y/o requerimientos de la solución implementada del servicio de soporte técnico y mantenimiento correctivo, remitido por el contratista.
2	48	NORMAL: La solución está operando de manera inadecuada, generando una alerta desde el mismo equipo o detectada por el personal técnico. Una alternativa de solución está disponible y es aceptable o correcciones técnicas/funcionales no críticas, es decir que el estado actual no perjudica el funcionamiento general	Superar el plazo máximo de atención para Nivel de Servicio NORMAL.	Se aplicará una penalidad de 3 % de la UIT vigente por cada ticket que no ha sido subsanado en el mes del servicio, dentro de los plazos indicados en los Acuerdos de Niveles de Servicio (SLA).	Revisión del Informe semestral de reporte de incidentes y/o requerimientos de la solución implementada del servicio de soporte técnico y mantenimiento correctivo, remitido por el contratista.

		de la solución.			
3	6	ALTA: La solución es operacional, pero su funcionalidad es inadecuada, impidiendo que las aplicaciones y/o servicios operen adecuadamente.	Superar el plazo máximo de atención para Nivel de Servicio ALTA.	Se aplicará una penalidad de 5 % de la UIT vigente por cada ticket que no ha sido subsanado en el mes del servicio, dentro de los plazos indicados en los Acuerdos de Niveles de Servicio (SLA).	Revisión del Informe semestral de reporte de incidentes y/o requerimientos de la solución implementada del servicio de soporte técnico y mantenimiento correctivo, remitido por el contratista.
4	4	URGENTE: Algún servicio crítico que brinda la solución no es operacional, la producción está detenida, imposibilidad absoluta de acceso o el problema está causando un impacto en producción o en la continuidad del servicio.	Superar el plazo máximo de atención para Nivel de Servicio URGENTE.	Se aplicará una penalidad de 10 % de la UIT vigente por cada ticket que no ha sido subsanado en el mes del servicio, dentro de los plazos indicados en los Acuerdos de Niveles de Servicio (SLA).	Revisión del Informe semestral de reporte de incidentes y/o requerimientos de la solución implementada del servicio de soporte técnico y mantenimiento correctivo, remitido por el contratista.

22. CLAUSULA ANTICORRUPCIÓN

- A. 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.
- B. 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 N° 30225, Ley de Contrataciones del Estado, aprobado por Decreto Supremo N°344-2018-EF.
- C. El Contratista se compromete a comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas.

23. MODALIDAD DE CONTRATACIÓN

Llave en mano.

24. SISTEMA DE CONTRATACIÓN.

Suma Alzada.

25. DOCUMENTACIÓN DE PRESENTACION OBLIGATORIA (DOCUMENTACIÓN ADICIONAL).

- Reportes obtenidos desde el portal oficial de "Gartner" y el enlace correspondiente, donde se acredite que el fabricante debe pertenecer al cuadrante de líderes de Gartner para "Network Firewall" o "Firewall de Redes" (últimos 5 reportes).
- Reporte obtenido desde el portal oficial de "Forrester" y enlace correspondiente, donde se acredite que el fabricante debe estar catalogado como líder en el último informe de Forrester Wave Enterprise Firewalls

- Reporte del fabricante donde se acredite que ninguno de los modelos ofertados deberá estar descontinuados, listados ni anunciados en el sitio web del fabricante como fin de vida (end-of-life), no deberán estar en el fin de venta (end-of-sale) y no deberán estar en el fin de soporte (end-of-support).
- Reporte que acredite el cumplimiento del requerimiento de throughput a 1 Gbps y el enlace correspondiente.

26. DOCUMENTACIÓN ADICIONAL PARA LA FIRMA DEL CONTRATO.

- Documentos que acrediten la formación académica del personal clave.
- Carta del fabricante la cual acredite que los equipos deben ser comercializados de última vigencia tecnológica.
- Seguros complementarios de trabajo de riesgo (SCTR) vigentes.

3.2. REQUISITOS DE CALIFICACIÓN

B.	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 360,000.00 (Trescientos Sesenta Mil con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 37,000.00 (Treinta y Siete Mil con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran bienes similares a los siguientes Firewall, UTM, Switches Administrables, Equipos de seguridad perimetral.</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 compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹⁷ 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 suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p>

¹⁷ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

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

(...)

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

	<p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”, debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <div data-bbox="292 936 1385 1099" style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <p><i>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”.</i></p> </div>
--	--

C.	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>UN JEFE DE PROYECTO: Tres (3) años de experiencia específica en lo siguiente: Gestión de proyectos de TI y/o proyectos de seguridad perimetral y/o jefe de proyectos de implementación de soluciones de seguridad perimetral y/o soluciones de seguridad gestionada y/o soluciones de seguridad de infraestructura de red y/o servicios de tecnología y/o proyectos de seguridad gestionada y/o perimetral y/o seguridad informática.</p> <p>UN SUPERVISOR DE SERVICIO: Tres (3) años de experiencia específica a lo siguiente: Supervisor de proyectos de seguridad informática y/o coordinador de servicio y/o soluciones de seguridad gestionada y/o soluciones de seguridad de infraestructura de red y/o servicios de tecnología y/o proyectos de seguridad gestionada y/o perimetral y/o seguridad informática y/o soporte técnico de soluciones de seguridad informática y/o perimetral.</p> <p>UN ESPECIALISTA TÉCNICO DE SERVICIO: Dos (2) años de experiencia específica a lo siguiente: Implementador o responsable de instalación y/o configuración de soluciones de seguridad perimetral y/o soluciones de seguridad gestionada y/o soluciones de seguridad de infraestructura de red y/o proyectos de seguridad gestionada y/o perimetral y/o seguridad informática.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <div data-bbox="292 1942 1426 2065" style="border: 1px solid black; padding: 5px;"> <p>Importante</p> <ul style="list-style-type: none"> <i>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</i> </div>

	<p><i>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.</i></p> <ul style="list-style-type: none"> <i>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.</i> <i>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</i>
--	---

CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

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

CAPÍTULO V PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación de “ADQUISICIÓN DE UNA SOLUCIÓN DE SEGURIDAD PERIMETRAL”, que celebra de una parte el Sistema Nacional de Evaluación, Acreditación y Certificación de la Calidad Educativa – Sineace, en adelante LA ENTIDAD, con RUC N° 20551178294, con domicilio legal en la Av. República de Panamá N° 3659 – distrito de San Isidro, provincia y departamento de Lima, 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° 0006-2023-SINEACE-1** para la Adquisición de una Solución de Seguridad Perimetral, 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 la Adquisición de una Solución de Seguridad Perimetral.

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 PAGO¹⁸

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en PAGOS A CUENTA, luego de la recepción formal y completa de la documentación correspondiente, según lo

¹⁸ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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.

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 60 días calendarios, el mismo que se computa desde el **DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO**.

CLÁUSULA ...: PRESTACIONES ACCESORIAS

Las prestaciones accesorias tienen por objeto brindar el mantenimiento preventivo, Soporte técnico, acuerdos de niveles de servicios – SLA, y Capacitación y/o entrenamiento.

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 un (01) año (365 días calendario), contados a partir del día siguiente de la firma del Acta de implementación de la solución y garantía

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 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.

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 el Especialista en Almacén y Control Patrimonial a cargo del almacén único de la Entidad, y la conformidad será otorgada por el Jefe de la Oficina de Tecnologías de la Información y Comunicaciones – OTIC, en el plazo máximo de SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN días de producida la recepción.

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

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

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

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

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

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

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

Importante

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

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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

ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹⁹

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

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

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

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con todos los gastos que demande esta formalidad.

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen durante la ejecución del presente contrato:

DOMICILIO DE LA ENTIDAD: [.....]

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

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

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

“LA ENTIDAD”

“EL CONTRATISTA”

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales²⁰.

¹⁹ 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).

²⁰ 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° 0006-2023-SINEACE-1

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 ²¹		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 compra²²

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.

²¹ 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.

²² Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de 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° 0006-2023-SINEACE-1

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 ²³		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²⁴		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ²⁵		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:

²³ 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.

²⁴ Ibidem.

²⁵ Ibidem.

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra²⁶

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.

²⁶ 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° 0006-2023-SINEACE-1
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° 0006-2023-SINEACE-1

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 la Adquisición de una Solución de Seguridad Perimetral, 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° 0006-2023-SINEACE-1

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 60 días calendario.

[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° 0006-2023-SINEACE-1

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° 00006-2023-SINEACE-1**

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] [%]²⁷

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES 100%²⁹

[CONSIGNAR CIUDAD Y FECHA]

²⁷ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

²⁹ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

Importante

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

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 0006-2023-SINEACE-1

Presente.-

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

CONCEPTO	PRECIO TOTAL
Prestacion Principal: Adquisición de una Solución de Seguridad Perimetral	
Prestaciones accesorias: Mantenimiento preventivo	
Prestaciones accesorias: Soporte técnico	
Prestaciones accesorias: Capacitación / Entrenamiento.	
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]”.
- “El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias”.*

ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 0006-2023-SINEACE-1
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ³⁰	FECHA DE LA CONFORMIDAD DE SER EL CASO ³¹	EXPERIENCIA PROVENIENTE ³² DE:	MONEDA	IMPORTE ³³	TIPO DE CAMBIO VENTA ³⁴	MONTO FACTURADO ACUMULADO ³⁵
1										
2										
3										
4										

³⁰ 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.

³¹ 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.

³² 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”*.

³³ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

³⁴ 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.

³⁵ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ³⁰	FECHA DE LA CONFORMIDAD DE SER EL CASO ³¹	EXPERIENCIA PROVENIENTE ³² DE:	MONEDA	IMPORTE ³³	TIPO DE CAMBIO VENTA ³⁴	MONTO FACTURADO ACUMULADO ³⁵
5										
6										
7										
8										
9										
10										
	...									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 9

DECLARACIÓN JURADA (NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 0006-2023-SINEACE-1
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 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° 0006-2023-SINEACE-1

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° 0006-2023-SINEACE-1

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.

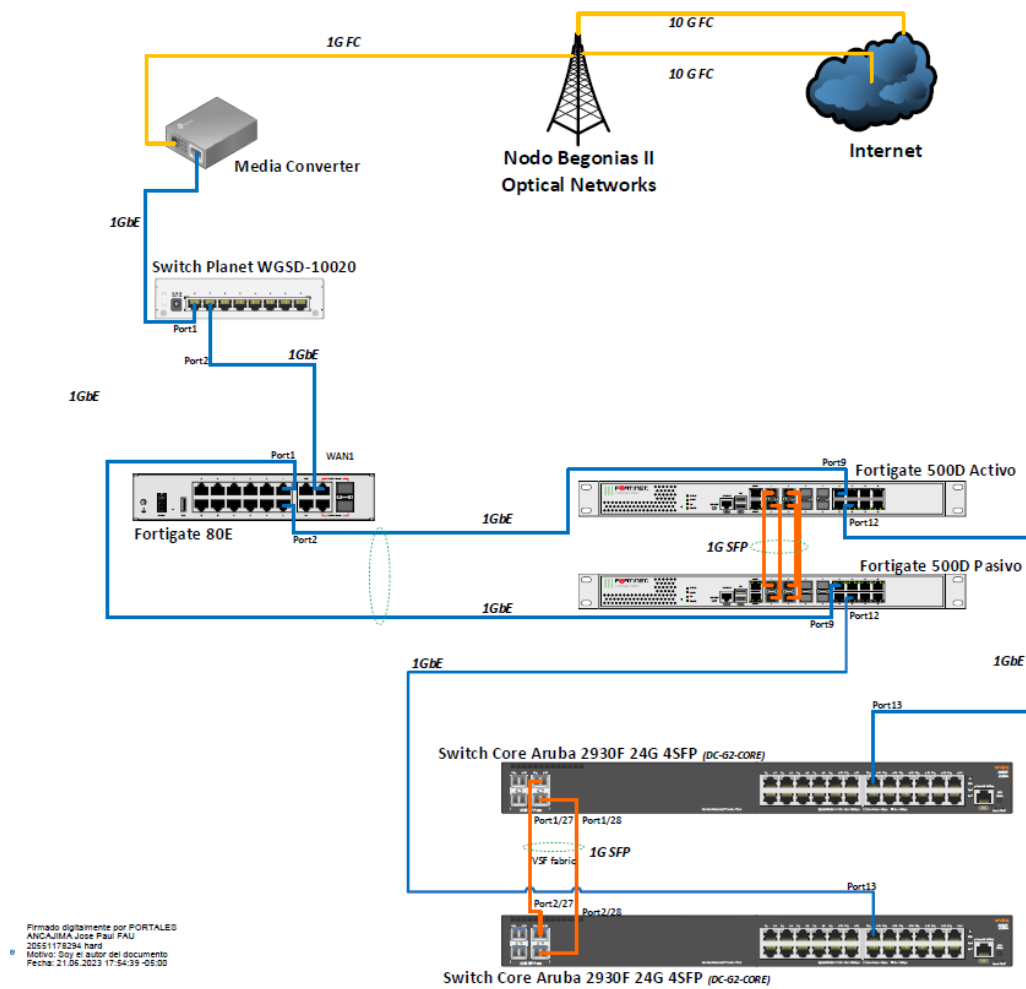
[CONSIGNAR CIUDAD Y FECHA]

.....
**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.

TOPOLOGÍA ACTUAL DE CONECTIVIDAD³⁶



³⁶ De acuerdo a la consulta N° 8 y 12