

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

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



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



SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	Importante • Abc	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	Advertencia • Abc	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	Importante para la Entidad • Xyz	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

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

Elaboradas en enero de 2019

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

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

LICITACIÓN PÚBLICA N°06-2023-SIS-1

CONTRATACIÓN DE BIENES

Adquisición de Solución de Seguridad Perimetral para la Sede Central
del SIS



DEBER DE COLABORACIÓN

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

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

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

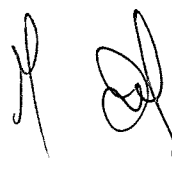
La Entidad y todo proveedor que se someta a las presentes Bases, sea como participante, postor y/o contratista del proceso de contratación deben permitir al OSCE o a la Secretaría Técnica de la Comisión de Defensa de la Libre Competencia del INDECOPI el acceso a la información referida a las contrataciones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



SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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



CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

Importante

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

El participante presentará su oferta de manera electrónica a través del SEACE, desde las

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>

00:01 horas hasta las 23:59 horas del día establecido para el efecto en el cronograma del procedimiento; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo a lo requerido en las bases.

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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



1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

Importante

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



CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

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

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

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

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

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

Advertencia

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

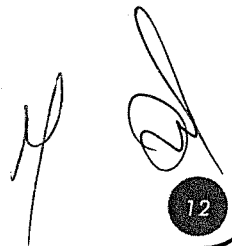
3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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



**CAPÍTULO I
GENERALIDADES****1.1. ENTIDAD CONVOCANTE**

Nombre : SEGURO INTEGRAL DE SALUD
RUC N° : 20505208626
Domicilio legal : Av. Paseo de la Republica Nro. 1645 Urb. Balconcillo – La Victoria
Teléfono: : (01) 514 5555
Correo electrónico: : consultor_ogar_log80@sisext.pe;
consultor_ogar_log09@sisext.pe;
mmallma@sis.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de la Adquisición de Solución de Seguridad Perimetral para la Sede Central del SIS

ITEM	PRESTACIÓN	DESCRIPCION	UNIDAD DE MEDIDA	Cantidad
Único	Principal	Solución de Seguridad Perimetral	Unidad	01
	Accesoria	Soporte Técnico	Servicio	01
		Mantenimiento Preventivo	Servicio	03
		Capacitación	Horas	36

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Formato N° 02 (042-2023-SIS-OGAR-UA), de fecha 13 de diciembre de 2023.

1.4. FUENTE DE FINANCIAMIENTO

RECURSOS ORDINARIOS

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. MODALIDAD DE EJECUCIÓN

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

Los bienes materia de la presente convocatoria se entregarán en concordancia con lo establecido en el expediente de contratación, en el siguiente plazo:

Prestación Principal: Entrega, instalación y puesta en operación de la Solución de Seguridad Perimetral

El contratista deberá presentar un plan de trabajo a los 10 días calendarios contados a partir del día siguiente de suscrito el contrato. En caso de que el contratista no cumpla con los plazos indicados previamente, se aplicará penalidad según numeral 5.9.2.

El contratista deberá realizar la entrega de los bienes en un plazo máximo de 90 días calendario, contados a partir del día siguiente de suscrito el contrato. En caso de que el contratista no cumpla con los plazos indicados, se aplicara penalidad según numeral 5.8. Hasta el día siguiente de concluida la entrega, la OGTI y el contratista suscribirán el Acta de Entrega de bienes.

El contratista deberá realizar la instalación de los bienes en un plazo máximo de 20 días calendario, contados a partir del día siguiente de suscrito el Acta de Entrega de bienes. En caso de que el contratista no cumpla con los plazos indicados, se aplicara penalidad según numeral 5.8. Hasta el día siguiente de concluida la instalación, la OGTI y el contratista suscribirán el Acta de instalación de bienes.

El contratista deberá realizar la puesta en operación de los bienes en un plazo máximo de 10 días calendario, contados a partir del día siguiente de suscrito el Acta de instalación de bienes. En caso de que el contratista no cumpla con los plazos indicados, se aplicara penalidad según numeral 5.8. Hasta el día siguiente de concluida la puesta en operación, la OGTI y el contratista suscribirán el Acta de conformidad técnica de la prestación principal (siempre y cuando no exista ningún inconveniente).

Plazo de entrega del equipo	120 días calendario
Plazo de entrega	90 días calendario
Instalación de los bienes	20 días calendario
Puesta en operación.	10 días calendario

Prestación Accesoría N° 01: Soporte Técnico

El contratista deberá realizar el servicio de soporte, durante un plazo de 1095 días calendarios, equivalente a 03 años, contados a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal". Por el incumplimiento de los tiempos de atención y solución se aplicará la penalidad establecida en el numeral 5.9.1.

Prestación Accesoría N°02: Mantenimientos Preventivos

El contratista deberá realizar un total de 03 mantenimientos a todos los equipos y componentes objeto del contrato (hardware y software) en un plazo de 1095 días calendarios, equivalente a 03 años (01 por año), contados a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal". El proveedor deberá realizar las actividades respectivas 60 días antes de culminado el periodo anual.

Prestación Accesoría N°03: Capacitación

A partir del día siguiente de firmada el "Acta de conformidad técnica", el contratista contará con hasta 30 días calendario para realizar las capacitaciones al personal técnico de la OGTI.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar de manera gratuita un ejemplar de las bases, para cuyo efecto deben solicitarlo en la Unidad Funcional de Abastecimiento, en el horario de oficina, sitio en Av. Paseo de la Republica N° 1645 – Lima-Lima- La Victoria.

Importante

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

1.11. BASE LEGAL

- Ley N° 31638, Ley de Presupuesto del Sector Público para el año fiscal 2023.
- Ley N° 31639, Ley de Equilibrio Financiero del Presupuesto del Sector Público para el año fiscal 2023.
- Decreto Supremo N° 082-2019-EF, que aprueba el Texto Único Ordenado de la Ley de Contrataciones del Estado, en adelante la Ley.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado, y sus modificatorias, en adelante el Reglamento.
- Ley N° 27806 - Ley de Transparencia y de Acceso a la Información Pública.
- Código Civil.
- Directivas del OSCE.
- Resoluciones emitidas por el Tribunal de Contrataciones del Estado.

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

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

Advertencia

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

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. (**Anexo N° 2**)
- d) Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)
- e) El Postor deberá considerar para la presentación de su oferta toda la documentación del fabricante, tales como brochure y/o catálogos y/o folletos y/o hojas de datos y/o enlaces web y/o whitepapers y/o cartas de fabricante, que le permita sustentar el cumplimiento de las características técnicas solicitadas para los equipos propuestos. La documentación podrá ser entrega en idioma original o

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

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

copia.

- f) Contar con autorización del fabricante para la distribución del equipamiento ofertado. Deberá acreditar con certificado y/o documento y/o carta emitida por el fabricante para la presentación de ofertas.
- g) Declaración jurada de plazo de entrega. (**Anexo N° 4**)⁴
- h) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo N° 5**)
- i) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6**.

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

Incorporar en la oferta los documentos que acreditan los “**Requisitos de Calificación**” que se detallan en el numeral 3.2 del Capítulo III de la presente sección de las bases.

2.2.2. Documentación de presentación facultativa

Advertencia

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo.

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.

En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

- g) Domicilio para efectos de la notificación durante la ejecución del contrato.
- h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación⁶ (**Anexo N° 11**).
- i) Detalle de los precios unitarios del precio ofertado⁷.
- j) La formación académica y Transferencia de Conocimientos se acreditará con cualquiera de los siguientes documentos: (i) copia del título universitario, (ii) constancias o (iii) certificados o (iii) cualquier otra documentación que, de manera fehaciente demuestre lo solicitado del personal clave solicitado. Dicha documentación se debe acreditar para la suscripción de contrato.
- k) 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. Dicha documentación se debe acreditar para la suscripción de contrato.
- l) Deberá contar con un Centro de Operaciones de Seguridad (SOC) propia para brindar el soporte 24x7x365 incluidos domingos y feriados. El SOC debe contar con certificación ISO27001, la cual debe ser adjuntada para la suscripción del contrato.

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya⁸.*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el*

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

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

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

⁸ Según lo previsto en la Opinión N° 009-2016/DTN.

presente numeral para el perfeccionamiento del contrato.

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes de la Entidad en Av. Paseo de la Republica N° 1645 Urb. Balconcillo – La Victoria, en el horario de 08:00 a 17:00 horas.

Importante

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

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista de acuerdo al siguiente detalle:

Prestación Principal: Entrega, instalación y puesto en operación de la Solución de Seguridad Perimetral (100% del monto total de la prestación principal)

Pago único correspondiente a la entrega del equipamiento, instalación y puesta en operación de la solución ofertada, la presentación de la documentación indicada en el numeral 5.3.1 (Entrega e instalación) y suscripción del acta de conformidad técnica de OGTI respectivas, previo informe técnico de la UIT.

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

- Corresponde a la Unidad de Almacén la recepción de los bienes y corresponde a la OGTI la emisión de la conformidad de la prestación principal, previo informe técnico de la UIT.
- Comprobante de pago.

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. Subsanada las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.

Dicha documentación se debe presentar en en Mesa de Partes de la Entidad en Av. Paseo de la Republica N° 1645 Urb. Balconcillo – La Victoria, en el horario de 08:00 a 17:00 horas.

Prestación Accesorio se pagara de acuerdo al siguiente detalle:

✓ **Prestación Accesorio N°03: Capacitación**

Pago único correspondiente al cumplimiento de la capacitación y/o entrenamiento, la presentación de la documentación indicada en el numeral 5.3.4 y suscripción del acta de conformidad técnica de OGTI respectivas, previo informe técnico de la UIT.

✓ **Prestación Accesorio N° 01: Soporte Técnico**

En seis (06) pagos iguales semestrales cumplimiento del servicio de soporte técnico, la presentación de la documentación indicada en el numeral 5.3.2 y la conformidad técnica de OGTI, previo informe técnico de la UIT. Deberá presentar los entregables correspondientes

✓ **Prestación Accesorio N°02: Mantenimientos Preventivos**

En tres (03) pagos iguales anuales al cumplimiento del servicio de mantenimiento preventivo, la presentación de la documentación indicada en el numeral 5.3.3 y la conformidad técnica de OGTI, previo informe técnico de la UIT. Deberá presentar los entregables correspondientes.

Nota: La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de servicios.

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

- Corresponde a la Unidad de Almacén la recepción de los bienes y corresponde a la OGTI la emisión de la conformidad de las prestaciones accesorias, previo informe técnico de la UIT.
- Comprobante de pago.

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. Subsanada las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.

Dicha documentación se debe presentar en en Mesa de Partes de la Entidad en Av. Paseo de la Republica N° 1645 Urb. Balconcillo – La Victoria, en el horario de 08:00 a 17:00 horas.



CAPÍTULO III REQUERIMIENTO

Importante

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

3.1. ESPECIFICACIONES TÉCNICAS



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

ESPECIFICACIONES TÉCNICAS

ADQUISICIÓN DE SOLUCIÓN DE SEGURIDAD PERIMETRAL PARA LA SEDE CENTRAL DEL SIS

1. OBJETO DE LA CONTRATACIÓN

Adquisición de una solución para seguridad perimetral para la Sede Central del SIS.

2. FINALIDAD PÚBLICA.

Contar una solución de Seguridad Perimetral de nueva generación acorde a las nuevas tendencias tecnológicas que protejan la estructura de red del Seguro Integral de Salud (SIS), contra accesos no autorizados y otras amenazas que puedan afectar el correcto funcionamiento de los servicios informáticos que ofrece la institución a sus asegurados a nivel nacional, permitiendo mejorar la seguridad y los niveles de disponibilidad de los servicios de infraestructura de red, para el apoyo a los usuarios en el cumplimiento de las metas y objetivos institucionales.

3. ANTECEDENTES

El Seguro Integral de Salud adquirió una solución para sistema de protección de intrusos para la zona perimetral en el año 2014, así como un equipo para seguridad de correo electrónico en el año 2013, y un equipo para monitoreo de redes en el año 2015; dichos equipos fueron dados de baja patrimonial en el último año, actualmente la plataforma tecnológica del centro de datos de la entidad, carece de equipamiento especializado de seguridad perimetral, con lo cual se corre el riesgo de que los sistemas de información CORE del SIS puedan afectarse por un ciberataque u otro similar, por lo que se hace necesario adquirir un equipamiento de seguridad perimetral que realice las funciones del equipamiento que se ha dado de baja.

4. OBJETIVOS DE LA CONTRATACION

Abastecer al SIS con nuevo equipamiento de seguridad perimetral, que será utilizado para apoyar con la protección informática del tráfico que pasa por los enlaces de internet existentes en la sede central del Seguro Integral de Salud (SIS).

- Realizar renovación de infraestructura tecnológica correspondiente a equipamiento de seguridad perimetral en la Entidad.
- Garantizar la continuidad y disponibilidad de los sistemas informáticos CORE de la Entidad, respecto a que los equipos solicitados van a proteger de tráfico malicioso que pueda dejar inoperativos dichas aplicaciones core.
- Mejorar el rendimiento de los servicios internos y externos que son proporcionados a los usuarios, asegurados del SIS y ciudadanía en general.

5. ALCANCES Y DESCRIPCIÓN DEL BIEN

El Seguro Integral de Salud requiere adquirir una solución de Seguridad Perimetral de acuerdo al siguiente detalle:

ITEM	PRESTACIÓN	DESCRIPCION	UNIDAD DE MEDIDA	Cantidad
Único	Principal	Solución de Seguridad Perimetral	Unidad	01
	Accesoría	Soporte Técnico	Servicio	01
		Mantenimiento Preventivo	Servicio	03
		Capacitación	Horas	36

Empleado digitalmente por FERRER
E. GUERRA José Hugo Marín PAU
00000000000000000000
Doy fe en
Fecha: 15.11.2023 13:07:15 -05:00

5.1. PRESTACIÓN PRINCIPAL: Entrega, instalación y puesta en operación de la Solución de Seguridad Perimetral

5.1.1. CARACTERÍSTICAS PRINCIPALES

- La solución de seguridad perimetral comprende de lo siguiente:
 - ✓ Solución de firewall de seguridad perimetral (NGFW)
 - ✓ Solución de firewall de aplicaciones web (WAF).
 - ✓ Solución de protección de correo electrónico.
 - ✓ Solución de monitoreo y detección de red o NDR
- Se debe tener en cuenta que se solicita que el hardware y/o software de los componentes de la solución sean especializados. No se aceptarán equipos de uso genérico como PCs o servidores.
- El Contratista deberá tener condición de empresa autorizada por el fabricante en la venta de los componentes de la solución a implementar (a). El Contratista deberá acreditar esto mediante una carta de fabricante de los componentes de la solución a implementar dirigida al SIS, la cual deberá ser presentada en la fecha de presentación de propuestas.
- Los equipos firewall de seguridad perimetral y firewall de aplicaciones web, tienen que ser ofrecidas en alta disponibilidad con dos (02) appliances físicos de las mismas características.
- Los equipos de la solución de seguridad perimetral deberán ser compatible y soportar el protocolo IPv6, debiendo el contratista configurar y habilitar dicho protocolo a solicitud del SIS sin costo adicional.
- El fabricante del equipo NGFW propuesto, deberá estar en el cuadrante de líderes de Gartner para "Enterprise Firewall" o firewalls empresariales, en los últimos 5 años.
- El fabricante del equipo WAF propuesto, deberá estar presente en el cuadrante de Gartner para "Web application and API Protection" en los últimos 2 años.
- El fabricante del equipo NGFW propuesto, deberá contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- Todos los appliances físicos ofrecidos en la solución deberán ser adecuados para montaje en rack 19".
- Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.

5.1.2. CARACTERÍSTICAS DEL EQUIPAMIENTO

5.1.2.1. FIREWALL DE SEGURIDAD PERIMETRAL

CARACTERÍSTICAS	DETALLE
Capacidades	<ul style="list-style-type: none"> ○ Throughput de Next Generation Firewall de 9.3 Gbps o superior, medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes. ○ Throughput de Prevención de Amenazas de 4.7 Gbps o superior, medido con tráfico productivo real (transacciones usando una mezcla de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<p>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.</p> <ul style="list-style-type: none"> o No se aceptarán cartas de fabricante como fundamento para el cumplimiento de performance, se deberá comprobar el requerimiento de throughput con documentación pública del fabricante adjuntando el link que lo respalde. o El equipo debe soportar como mínimo: 1,350,000 sesiones simultáneas y 135,000 sesiones por segundo, medidos con paquetes HTTP de 1 byte. o Raqueable en dos unidades de rack como máximo. o Debe contar con fuente de poder redundante con capacidad de cambio en caliente. o Disco de estado sólido interno de 240 GB o superior. o Mínimo 04 interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red o Mínimo 04 interfaces multigigabit de red 1G/2.5G/5G en formato RJ45 para el tráfico de datos de la red o Mínimo 04 interfaces multigigabit de red 1G/2.5G/5G PoE en formato RJ45 para el tráfico de datos de la red o Mínimo 02 interfaces de red 1G en formato SFP para el tráfico de datos de la red o Mínimo 08 interfaces de red 1G/10G en formato SFP/SFP+ para el tráfico de datos de la red o La plataforma deberá contar con al menos una (01) interfaz 10G dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad. o Estar licenciada para soportar 1000 clientes de VPN SSL simultáneos.
Características Técnicas	<ul style="list-style-type: none"> • El dispositivo de seguridad debe soportar VLAN Tags 802.1qs, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino. • Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2). • Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones. • Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.

	<ul style="list-style-type: none"> • Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino. • Soportar DNS Dinámico en las interfaces de red del equipo de seguridad. • Soportar túneles GRE como punto inicio o finalización del túnel. • Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel. • Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo. • Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
Alta Disponibilidad	<ul style="list-style-type: none"> • Soporte a configuración de alta disponibilidad Activo/Pasivo y Activo/Activo, con despliegues de los equipos tanto en modo transparente como en modo capa 3 (L3). • La configuración en alta disponibilidad debe sincronizar: Sesiones; Certificados de descifrado, Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QoS y objetos de red. • Debe ser posible el monitoreo de fallo de enlaces, ya sea ante la caída de al menos una de las interfaces del equipo, una conexión física adyacente o pérdida de conectividad hacia una IP desde una de las interfaces. • Debe permitir cifrar la comunicación entre dos Firewall de HA durante la sincronización de las configuraciones.
Funcionalidades	<ul style="list-style-type: none"> • El control de políticas basado en zonas, puertos, direcciones IP, segmentos de red o rangos, ubicación geográfica, usuarios y grupos de usuarios, así como en categorías y agrupaciones estáticas y dinámicas de aplicaciones (según sus características) y categorías de aplicaciones. • Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención. • Permitir el agendamiento de las políticas de seguridad. • Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa. • Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método. • Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría. • Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules). • Debe mostrar la primera y última vez que se utilizó una regla de seguridad. • Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<ul style="list-style-type: none"> • Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall
Descifrado de tráfico SSL/TLS	<ul style="list-style-type: none"> • Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos. • Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall. • Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3. • Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros. • Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS • Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI). • Debe permitir el descifrado selectivo de categorías de URLs, por ejemplo, debe ser capaz de especificar el no descifrado de páginas con contenido sensible, mientras forzar el descifrado de páginas de clasificación de riesgo alto o medio • Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards. • Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores. • Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).
Control de Aplicaciones	<ul style="list-style-type: none"> • Reconocer por lo menos 2900 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.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<ul style="list-style-type: none"> • Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros. • Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado. • Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante. • Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos. • Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7. • Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.
Protección ante ataques de denegación de servicio (DoS)	<ul style="list-style-type: none"> • Debe definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood. • Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa • La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor) • La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS • Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo • La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección. • Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route • Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex). • Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.
Análisis de malware de día cero	<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. Como mínimo se requiere que el Sandbox propuesto



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<p>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.</p> <ul style="list-style-type: none"> • Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware. • El equipo debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen. • Debe permitir al administrador la descarga del archivo original analizado por el Sandbox. • Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración. • Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e .class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado. • Permitir la subida de archivos al sandbox de forma manual y vía API. • Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hipervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
Prevención de amenazas conocidas	<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. • Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos • Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante. • El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot. • 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 origina la amenaza. • Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.



de Salud

	<ul style="list-style-type: none"> • Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención. • Debe soportar la creación de firmas de IPS basadas en el formato de Snort.
Filtros 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 contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas. • Debe evitar vulnerabilidades de JavaScript y contenido phishing en el tráfico web utilizando un motor tiempo real basado en machine learning • Debe utilizar machine learning para analizar URL en tiempo real y clasificarlas en categorías benignas o maliciosas • Debe ser capaz de bloquear URLs maliciosas no vistas con anterioridad, es decir, URLs que no hayan sido categorizadas previamente por el fabricante • Debe poseer algoritmos que evalúen URLs en tiempo real para bloquear URLs no categorizadas por crawlers, inclusive URLs resistentes a técnicas de cloaking • Debe incluir escaneo en línea basado en machine learning para detectar ataques de phishing no vistos antes • Debe poseer capacidades anti evasivas para contener evaluaciones de cloaking, Captchas y codificación de caracteres • Debe emplear modelos de aprendizaje automático para analizar imágenes en páginas web y determinar si están imitando marcas conocidas, previniendo intentos de phishing. • Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad. • Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site. • Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo ataques de phishing.
Protección avanzada de DNS	<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. • El servicio de protección de DNS debe alimentarse de telemetría provista por clientes a nivel mundial y más de 30 fuentes de inteligencia de amenazas de terceros. • La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).



de Salud

	<ul style="list-style-type: none"> • Debe utilizar machine learning y/o inteligencia artificial para detectar nuevos dominios nunca vistos autogenerados por algoritmos DGA • Debe poseer políticas para bloquear dominios DGA o interrumpir las consultas de DNS a dichos dominios. • Debe ayudar a contener ataques emergentes basados en DNS, que utilicen técnicas de tunelización lenta sobre tráfico DNS, técnicas de entradas de DNS pendientes y adquisición de subdominios • Debe ser capaz de predecir nuevos dominios maliciosos inmediatamente luego de su registro, antes de que puedan ser utilizados en ataques • Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS • Debe analizar las consultas de DNS, incluyendo las tasas de consultas y patrones, entropía y frecuencia de n-grams para detectar posibles intentos de tunelización. • Debe bloquear resoluciones de DNS que usen técnicas de SNI Spoofing utilizadas para eludir los controles de descifrado.
Identificación de usuario	<ul style="list-style-type: none"> • Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E-Novell Directory, Exchange y base de datos local. • Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente. • Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI. • Debe disponer de un servicio en nube o onpremise que extraiga automáticamente la información del usuario grupos de usuario de varios IDPs y proveedores de SSO como Azure AD, okta, Google identity y PingID y la ponga a disposición de los NGFW para ser incluidos en la política de seguridad. • Debe disponer de un servicio en nube o onpremise que simplifique la autenticación SAML de usuarios, que actúe como Service Provider único frente a IDPs o proveedores de SSO • Debe disponer de un servicio en nube o onpremise que almacene todos los grupos disponibles del Active Directory, los filtre y ponga a disposición únicamente los grupos necesarios que el NGFW utilice en la política de seguridad • Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM. • Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios. • Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación. • Debe permitir la definición de grupos dinámicos de usuarios.
Filtro de Datos	<ul style="list-style-type: none"> • Los archivos deben ser identificados por extensión y firmas. • Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK,



Ministerio de Salud

	<p>Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.</p> <ul style="list-style-type: none"> • Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.
Conexión VPN	<ul style="list-style-type: none"> • Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPsec o SSL. • La VPN IPsec debe soportar como mínimo: • DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard) • Autenticación MD5, SHA-1, SHA-2; • Diffie-Hellman Group 1, Group 2, Group 5 y Group 14; • Algoritmo Internet Key Exchange (IKEv1 & IKEv2); • Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN. • Las VPN client-to-site deben poder operar usando el protocolo IPsec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo. • Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA). • Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN. • Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN. • El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X. • Debe permitir los siguientes tipos de conexión del cliente al túnel VPN: • Antes del usuario se autentique en la estación; • Después de la autenticación del usuario en la estación usando Single Sign On (SSO); • Bajo demanda del usuario; • Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
Funcionalidades SDWAN	<ul style="list-style-type: none"> • La solución debe contar con una consola de monitoreo con la capacidad de poder identificar fácilmente las aplicaciones y enlaces sus estados dentro de la red de SD-WAN (aplicaciones con problemas de jitter, latencia, pérdida de paquetes y sus diferentes estados dentro de la red) pudiendo ver el estado de estas en por lo menos en los últimos 5 minutos, última hora, último día o bien haciendo filtros personalizados. • 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. • 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. • 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.



PERU

Ministerio
de Salud

Laboratorio Central de

Seguro Integral de Salud

	<ul style="list-style-type: none"> • 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 • Soportar la transmisión de paquetes duplicados por diferentes enlaces al utilizar la red de SD-WAN con el objetivo de mantener una calidad de experiencia alta al usar aplicaciones de misión crítica y prevenir la pérdida de paquetes, incremento de latencia, jitter, etc. • Capacidad de monitorear la salud de los enlaces a través de aplicaciones de SaaS y aplicaciones de Cloud, para poder determinar si esas aplicaciones son enviadas a internet de manera directa o bien a través de algún camino a través de la red de SD-WAN. • Capacidad de definir el tiempo de intercambio de heartbeats entre los puntos del túnel SD-WAN. • Capacidad de realizar fail over
Consola de gestión centralizada	<ul style="list-style-type: none"> • Posibilita la administración de varios equipos. • Debe ser entregada como appliance físico. • Debe contar con una capacidad mínima de 10TB útiles de disco. • Rackeable de 1 RU, de la misma marca o fabricante del NGFW. • Permitir exportar las reglas de seguridad en formato CSV y PDF • Deberá ser capaz de recibir una ratio mínima de 10,000 logs por segundo. • La plataforma de gestión centralizada, reportes, monitoreo y centralización de logs debe correlacionar la información recibida; de forma que rastree patrones en la red y correlacione eventos que indican una escalada de comportamiento sospechoso o eventos que equivalen a actividad maliciosa • Centralizar la gestión y monitoreo de las redes y equipos SD-WAN. • Cada Firewall gestionado deberá generar una alerta si es que pierde conectividad con la consola de gestión centralizada. • Debe generar una estructura jerárquica para poder diferenciar políticas generales y locales y así mejorar la administración global de la compañía. • Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables. Debe ser posible crear un rol que permita ver las configuraciones de uno o un grupo de equipos Firewall específicos y ocultar la configuración del resto de equipos. • Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad. • Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino) • Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.



PERU

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<ul style="list-style-type: none"> • Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política. • Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules). • Debe poder programar push de configuraciones y políticas de seguridad sin la participación humana a múltiples firewalls y múltiples sistemas o dominios virtuales, permitiendo impulsar cambios de manera eficiente en todo el proceso implementación. • Debe brindar la posibilidad de realizar un seguimiento de todos los cambios. Capturando los registros del sistema y los registros de configuración, incluidos los errores. • Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup). • Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada. • Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP). • Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizó, su IP y el horario de la alteración; • Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema. • Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispysware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico. • Ante eventuales caídas de la consola de gestión, las funcionalidades de identificación de Shadowing Rules y personalización de reportes de tráfico, antivirus, IPS, sandboxing, control de aplicaciones, entre otros, deben poder ser realizadas de forma local en cada Firewall, caso contrario el postor deberá incluir dos consolas de gestión en Alta Disponibilidad para mantener la redundancia de estas capacidades. • Debe soportar la administración de los NGFW utilizando el estándar OpenConfig (OC) para automatizar las tareas de configuración en toda su infraestructura. • La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.
--	---

5.1.2.2. FIREWALL DE APLICACIONES WEB

CARACTERISTICAS	DETALLE
Capacidades	<ul style="list-style-type: none"> • Tipo appliance de propósito específico. • Debe ser adecuado para montaje en rack 19", de 2RU o inferior. • Disco SSD con capacidad de 250GB o superior.



PERU

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<ul style="list-style-type: none"> • 02 interfaces Gigabit SFP o superior. • 04 interfaces Gigabit Ethernet cobre o superior. • Soporte IPv6
Rendimiento	<ul style="list-style-type: none"> • Throughput mayor o igual a 500 Mbps.
Seguridad	<ul style="list-style-type: none"> • Debe proteger contra ataques de día cero, para ello deberá hacer uso de un sandbox del mismo fabricante. • Debe soportar filtros de seguridad que bloquean ataques de fuerza bruta. • Debe soportar filtros de seguridad que bloquean ataques a la base de datos. • Debe soportar filtros de seguridad que bloquean ataques de métodos y parámetros HTTP. • Debe soportar filtros de seguridad para proteger las sesiones de los usuarios remotos. • Debe soportar filtros de seguridad que protejan las aplicaciones y servicios web. • Debe soportar aprendizaje sin manipulación del administrador. • Debe incluir protección anti-bot. • Debe incluir protección API • La solución debe permitir la restricción de parámetros como logical application attack, buffer overflow, zero day attack mediante políticas. • La solución debe ser capaz de crear una política de seguridad de forma automática, a través de un proceso de autoaprendizaje. • La solución debe permitir URL Access Restrictions. • Protección de ataques de aplicaciones: <ul style="list-style-type: none"> ✓ OWASP Top 10. ✓ SQL Injection. ✓ Cross-site scripting. ✓ Cross Site Request Forgery. ✓ Session Hijacking. ✓ Built-in Vulnerability Scanner. ✓ Third-party scanner integration (virtual patching). • Seguridad Web: <ul style="list-style-type: none"> ✓ Automatic profiling (lista blanca). ✓ Web server and application signatures (lista negra). ✓ IP Reputation. ✓ IP Geolocation. ✓ HTTP RFC compliance. • Application delivery: <ul style="list-style-type: none"> ✓ Layer 7 server load balancing. ✓ URL Rewriting. ✓ Content Routing. ✓ HTTPS/SSL Offloading. ✓ HTTP Compression.
Administración	<ul style="list-style-type: none"> • Interface de configuración vía Web (HTTP, HTTPS). • Soporte a por lo menos dos niveles de administración: Lectura/Escritura (Read/Write) y Sólo Lectura (Read-Only). • Soporte a SNMP • Soporte a registro (logging) de la actividad. • Soporte a syslog externo.

Alta Disponibilidad	<ul style="list-style-type: none"> • Soporte a capacidades de configuración de equipos en Activo-Activo o Activo-Pasivo. • Soporte a sincronización de políticas. • Fuentes de poder redundantes integradas
---------------------	--

5.1.2.3. PROTECCIÓN DE CORREO ELECTRÓNICO

CARACTERISTICA	DETALLE
Capacidades	<ul style="list-style-type: none"> • La solución de protección de correo electrónico será otorgada por medio de un appliance físico de propósito dedicado o por medio de una suscripción en nube. • La solución debe estar contemplado para 1500 buzones de correos electrónicos. La Entidad utilizará la solución para proteger cuentas de correo electrónico en Microsoft 365 (cloud) y en Zimbra (on premises). • La solución provee una herramienta que permita de manera centralizada gestionar como mínimo las siguientes características: <ul style="list-style-type: none"> ✓ Gestionar la protección de la solución en grupos creados o en forma individual. ✓ Ver eventos agrupados por categorías de incidentes o amenazas. ✓ Mostrar en forma gráfica el contexto y relacionamiento de los compromisos detectados. Se precisa que se refiera a que se muestren: "correos entrantes y salientes, indicando los correos que fueron bloqueados por virus, spam, URL maliciosos entre otros" o "la tendencia de detecciones de correos no deseados (spam)". ✓ Integración con trazabilidad gráfica que permita visualizar los detalles de incidentes. ✓ Visibilidad de logs y estadísticas. ✓ Posibilidad de notificación al usuario final cuando un correo entrante (que lo tenga como usuario destino) ha sido retenido por la solución. ✓ Posibilidad de notificación al usuario final cuando un correo saliente (generado por el usuario) ha sido retenido por la solución. ✓ La solución debe tener la capacidad de almacenar datos de los últimos treinta (30) días como mínimo, y encontrarse disponibles para su análisis. ✓ Capacidad de integración por medio de API's abiertas a consolas externas centralizadas. Se precisa que se integrará a tecnología Microsoft 365, asimismo, en caso se requiera licenciamiento adicional, ello no representará ningún costo adicional para la Entidad. ✓ Mostrar a nivel de reporte las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes relacionados con Business Email Compromise (BEC).
Seguridad	<ul style="list-style-type: none"> • Debe tener actualizaciones de amenazas en vivo para detener los últimos ataques, para ello debe contar con la actualización periódica de los módulos de antivirus o firmas o algoritmos o firmas del módulo de antivirus, que emplea la solución de protección de correo electrónico. • Debe tener detección antispam, antivirus (o antimalware) y antiphishing. • Debe tener un filtro de reputación que pueda bloquear al menos con un 90% del spam. • Debe tener tecnología de "filtrado de reputación de próxima generación" y/o "reputación dinámica de IP", que elimine el spam de botnet en el nivel de conexión IP al monitorear las solicitudes de conexión y rechace aquellas que muestren evidencia de conexiones de botnet.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

	<ul style="list-style-type: none"> • Debe proteger contra el spam tipo "Snowshoe Spamming" • Debe tener un portal para el usuario final que luego permita a los usuarios publicar correos electrónicos bajo demanda y/o resúmenes de cuarentena en el mensaje que brinden un resumen diario del correo en cuarentena, con la opción de liberarlos directamente y/o desde la bandeja de entrada. • Debe tener técnicas de autenticación SPF, DKIM y DMARC para identificar y permitir correos electrónicos legítimos mientras bloquea a los impostores. • Debe tener detección de anomalías en el encabezado que identifique si el nombre para mostrar del remitente es el mismo que un nombre de usuario interno.
Configuración y Administración	<ul style="list-style-type: none"> • Debe ser compatible con Microsoft Exchange Online y Microsoft Office 365 • En el caso de Microsoft Office 365, debe tener la capacidad de integrarse vía API sin la necesidad de modificar registros DNS. • Debe ser compatible con cualquier servicio de correo en el que sea propietario del dominio y controle los registros DNS asociados. • Debe tener la capacidad de sincronizarse con Microsoft Active Directory • Debe tener la capacidad de sincronizar con Microsoft Azure Active Directory • Debe tener la capacidad de soportar múltiples dominios para la misma organización. • Debe poder mantener a los usuarios sincronizados automáticamente con el producto mediante ADSync o equivalente. • Debe proporcionar al administrador la capacidad de agregar manualmente registros de alias de direcciones de correo electrónico cuando Active Directory no esté disponible. • Debe tener la capacidad de crear diferentes tipos de roles para la gestión o administración de la plataforma. • Debe proporcionar al administrador la capacidad de encontrar buzones de correo específicos. • Debe tener un portal de autoservicio para usuarios finales. • El portal de autoservicio debe permitir a los usuarios administrar correos electrónicos en cuarentena (aceptar / eliminar correos electrónicos) • El portal de autoservicio debe permitir a los usuarios ver los mensajes en caso de interrupción utilizando la bandeja de entrada de emergencia, esta característica será considerada opcional. • Debe poder crear políticas de seguridad de correo electrónico únicas para individuos, grupos o todo el dominio.
Continuidad	<ul style="list-style-type: none"> • Debe tener la capacidad de manejar una cola de correo electrónico que garantice que no se pierda ningún correo. • En caso de una interrupción de su servicio de correo electrónico de Microsoft, el producto debe tener la capacidad de poner en cola automáticamente los correos electrónicos del destinatario y luego entregarlos una vez que se restablezca el servicio. • Debe proporcionar al usuario acceso a una bandeja de entrada de emergencia 24 horas al día, 7 días a la semana. • Debe tener la capacidad de enviar alertas cuando el correo no se pueda entregar a un servidor / servicio en caso de interrupciones de un proveedor de servicios de correo electrónico en la nube de terceros.
Protección contra suplantación de identidad	<ul style="list-style-type: none"> • Debe poder comparar el nombre para mostrar de los correos electrónicos entrantes con el nombre para mostrar de las marcas de servicios en la nube y tener la opción de poder parametrizar usuarios con categoría VIP para evitar la suplantación de identidad dentro de la organización.



de Salud

	<ul style="list-style-type: none"> • Debe poder hacer un análisis de dominios similares para identificar nombres de dominio de uso corporativo. • Los mensajes sospechosos se pueden bloquear, poner en cuarentena, etiquetar con una advertencia en la línea de asunto o agregar un banner con un enlace directo a la lista de bloqueo a nivel de usuario.
Protección de la información	<ul style="list-style-type: none"> • Debe escanear automáticamente los cuerpos de los mensajes y los archivos adjuntos en busca de datos confidenciales para establecer políticas para bloquear o cifrar los mensajes. • Debe tener un cifrado basado en inserción que proteja todo el correo electrónico o solo los archivos adjuntos. • Debe tener un cifrado TLS reforzado que evite las escuchas cuando los mensajes están en tránsito. • Debe tener capacidades de control de contenido y prevención de pérdida de datos.
Protección activa contra amenazas	<ul style="list-style-type: none"> • Debe tener capacidad de reescritura de URL para verificar la reputación del sitio web de los enlaces de correo electrónico antes de la entrega y en el momento en que hace clic, bloqueando ataques furtivos y retardados. • Debe tener una zona de pruebas basada en la nube que pueda detectar malware conocido y desconocido y aplicaciones no deseadas antes de que se ejecute.
Informes	<ul style="list-style-type: none"> • Debe contar con un Panel de Control (o Dashboard), en donde se ilustre de manera general el comportamiento del estado de los correos electrónicos analizados, así mismo deberá mostrar que buzones de correo electrónico se encuentran en riesgo. • Debe proporcionar informes de estadísticas dentro de la consola en forma de tablas y gráficos con rangos de fechas personalizados. • Debe incluir un informe que proporcione información completa sobre el encabezado del mensaje y cualquier archivo adjunto. • Debe incluir un informe que proporcione detalles de los pasos por los que pasó el mensaje en la infraestructura de análisis de correo electrónico. • Debe incluir un Informe de amenazas avanzado que proporcione un resumen de los mensajes entrantes que se detonaron en el entorno de la zona de pruebas, que se puede filtrar por fecha y el resultado del análisis durante el último año. • Debe incluir un reporte sobre detecciones asociadas a la política para prevención de Fuga de Información.

5.1.2.4. MONITOREO Y DETECCIÓN DE RED

CARACTERÍSTICAS	DETALLE
Capacidad	<ul style="list-style-type: none"> • Appliance dedicado de uso específico para la función solicitada. No se aceptarán NGFW o equipamiento similar para el cumplimiento del requerimiento. • Interfaces QSFP+: 1 o superior • Interfaces SFP+: 14 o superior (deberá incluir 01 transceiver SR SFP+) • Interfaces GE RJ45: 4 o superior • Local Storage: 1 TB o superior • Slot para Expansion: 01 o superior • Rackeable, incluir sus accesorios. No deberá superar 2UR • Fuentes de Poder: 02 (AC Power) • Breach Detection o NDR Throughput: Mínimo 9.5 Gbps • Nuevas sesiones por segundo: 470,000



de Salud

	<ul style="list-style-type: none"> • Máximo Sesiones Concurrentes: 4,200,000
Funcionalidades	<ul style="list-style-type: none"> • La solución propuesta debe soportar el modo de operación de tapping, sin ser intrusiva para la red del cliente. • La solución debe poder integrarse con firewalls de la misma marca para poder mitigar amenazas. • La solución debe soportar más de 3,500 aplicaciones, debe soportar el filtro de aplicaciones por nombre, categoría, subcategoría, tecnología y riesgo. • La solución debe poder identificar aplicaciones móviles del tipo iOS o Android. • La solución debe ser capaz de identificar las aplicaciones en la nube, debe proporcionar monitoreo y estadísticas multidimensionales para las aplicaciones en la nube, incluyendo la categoría de riesgo y las características. • La solución debe soportar al menos 2,000 firmas. Debe soportar firmas personalizadas, manual, actualizaciones automáticas de inserción o extracción de firmas y una enciclopedia de amenazas integrada. • La solución debe ser compatible con la protección de inyección SQL, CC y ataques XSS. • La solución debe soportar la detección de anomalías de protocolo, detección basada en la velocidad. Incluyendo HTTP, SMTP, IMAP, POP3, VOIP, NETBIOS, etc. • La solución debe permitir crear listas blancas para el módulo de IPS. • La solución debe contar con perfiles predefinidos de IPS. • La solución debe ser compatible con Antivirus basado en flujo: los protocolos incluyen HTTP, SMTP, FTP. • La solución debe soportar la detección de virus para archivos comprimidos como RAR, ZIP, TAR. • La solución debe poder proteger el sistema contra ataques de fuerza bruta en el nombre de usuario y la contraseña. • La solución debe ser compatible con el entorno de ejecución virtual de malware, basado en la nube para encontrar amenazas desconocidas. • La solución debe ser compatible con la carga de archivos maliciosos en el entorno limitado de la nube para su análisis. • La solución debe tener una interfaz de usuario web integrada (WebUI) e interfaz de línea de comandos (CLI). • La solución debe soportar el acceso de administración desde HTTP / HTTPS, SSH, telnet, consola. • La solución debe ser compatible con la política de seguridad de contraseña para las cuentas de administrador. • Admite alertas del tipo correo electrónico, mensaje de texto. • Logs: incluidos registros de eventos, redes, amenazas, configuración y sesiones. • Admite SYSLOG estándar. • La solución debe soportar análisis por correlación de amenazas, correlación entre amenazas desconocidas, comportamiento anormal y comportamiento de aplicaciones para descubrir amenazas o ataques potenciales. • La solución debe permitir la actualización de la base de datos del modelo de comportamiento de malware en línea en tiempo real. • La solución debe soportar la detección de más de 2000 familias de malware conocidas y desconocidas, incluidos Virus, Gusanos, Troyanos, Desbordamiento, etc. • La solución debe ser compatible con la detección avanzada de malware basada en comportamiento.



Ministerio de Salud

	<ul style="list-style-type: none"> • La solución debe ser compatible para detectar ransomware y malware. • La solución debe soportar el modelado de comportamiento basado en el tráfico de línea de base L3-L7 para revelar un comportamiento anómalo de la red • La solución debe soportar la visualización de amenazas de Intranet para los servidores (activos críticos), así como la detección del tráfico anormal relacionado a ellos. • La solución debe soportar visibilidad para la información básica basada en el host, índice de riesgo, las amenazas y el tráfico anormal. • La solución debe soportar visibilidad de amenazas, incluido el nombre de amenaza, tipo de amenaza, nivel de riesgo, base de conocimiento, paquete forense, etc. • La solución deberá contar con licenciamiento incluido para el uso de cloud sandboxing del fabricante durante el periodo de garantía.
--	---

5.1.3. CONDICIONES GENERALES

- El contratista deberá presentar un plan de trabajo a los 10 días calendario contados a partir del día siguiente de suscrito el contrato, dicho plan permitirá describir las tareas y actividades a realizarse para la implementación de los bienes ofertados, sujeto a revisión y ratificación por el SIS, el cual tendrá 03 días calendario para aprobarlo; de presentarse alguna observación deberá ser subsanada por el contratista en un plazo no mayor de 02 días calendario; este plazo no será computable respecto al plazo total. En caso de que el contratista no cumpla con los plazos indicados se aplicará penalidad según numeral 5.9.2.
- Dicho plan debe contener como mínimo lo siguiente:
 - ✓ Cronograma de actividades para la entrega de equipos
 - ✓ Cronograma de actividades para la instalación, configuración y puesta en producción, de acuerdo a la siguiente estructura:
 - Inicio
 - Descripción de Plataforma
 - Ambiente que se está cambiando
 - Ventana que estará fuera de servicio
 - Kick Off.
 - Requerimientos y Diseño
 - Relevamiento de Información.
 - Propuesta de arquitectura de la solución.
 - Actividades preparatorias (comunicación, respaldos, incidentes, equipamiento de reemplazo, recursos)
 - Análisis de riesgos
 - Implementación
 - Plan de Pruebas
 - Plan de vuelta atrás
 - Instalación física.
 - Configuración e instalación del hardware, software y licenciamiento.
 - Migración y toma de operación.
 - Puesta en Marcha
 - Puesta en Producción.
 - ✓ Cronograma de actividades del servicio soporte y capacitación.
 - ✓ Procedimientos de backup, instalación y configuración de toda la solución.

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]



PERU

Ministerio
de Salud

INstituto de Promoción y
Atención de Salud

Seguro Integral de Salud

✓ Acuerdos de Nivel de Servicios.

- Antes del inicio de labores efectivas del personal técnico para la ejecución de trabajos en el SIS, el proveedor deberá presentar los Seguros SCTR (Seguro Complementario de Trabajo de Riesgo) vigente del personal técnico al personal de la OGTI y durante la ejecución de trabajos el personal técnico del proveedor deberá presentarse con los equipos de protección personal (EPP).
- El SIS no se responsabiliza por accidentes que pudiera sufrir el personal técnico o profesional del proveedor durante la ejecución de trabajos en la Sede Central del SIS.
- De corresponder, el proveedor deberá subsanar 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.
- En caso fuese necesario trasladar o movilizar recursos humanos, equipos, cables, u otros, objetos del contrato, el traslado o movilización que sean necesarios serán entera responsabilidad del proveedor.
- El proveedor se compromete a no violar la confidencialidad, seguridad y propiedad de los archivos, programas y sistemas de aplicación que existan al interior del SIS.
- El SIS brindará el espacio para la instalación del equipamiento, energía establecida y los accesos necesarios para la implementación de la solución.
- Quedará a disposición del proveedor, la posibilidad de visitar las instalaciones del Centro de Datos del SIS, no se aceptarán costos adicionales en las tareas de instalación y en la puesta en marcha originados por desconocimiento de los espacios. Los postores interesados en realizar las visitas a los sitios de instalación deberán solicitar y coordinar las mismas hasta 03 días antes de la presentación de ofertas.
- El contratista deberá realizar la provisión, configuración, instalación del equipo, basado en las mejores prácticas recomendados por el fabricante de los equipos de la solución de seguridad perimetral, sin que esto genere gastos adicionales a la institución.
- El Contratista deberá proporcionar el licenciamiento perpetuo del firmware (para el caso de appliances físicos) y otorgar garantía por un periodo de tres (3) años por el equipamiento de la solución ofertada.
- El equipo deberá tener la última versión del firmware.
- El Contratista deberá asociar los equipos a la siguiente cuenta: licencias@sis.gob.pe para el registro de los equipos.
- La terminación de los cables de energía hacia la toma de energía del gabinete de comunicaciones deberá ser NEMA 5-15P.
- Las labores que involucren el corte de algún servicio en producción no podrán ser efectuados en horario de oficina para no interrumpir las labores del personal, en caso contrario, se realizarán en un horario previa coordinación con el responsable de la Oficina General de Tecnología de la Información.
- El equipo y sus kits de montaje deben ser originales del fabricante del equipo ofrecido, y no deberán tener notificación a la fecha de presentación de la oferta de End Of Sale y End Of Life.
- El postor deberá incluir en su propuesta un Workstation, la cual será utilizada para monitorear las soluciones adquiridas, con las siguientes características:
 - Procesador Intel i5 o i7 de 11va generación o superior.
 - Memoria RAM de 16 Gb o superior
 - Disco de estado sólido de 500 Gb o superior
 - Dos salidas HDMI o superior
 - Dos conexiones de red de 1G RJ 45 o superior
 - Dos monitores de 50" y accesorios para su conexión con la Workstation propuesta.



PERU

Ministerio
de Salud

Dirección Administrativa

Seguro Integral de Salud

- o Incluir los accesorios necesarios para que los monitores sean instalados en pared.
- Deberá contar con un Centro de Operaciones de Seguridad (SOC) propia para brindar el soporte 24x7x365 incluidos domingos y feriados. El SOC debe contar con certificación ISO27001, la cual debe ser adjuntada para la suscripción del contrato.

5.1.4. ACONDICIONAMIENTO, MONTAJE E INSTALACIÓN

El Contratista deberá considerar lo siguiente para la implementación del equipamiento:

- a) El contratista deberá instalar los equipos de seguridad perimetral de acuerdo a las buenas prácticas, guías y/o manuales de instalación y operación de cada fabricante que integra la solución, considerando el cronograma de actividades propuestos en el Plan de Trabajo.
- b) La instalación de los equipos deberá realizarse mediante el uso necesario de pernos enjaulados, en los gabinetes ubicados dentro del centro de datos de la Entidad.
- c) Debe realizar todas las configuraciones para garantizar que la operatividad del equipamiento actual de seguridad perimetral no se vea interrumpido durante el acondicionamiento.
- d) El contratista deberá migrar todas las configuraciones del equipo Firewall Sophos XG450 hacia los nuevos equipos ofertados en coordinación con la OGTI.
- e) Realizar copia de seguridad a nivel de configuración y sistema de archivos de cada uno de los componentes del equipamiento a reemplazar en coordinación con la OGTI del SIS antes de iniciar el acondicionamiento.
- f) Desmontaje y retiro de los componentes a reemplazar, del equipamiento actual del Data Center (equipos de seguridad perimetral) e instalación y montaje de los equipos nuevos a suministrar (equipos de seguridad perimetral) en el Data Center del SIS.
- g) El contratista deberá tener en cuenta que, para la instalación del equipamiento a suministrar se dispondrá de los espacios y energía que ocupa el equipamiento actual, teniendo en cuenta que, se podrá disponer de un espacio libre y energía para un gabinete que podrá utilizar el contratista para realizar las permutaciones que crea conveniente para llevar a cabo la instalación y migración entre el equipamiento nuevo y el actual.
- h) El Contratista deberá proveer e implementar todo el cableado necesario para la conectividad de los equipos de la solución de seguridad perimetral hasta los equipos: switch de core, y/o administrador de ancho de banda y/o balanceador de enlaces de la Entidad, que se encuentren en el mismo rack de comunicaciones o en el rack contiguo (a su lado). El cableado provisto deberá ser compatible con los equipos con que se conectarán y deberán ser etiquetados para el reconocimiento del equipo desde y hacia al que se conectarán.
- i) Los trabajos de cableado se realizarán previa coordinación y aceptación de la Oficina General de Tecnologías de la Información. Los costos del cableado necesario serán asumidos por el Contratista.
- j) La Oficina General de Tecnologías de la Información supervisará y verificará los materiales previa implementación de los mismos.
- k) El contratista deberá realizar el análisis de requerimientos para la implementación de los equipos de acuerdo a la necesidad formulada por la OGTI del SIS, el contratista luego del análisis propondrá la mejor arquitectura y configuración de equipos a instalar.
- l) El servicio de instalación y configuración a realizar incluirá el uso de sus propios recursos humanos, herramientas, útiles, materiales de trabajo y equipos; por lo que el servicio deberá ser presupuestado a todo costo, y por lo tanto al SIS no le debe significar costo adicional al propuesto por la empresa.
- m) El contratista deberá retirar los equipos existentes (desinstalar) e instalar los equipos ofertados para lo cual deberá proveer los conectores, módulos, cableado, hardware, software y licencias necesarias para cumplir con la arquitectura propuesta de acuerdo a la necesidad formulada por la OGTI del SIS.
- n) El contratista deberá verificar las zonas de seguridad del SIS y en base a su análisis y recomendaciones, realizará la configuración la solución perimetral para segmentar la red del SIS en un mínimo de 6 (seis) zonas de seguridad de red.



PERU

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

- o) La configuración y puesta en marcha que se realizarán en los equipos de la solución de seguridad perimetral se realizarán previa coordinación con la OGTI, así como el Contratista deberá realizar configuraciones para aumentar y/o fortalecer el rendimiento y la seguridad en los equipos de la solución propuesta y consecuentemente en la red
- p) El SIS será responsable de que los equipos de comunicaciones hacia donde irán conectados los equipos de la solución propuesta, cuenten con el mínimo de interfaces disponibles, así como entregara puntos de energía estabilizadas.

5.2. PRESTACIONES ACCESORIAS

5.2.1. Prestación Accesorio N° 01: Soporte Técnico

Dentro del Plan de Trabajo, el proveedor deberá incluir el "Cronograma del Servicio de Soporte" con fechas de la presentación de informes semestrales para la presente prestación, sujeto a revisión y ratificación por el SIS.

El contratista deberá brindar lo siguiente para todos los componentes de la infraestructura objeto del contrato:

- a. El Contratista deberá brindar soporte técnico remoto o en sitio con una modalidad 24x7 por el período de tres (03) años contados a partir del día siguiente de la firma del Acta de Conformidad técnica de la prestación principal para toda la solución ofertada (hardware y software), incluye componentes.
- b. Reparación de los equipos, incluye corrección de fallas, a todo costo (mano de obra y repuestos) respaldado por el fabricante.
- c. Cambio de partes y reconfiguración de los mismos para posibilitar el correcto funcionamiento del equipo.
- d. Las partes que necesiten ser reemplazados se harán por partes nuevas sin costo adicional a la entidad.
- e. El registro de cada atención debe ser por medio de la web o teléfono del fabricante o correo electrónico.
- f. Movimiento físico de los equipos dentro del Centro de Datos (traslado de gabinete a gabinete) o hacia otro ambiente dentro de la sede central o hacia otro site fuera de la entidad.
- g. El postor debe contar con una mesa de ayuda en Lima donde se realice las llamadas para la gestión de eventos, requerimientos e incidentes del servicio solicitado por medio de tickets.
- h. Las atenciones por incidencias o problemas que no pudiesen ser solucionado en forma remota, el contratista está obligado a realizarlas en sitio.
- i. El contratista deberá atender consultas técnicas sobre nuevas características o funcionalidades que la marca presente en el mercado, relacionado al presente servicio.
- j. El contratista deberá emitir procedimientos de las soluciones de las incidencias o requerimientos, según lo requiera la entidad.
- k. El servicio incluirá todo lo necesario por parte del contratista para atender y solucionar las incidencias y solicitudes que puedan ocurrir.
- l. El contratista podrá realizar soporte remoto usando herramientas de control remoto seguras, según el caso en coordinación con los especialistas de la OGTI.
- m. El proveedor deberá brindar soporte técnico y soporte del fabricante hasta la culminación del periodo del contrato.
- n. El soporte de fábrica deberá permitir al SIS y al Contratista abrir casos directamente al fabricante, a través de su mesa de ayuda (se podrá llamar al número de asistencia técnica del fabricante y recibirá un número de ticket de atención expedido por este). Asimismo, el soporte de fábrica deberá brindarse en idioma inglés y/o castellano; y el soporte de Contratista deberá brindarse en idioma castellano.
- o. El contratista está obligado a cumplir con los tiempos de atención y soluciones de las atenciones de consultas, requerimiento e incidencias, de no cumplir con dichos tiempos se aplicará la penalidad establecida en el numeral 5.9.1. También se considera solución,



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

el escalamiento hacia el fabricante en caso de que el problema identificado corresponda a una corrección del software o limitación tecnología del software ofertado.

Atención de consultas, requerimientos e incidencias

- ✓ Se entenderá por incidencia a una interrupción parcial o total de uno de los componentes de la infraestructura del presente servicio, así como una pérdida de la calidad del mismo.
- ✓ Toda actividad o provisión de bienes (traslado de personal técnico, computadores, laptops, otros) que fueran necesarios que tenga que ejecutar el contratista para subsanar la incidencia y continuar con la prestación del servicio afectado se realizará sin costo alguno para el SIS.
- ✓ El contratista, al inicio de la presente prestación, establecerá un canal de comunicación para la atención de incidencias, los cuales deben incluir como mínimo un correo electrónico, un número telefónico y un sistema de registro de tickets.
- ✓ Mediante los canales de comunicación el SIS notificará las incidencias que se presenten incluyendo la siguiente información: fecha, hora, descripción del problema y contacto en la institución; y el contratista deberá generar un ticket indicando la fecha y hora en que se recibió la llamada o se envió el correo, estos datos se tomarán para realizar el control de tiempos de respuesta.
- ✓ Deberá informar sobre la metodología de trabajo y las actividades que realizará para el servicio de soporte e incidencias.
- ✓ En el ticket de atención de la mesa de servicio o ayuda del contratista, se debe registrar como mínimo la fecha, hora de los tiempos de respuesta y solución.
- ✓ El contratista debe generar el ticket de atención una vez que se reporte la incidencia o avería mediante llamada telefónica o correo electrónico o página web a través de su mesa de ayuda. Si el reporte es vía telefónica, la operadora brindará un número de atención (ticket de mesa de ayuda) para el seguimiento de la incidencia reportada. Si el reporte es vía correo electrónico o web, el sistema de mesa de ayuda del contratista, deberá automáticamente generar un número de ticket para su seguimiento.
- ✓ Se detallan a continuación los tipos de criticidad respecto a las incidencias:
 - **Muy crítico:**
El componente de la infraestructura no es operacional y no hay alternativa de solución posible, o una alternativa existe, pero es inaceptable por el impacto a su negocio. El desarrollo o la producción está detenida o el problema está causando un impacto en la posibilidad de seguir desarrollando.
 - **Crítico**
El componente de la infraestructura opera, pero su funcionalidad está seriamente afectada. Puede existir una alternativa de solución, pero el implementarla lleva tiempo y puede afectar adversamente los servicios.
 - **Normal**
El componente de la infraestructura está operando, pero el desarrollo o la producción no están siendo impactadas. El desarrollo o la producción pueden continuar por un tiempo antes de que el problema se vuelva crítico. Una alternativa de solución está disponible y es aceptable.
También incluye requerimientos de alguna funcionalidad o procedimiento o para alguna consulta técnica sobre el funcionamiento de la solución.

a) Tiempo de Atención

Es el tiempo en que el contratista tiene que atender la avería o incidencia o requerimiento; el tiempo de atención no excederá bajo ningún motivo de lo indicado en la Tabla de tiempos y atención, contados desde el registro ticket de atención a través de la mesa de ayuda y/o llamada telefónica realizada al



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

contratista y finaliza cuando el contratista inicia la atención de la avería o incidencia, de no cumplir con los tiempos se aplicará la penalidad indicada en el numeral 5.9.1.

b) Tiempo de Solución

Periodo de tiempo transcurrido desde que el contratista se pone en contacto con el SIS (de manera presencial o remota), hasta solucionar la incidencia o encontrar un "workaround" o solución temporal al mismo o realizar el requerimiento; el tiempo máximo para la puesta del servicio normal es según lo indicado en la Tabla de tiempos y atención dependiendo de tipo de problema, contados a partir del tiempo de atención, sin contar el tiempo de respuesta del SIS. De no cumplir con los tiempos se aplicará la penalidad indicada en el numeral 5.9.1.

Tiempos	Problemas Muy Críticos	Problemas Críticos	Normal
a) Tiempo de Atención	30 minutos (en 24 x 7)	2 horas (en 24 x 7)	6 horas (En horario de trabajo de SIS)
b) Tiempo de Solución	4 horas (en 24 x 7)	6 horas (en 24 x 7)	02 día calendario (En horario de trabajo de SIS)

Tabla de Tiempos de atención y solución.

Como parte del servicio de Soporte Técnico el contratista deberá realizar el monitoreo y gestión de la seguridad considerando los siguientes puntos:

- a. El contratista deberá contar con el equipamiento necesario (on premise o en la nube) que permita procesar y monitorear los eventos de seguridad recolectados en tiempo real para detectar sucesos relevantes en la infraestructura (equipos de la solución de seguridad perimetral) gestionada que puedan ser indicativos de un ataque y emitir las alertas oportunas.
- b. Para el monitoreo y seguridad gestionada de los eventos de seguridad, deberá considerar lo siguiente:
 - Recolección de información de logs en los dispositivos en "tiempo real".
 - Modelamiento de equipos en monitoreo, establecimiento y evaluación del comportamiento base de la plataforma de forma recurrente.
 - Almacenamiento de la información de logs (dependiendo del periodo acordado).
 - Configuración, afinamiento y monitoreo de alertas de correlación de eventos (eventos provenientes de más de un dispositivo de igual o diferente plataforma).
 - Notificaciones ante la identificación de las alertas de correlación proporcionando análisis y recomendaciones.
 - Construcción de reglas o motor de correlación de eventos en tiempo real, alineadas con políticas de seguridad del SIS.
 - Los registros de eventos recolectados en la herramienta SIEM o NG-SIEM deberán ser retenidos en línea al menos por tres (3) meses. Los registros anteriores a 3 meses se deben almacenar en medios off-line, por al menos un (01) año. El contratista deberá establecer los procedimientos necesarios para el resguardo off-line seguro y "recuperación o visualización" de los registros de log en caso de ser requeridos. Se precisa que se requiere que el SIEM o NG-SIEM soporte minimamente la recolección de mil (1000) EPS (eventos por segundo), la cual debe estar debidamente licenciada y lista para su uso.



de salud

- Las reglas de correlación deben ser afinadas de manera regular para reducir los falsos positivos. En caso de detección de cualquier incidente de este tipo, el contratista deberá tomar acciones de manera inmediata hasta solucionar los falsos positivos.
- La solución debe ser capaz de generar, registrar y enviar alertas a través de "formatos de mensaje" o "medios", como: SMTP y/o Syslog y/o SMS y/o SNMP; como parámetros configurables por usuario.
- Detección oportuna de amenazas de seguridad que estén en proceso de materializarse o se hayan materializado.
- Deberá ejecutar las actividades necesarias para neutralizar rápidamente una amenaza o mitigar el riesgo de ser víctimas de un ataque cibernético.
- Entrega de información de contexto al cliente durante el incidente.
- Desarrollo o modificación de reglas de correlación, cambios de configuración en dispositivos y sintonización que permitan la detección.
- Análisis de eventos correlacionados.
- Calificación de severidad para las amenazas o alertas de seguridad.
- c. Deberá brindar los accesos necesarios para que el personal especialista de la OGTI del SIS tenga acceso a dicha herramienta.
- d. El contratista debe monitorear la solución ofertada, para detectar alguna anomalía o vulnerabilidad de seguridad en la red de datos del SIS, una vez detectada generará un ticket de atención y tomará las medidas correctivas en coordinación con el especialista del SIS, para así velar por la Confidencialidad, Integridad y Disponibilidad de la red de datos.
- e. El contratista deberá de detectar y recolectar evidencias de las incidencias que ocurran en la infraestructura del SIS y que puedan poner en peligro la seguridad de la información.
- f. El contratista deberá de contar con un equipo especializado para respuestas en incidentes de ciberseguridad, que brinde acciones inmediatas ante cualquier ataque a la red del SIS.
- g. Monitorear información sobre el estado de los dispositivos, sistemas, aplicaciones y servicios desde el punto de vista de la disponibilidad y el rendimiento.
- h. Disponibilidad del monitoreo y seguridad gestionada en modo 24x7x365.
- i. Para el monitoreo y seguridad gestionada se debe incluir un Centro de Operaciones de Seguridad (SOC) y todas las herramientas que el SOC requiera para cubrir a cabalidad con los servicios ofertados y que cumplan con las especificaciones mencionadas a través del presente pliego. Sin embargo, en el caso que se requieren herramientas adicionales para el cumplimiento de los objetivos del presente pliego, estas deberán ser proporcionadas para la prestación del servicio sin que esto incluya costos adicionales para el SIS.

5.2.2. Prestación Accesorio N°02: Mantenimientos Preventivos

- a. El Contratista realizará el mantenimiento preventivo de forma anual, en total tres mantenimientos durante todo el periodo que dure el servicio.
- b. Entre las actividades de mantenimiento preventivo se deberán considerar lo siguiente:
 - Revisión y/o actualización del sistema operativo del equipo con la finalidad de tener instalado la versión más estable publicada por el fabricante.
 - Revisión de las políticas de seguridad, a fin de corregir o establecer alguna mejora en la seguridad de la información provista por el equipo.
 - Revisión de logs para identificar fallos ocurridos dentro del equipo.
 - Revisión de los componentes del equipo.
 - Pruebas de continuidad de corrientes en fuentes redundantes.
 - Revisión de interfaces del equipo con la finalidad de evitar sulfatación.
 - Limpieza interna (de ser solicitada por la OGTI) y externa de hardware.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

- Instalación de actualizaciones tecnológicas, nuevas versiones de software, de service pack, hotfixes, microcódigos, firmware, BIOS, mantenimiento de las versiones de software base, entre otros, deberán darse de manera obligatoria durante el periodo de garantía y soporte. Todas ellas deben ser versiones estables.
- Para cada mantenimiento preventivo, el contratista debe incluir un análisis de amenazas avanzadas en la red del SIS, para lo cual deberá instalar, durante al menos dos semanas, un sistema de monitoreo en la red de la entidad, y realizar las siguientes tareas:
 - o Verificación de actividad sospechosa y maliciosa en cualquier lugar de la red del SIS.
 - o Detección de nuevas amenazas.
 - o Verificación de vulnerabilidades en la red.
 - o Se incluirá un informe personalizado con los detalles para tomar las medidas correctivas del caso.
 - o El postor deberá indicar el modelo y marca del sistema o software o equipos a utilizar.
- Finalizado el trabajo, el contratista realizará las pruebas de operación en conjunto con el especialista del SIS y presentará un informe detallado del servicio.
- De presentarse alguna avería se deberá atender dentro de los tiempos de atención descritos en la "Tabla de tiempos de atención y solución".

5.2.3. Prestación Accesorio N°03: Capacitación

- a. El contratista deberá efectuar la capacitación de la solución ofertada para el personal de la OGTI del SIS.
- b. El contratista deberá incluir en su plan de trabajo las actividades de la capacitación, el cual consiste en una transferencia de conocimiento (teórico y práctico), que debe ser adaptado a medida del requerimiento de la Entidad y debe abarcar el siguiente tema:
 - Uso, administración, resolución de problemas de los equipos que componen la Solución de Seguridad Perimetral.
- c. El plan de capacitación debe contemplar como mínimo:
 - Relación de cursos.
 - Objetivos de los cursos.
 - Contenido de los cursos.
 - Turnos y Duración.
 - Lugar.
 - Material didáctico y recursos pedagógicos.
- d. La fecha de inicio y horario de la capacitación serán coordinados entre la OGTI y el Contratista. El tiempo mínimo de capacitación deberá ser de 50 horas lectivas.
- e. La capacitación estará dirigida a 02 profesionales de la OGTI.
- f. La capacitación será virtual y/o presencial, el contratista deberá brindar las facilidades como medios didácticos, herramientas, programas y material que se requiera para desarrollar los laboratorios y cumplir con los objetivos de cada curso. En caso la capacitación sea presencial, se realizará en Lima Metropolitana, en la Sede Central de la Entidad o en las instalaciones del contratista.
- g. La documentación o material para la capacitación, los cuales abarquen los conceptos de la solución ofertada, deberá ser oficial y contar con una validez de 1 año para el total de profesional.
- h. Al finalizar la capacitación, el contratista brindará a cada participante certificado de capacitación indicando las horas lectivas, fechas que se realizó la capacitación y la firma del instructor certificado por la marca ofertada.
- i. Las capacitaciones se dictarán en idioma español brindado por parte de un especialista del contratista.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

5.3. ENTREGABLES

5.3.1. Prestación Principal: Entrega, instalación y puesta en operación de la Solución de Seguridad Perimetral

- La entrega de los bienes, plan de trabajo, documento del fabricante (original o copia) indicando que los equipos son nuevos y un reporte de validación de garantía de la página del fabricante.
- Documento donde se detalle el plan de pruebas (conectividad de red, seguridad de red y alta disponibilidad) y sus resultados.
- Documento en donde detalle el plan de capacitación, de trabajo y servicio de soporte.
- Documento indicando la entrega de todo el equipamiento objeto del contrato a nombre del SIS.
- Documento de instalación, configuración y puesta de la infraestructura ofertada.
- Acta de entrega de equipos.
- Acta de conformidad técnica de la prestación principal
- Diagramas de la nueva arquitectura y enlaces de la solución.
- Inventario del total de equipos (hardware y software) de la presente contratación.
- Licenciamiento de la infraestructura ofertada.
- Un manual de ayuda, en el que se explica detalladamente el funcionamiento de cada una de las opciones del interfaz de administración de la solución.
- Procedimientos de Configuración de la Solución.
- Procedimientos de Monitoreo y seguridad gestionada de la Solución.
- Procedimientos para Resolución de Problemas

El contratista deberá realizar la entrega de lo indicado en el presente numeral en un plazo máximo de 05 días calendario, contados a partir del día siguiente de suscrito el acta de conformidad técnica de la prestación principal. En caso de que el contratista no cumpla con los plazos indicados previamente, se aplicará penalidad según numeral 5.8.

5.3.2. Prestación Accesorio N° 01: Soporte Técnico

Para el soporte técnico, se presentarán informes técnicos semestrales describiendo lo siguiente:

- Reporte detallado de incidentes o requerimientos suscitados, así como su identificación, hora de registro, hora de inicio de atención, hora de solución, acciones realizadas para solucionar la incidencia.
- Reporte detallado a nivel de disponibilidad de cada componente de la solución.
- Reporte detallado de los registros generados por los eventos de alerta y registro de backups en cada componente de la solución.
- Reporte detallado de análisis de seguridad de la solución.
- Lista de cambios y mejoras hechos por la empresa (una nueva regla, un nuevo proceso o protocolo, actualización de una versión, etc.).
- Información de eventos de seguridad identificados y recomendaciones de mejora.
- Análisis de tendencias de la amenaza y posición de seguridad del cliente respecto a esta.
- Reporte de evidencia de los eventos de seguridad críticos encontrados, estos deben estar ordenados por tipo, para gestionar los riesgos.

Para la conformidad el proveedor entregará la documentación indicada en el presente numeral, en un plazo máximo de 10 días calendario contados desde el día siguiente de culminado el periodo semestral. Por el incumplimiento de los tiempos de entrega de documentos se aplicará la penalidad establecida en el numeral 5.9.2.



PERU
Ministerio de Salud

Seguro Integral de Salud

5.3.3. Prestación Accesorio N°02: Mantenimientos Preventivos

Para el mantenimiento preventivo, se presentarán informes anuales señalando el detalle de las actividades realizadas sobre todo el equipamiento perteneciente al SIS, hallazgos, conclusiones y recomendaciones.

Para la conformidad el proveedor entregará la documentación indicada en el presente numeral, en un plazo máximo de 10 días calendario contados desde el día siguiente de culminado el periodo anual. Por el incumplimiento de los tiempos de entrega de documentos se aplicará la penalidad establecida en el numeral 5.9.2.

5.3.4. Prestación Accesorio N°03: Capacitación

El contratista deberá entregar los Certificados de la Capacitación, donde se detalle el nombre del curso brindado, las fechas y números de horas lectivas que duró la capacitación. Asimismo, los certificados deben ser firmados por el instructor.

Para la conformidad el proveedor entregará la documentación indicada en el presente numeral, en un plazo máximo de 10 días calendario contados desde el día siguiente de culminada la capacitación. Por el incumplimiento de los tiempos de entrega de documentos se aplicará la penalidad establecida en el numeral 5.9.2.

El contratista remitirá la información referente a cada entregable en formato digital (.pdf y/o .word), de corresponder, teniendo en cuenta que el archivo en pdf debe estar debidamente visado en cada hoja por el contratista; los formatos citados deben ser enviados mediante el Formulario de Mesa de Partes Virtual (<https://sed.sis.gob.pe:8181/appmesapartesonline>) con la versión completa de cada uno de los entregables.

5.4. LUGAR Y PLAZO DE EJECUCIÓN

Los lugares y plazos para la ejecución del servicio se describen a continuación:

5.4.1. Lugar de entrega

Los bienes deben ser entregados en el almacén del SIS, sito en Av. Paseo de la República 1645, La Victoria. En el horario de 8:30 a 17:30 horas. La instalación será en el Centro de Datos de la sede central del SIS.

Cabe señalar que, la dirección de entrega puede variar, sin generar costo alguno para la Entidad. De ser el caso, la nueva dirección será comunicada oportunamente.

Plazos

5.4.2. Plazos de Ejecución

5.4.2.1. Prestación Principal: Entrega, instalación y puesta en operación de la Solución de Seguridad Perimetral

- El contratista deberá presentar un plan de trabajo a los 10 días calendario contados a partir del día siguiente de suscrito el contrato. En caso de que el contratista no cumpla con los plazos indicados previamente, se aplicará penalidad según numeral 5.9.2.
- El contratista deberá realizar la entrega de los bienes en un plazo máximo de 90 días calendario, contados a partir del día siguiente de suscrito el contrato. En caso de que el contratista no cumpla con los plazos indicados, se aplicará penalidad según numeral 5.8. Hasta el día siguiente de concluida la entrega, la OGTI y el contratista suscribirán el Acta de Entrega de bienes.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

- El contratista deberá realizar la instalación de los bienes en un plazo máximo de 20 días calendario, contados a partir del día siguiente de suscrito el Acta de Entrega de bienes. En caso de que el contratista no cumpla con los plazos indicados, se aplicará penalidad según numeral 5.8. Hasta el día siguiente de concluida la instalación, la OGTI y el contratista suscribirán el Acta de instalación de bienes.
- El contratista deberá realizar la puesta en operación de los bienes en un plazo máximo de 10 días calendario, contados a partir del día siguiente de suscrito el Acta de instalación de bienes. En caso de que el contratista no cumpla con los plazos indicados, se aplicará penalidad según numeral 5.8. Hasta el día siguiente de concluida la puesta en operación, la OGTI y el contratista suscribirán el Acta de conformidad técnica de la prestación principal (siempre y cuando no exista ningún inconveniente).

5.4.2.2. Prestación Accesorio N° 01: Soporte Técnico

El contratista deberá realizar el servicio de soporte, durante un plazo de 1095 días calendarios, equivalente a 03 años, contados a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal". Por el incumplimiento de los tiempos de atención y solución se aplicará la penalidad establecida en el numeral 5.9.1.

5.4.2.3. Prestación Accesorio N°02: Mantenimientos Preventivos

El contratista deberá realizar un total de 03 mantenimientos a todos los equipos y componentes objeto del contrato (hardware y software) en un plazo de 1095 días calendarios, equivalente a 03 años (01 por año), contados a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal". El proveedor deberá realizar las actividades respectivas 60 días antes de culminado el período anual.

5.4.2.4. Prestación Accesorio N°03: Capacitación

A partir del día siguiente de firmada el "Acta de conformidad técnica", el contratista contará con hasta 30 días calendario para realizar las capacitaciones al personal técnico de la OGTI.

5.5. REQUISITOS DE PROVEEDOR Y/O PERSONAL

5.5.1. REQUISITOS DEL PROVEEDOR

- ✓ Contar con autorización del fabricante para la distribución del equipamiento ofertado. Deberá acreditar con certificado y/o documento y/o carta emitida por el fabricante para la presentación de ofertas.
- ✓ El Proveedor deberá considerar para la presentación de su oferta toda la documentación del fabricante, tales como brochure y/o catálogos y/o folletos y/o hojas de datos y/o enlaces web y/o whitepapers y/o cartas de fabricante, que le permita sustentar el cumplimiento de las características técnicas solicitadas para los equipos propuestos. La documentación podrá ser entrega en idioma original o copia.



PERU

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

5.5.2. REQUISITOS DEL PERSONAL CLAVE

• Jefe de Proyecto (01 Persona)

Actividades:

- ✓ Elaboración del plan de capacitación, soporte y trabajo.
- ✓ Elaborar cronograma de actividades.
- ✓ Elaboración de actas del proyecto.
- ✓ Coordinar y agendar reuniones y emitir las actas correspondientes.
- ✓ Coordinar y/o Elaborar entregables.
- ✓ Realizar la gestión, ejecución, control, seguimiento y cierre del proyecto, de acuerdo con el Plan de Trabajo.
- ✓ Gestión del recurso humano asignado al proyecto.
- ✓ Gestionar actividad de traslado.
- ✓ Reportar el estado del Proyecto.

Formación Académica:

Título profesional en Informática y/o Sistemas y/o Electrónica y/o Telecomunicaciones y/o redes. Debe estar colegiado y habilitado al momento de la presentación de la propuesta.

Capacitación

Contar con Certificado vigente en Gestión de Proyectos PMP (Project Management Professional) y/o "ITIL Foundation Certificate" y/o "Lead Cybersecurity Professional Certificate" y/o "Cyber Security Foundation Professional Certificate".

Experiencia del personal:

Contar con 03 años de experiencia gestionando proyectos de tecnologías de la información y/o ciberseguridad.

• Especialista Implementador (02 Personas)

Actividades

- ✓ Gestionar y ejecutar la implementación de la solución ofertada.
- ✓ Deberá ejecutar el soporte, instalaciones, mantenimiento y atención de incidencias, de ser el caso.
- ✓ Elaboración de manuales y procedimientos, de ser el caso.
- ✓ Mantener actualizadas las bitácoras y registros del mantenimiento del equipamiento ofertado.

Formación Académica:

Titulado o Bachiller o Técnico titulado en: Informática y/o Sistemas y/o Computación y/o Electrónica y/o Telecomunicaciones y/o Redes y/o Redes de comunicaciones de datos y/o Sistemas de Información.

Capacitación

Certificación oficial vigente en al menos tres marcas de la solución ofertada.

Experiencia del personal:

Contar con 02 años de experiencia como implementador y/o administrador y/o soporte y/o similar de soluciones de ciberseguridad.

La formación académica y Transferencia de Conocimientos se acreditará con cualquiera de los siguientes documentos: (i) copia del título universitario, (ii) constancias o (iii)



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

certificados o (iii) cualquier otra documentación que, de manera fehaciente demuestre lo solicitado del personal clave solicitado. Dicha documentación se debe acreditar para la suscripción de contrato.

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. Dicha documentación se debe acreditar para la suscripción de contrato.

El Proveedor se compromete, a no reasignar ni remover a ninguno de los miembros que formen parte del equipo de trabajo. Si debiera producirse un reemplazo, el/la reemplazante debe ser aprobado por la Entidad y reunir al menos las mismas habilidades, competencias y experiencia que el/la reemplazado/a.

5.6. SISTEMA DE CONTRATACION

Suma alzada

5.7. FORMA DE PAGO

5.7.1. Prestación Principal: Entrega, instalación y puesto en operación de la Solución de Seguridad Perimetral (100% del monto total de la prestación principal)

Pago único correspondiente a la entrega del equipamiento, instalación y puesta en operación de la solución ofertada, la presentación de la documentación indicada en el numeral 5.3.1 (Entrega e instalación) y suscripción del acta de conformidad técnica de OGTI respectivas, previo informe técnico de la UIT.

5.7.2. Prestación Accesorio N°03: Capacitación

Pago único correspondiente al cumplimiento de la capacitación y/o entrenamiento, la presentación de la documentación indicada en el numeral 5.3.4 y suscripción del acta de conformidad técnica de OGTI respectivas, previo informe técnico de la UIT.

5.7.3. Prestación Accesorio N° 01: Soporte Técnico

En seis (06) pagos iguales semestrales cumplimiento del servicio de soporte técnico, la presentación de la documentación indicada en el numeral 5.3.2 y la conformidad técnica de OGTI, previo informe técnico de la UIT. Deberá presentar los entregables correspondientes.

5.7.4. Prestación Accesorio N°02: Mantenimientos Preventivos

En tres (03) pagos iguales anuales al cumplimiento del servicio de mantenimiento preventivo, la presentación de la documentación indicada en el numeral 5.3.3 y la conformidad técnica de OGTI, previo informe técnico de la UIT. Deberá presentar los entregables correspondientes.

Nota: La Entidad paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes de otorgada la conformidad de servicios.

5.8. PENALIDADES

De acuerdo al numeral 162.1 del artículo 162 de del Reglamento de la Ley de Contrataciones del Estado, 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:



Ministerio de Salud

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

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.

5.9. OTRAS PENALIDADES

5.9.1. PENALIDAD POR TIEMPO DE ATENCIÓN

Supuestos: Si el contratista no cumple con los tiempos de atención y solución de la Prestación Accesorio N° 01 y 02 en los plazos establecidos en la "Tabla de tiempos de atención y solución" del presente servicio.

Forma de Cálculo: La entidad calculará la penalidad de la siguiente manera:

Tabla de penalidad que se utilizará al servicio

Penalidades imputables al contratista	Tiempo incumplido	% Deducible de la facturación semestral
	1 a 40 minutos	0.1%
	41 a 100 minutos	0.2%
	101 a 200 minutos	0.4%
	201 a 300 minutos	0.6%
	301 a 600 minutos	0.8%
	601 a 1440 minutos (01 día)	1%

El tiempo incumplido se tomará en cuenta desde el no cumplimiento de los tiempos indicados en la "Tabla de tiempos de atención y solución".

La medición de los minutos incumplidos se realizará por separado y acumulativo, para los tiempos de atención y solución de las averías reportadas o requerimientos realizados.

La entidad tiene derecho para exigir, además de la penalidad, el cumplimiento de la obligación contractual.

Procedimiento: Según Informe de la UIT-OGTI, se informará a OAB el tiempo incumplido por separado.

5.9.2. PENALIDAD POR ENTREGA DE DOCUMENTOS:

Tabla de penalidades que se utilizará en la entrega de documentos.

N°	Supuesto de aplicación de penalidad	Forma de cálculo	Procedimiento
01	No presentar los planes de Trabajo, Capacitación y Soporte o no subsanar las observaciones dentro del plazo establecido.	5% de la UIT, por cada día de demora por caso.	Mediante notificación vía correo electrónico al contratista, se comunicará el haber incurrido en el supuesto de penalidad contemplado en la presente tabla, debiendo el contratista presentar



de salud

02	No presentar informe semestrales y anual del soporte técnico y mantenimiento, respectivamente.	2% de la UIT, por cada día de demora por caso.	su descargo a la OGTI, en un plazo máximo de dos (02) días calendario de comunicado el hecho; lo cual de no levantar lo observado procederá a efectuarse la aplicación de la penalidad correspondiente conforme al cálculo establecido.
----	--	--	---

Nota: La aplicación de la penalidad estará basada en el valor vigente de la UIT

5.10. MODO DE EJECUCION CONTRACTUAL

Llave en mano

5.11. CONFIDENCIALIDAD

El proveedor se compromete a mantener en reserva y no revelar a tercero alguno, toda la información a la que tenga acceso o que le sea suministrada por parte del SIS. Deberá adoptar bajo responsabilidad las medidas de índole técnico y administrativo para que el contenido de dicha información no se divulgue a terceros a fin de garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos suministrados y los riesgos a que están expuesto, prevengan de la acción humana o del medio físico natural, tomando las medidas necesarias. El proveedor ganador deberá firmar un acuerdo de confidencialidad, este acuerdo deberá firmarse a los dos días hábiles luego de haberse firmado el contrato.

5.12. CLAUSULA ANTICORRUPCION

Son de aplicación las normas derivadas del Código de Ética de la Función Pública y de la normativa en materia de la lucha contra la corrupción, en particular del numeral 138.4 del artículo 138 del Reglamento de Contrataciones del Estado aprobado por Decreto Supremo por el cual el Proveedor:

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 138 del Reglamento de la Ley de Contrataciones del Estado, ofrecida, negociando o efectuando, cualquier pago o, en general, cualquier beneficio o incentivo ilegal con relación al contrato.

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 la administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

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.

5.13. RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme del SIS no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos. Las discrepancias referidas a defectos o vicios ocultos deben ser sometidas a conciliación y/o arbitraje. En dicho caso el plazo de caducidad se computa a partir de la conformidad otorgada por el SIS hasta treinta (30) días hábiles posteriores al vencimiento del plazo de responsabilidad del contratista previsto en el contrato, según lo dispuesto en el artículo 173° del Reglamento de la Ley de Contrataciones del Estado. El plazo por responsabilidad de vicios ocultos será por tres (03) años.



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

5.14. RECEPCIÓN Y CONFORMIDAD:

Corresponde a la Unidad de Almacén la recepción de los bienes y corresponde a la OGTI la emisión de la conformidad de la prestación principal y las accesorias, previo informe técnico de la UIT.

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. Subsanada las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.



PERÚ

Ministerio
de Salud

Departamento de

Seguro Integral de Salud

REQUISITOS DE CALIFICACIÓN

A	CAPACIDAD LEGAL
A.1	HABILITACIÓN
	No aplica
B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u> El postor debe acreditar un monto facturado acumulado equivalente a S/. 3'000,000.00 (tres millones de 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>Se consideran bienes similares a los siguientes: Venta de hardware y/o suscripciones y/o licencias de software y/o suscripciones en nube y/o licencias con equipamiento que incluyan servicios de instalación y/o configuración y/o soporte para equipamiento y/o servicio en nube de ciberseguridad y/o sistema de protección y/o seguridad para red (Firewall y/o NGFW y/o WAF y/o IPS y/o ANTIDDOS y/o SIEM y/o NDR y/o Antispam y/o Filtro de Contenido Web)</p> <p><u>Acreditación:</u> 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 pago, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de 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> <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>



de Salud

	<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 venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.</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> <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>
C	CAPACIDAD TECNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none"> • Jefe de Proyecto (01 Persona) Contar con 03 años de experiencia gestionando proyectos de tecnologías de la información y/o ciberseguridad. • Especialista Implementador (02 Personas) Contar con 02 años de experiencia como implementador y/o administrador y/o soporte de soluciones de ciberseguridad. <p><u>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</u></p> <p><u>Acreditación:</u> 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> <p>Importante</p> <ul style="list-style-type: none"> • Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento • En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. • Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. • Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.

Importante



PERÚ

Ministerio
de Salud

Despacho Ministerial

Seguro Integral de Salud

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

Generado por PEFMSO
Jose Hugo Martin P. S.U.
SIS-1
11/2023 13:30:27 -05:00

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/ 3'000,000.00 (tres millones de 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>Se consideran bienes similares a los siguientes: <i>Venta de hardware y/o suscripciones y/o licencias de software y/o suscripciones en nube y/o licencias con equipamiento que incluyan servicios de instalación y/o configuración y/o soporte para equipamiento y/o servicio en nube de ciberseguridad y/o sistema de protección y/o seguridad para red (Firewall y/o NGFW y/o WAF y/o IPS y/o ANTIDDOS y/o SIEM y/o NDR y/o Antispam y/o Filtro de Contenido Web)</i></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 pago⁹, 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</p>

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".

acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo N° 8** referido a la Experiencia del Postor en la Especialidad.

En el caso de 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.

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

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

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

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

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

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

Importante

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

C	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Jefe de Proyecto (01 Persona) Contar con 03 años de experiencia gestionando proyectos de tecnologías de la información y/o ciberseguridad.</p> <p>Especialista Implementador (02 Personas) Contar con 02 años de experiencia como implementador y/o administrador y/o soporte de soluciones de ciberseguridad.</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> <p>Importante</p> <ul style="list-style-type: none"> El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores. Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y

culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.

Importante

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



CAPÍTULO IV FACTORES DE EVALUACIÓN

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

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

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

Importante

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

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 la Adquisición de Solución de Seguridad Perimetral para la Sede Central del SIS, que celebra de una parte Seguro Integral de Salud, en adelante LA ENTIDAD, con RUC N° 20505208626, con domicilio legal en Av. Paseo de la Republica Nro. 1645 Urb. Balconcillo – La Victoria, representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...] Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [...], el comité de selección adjudicó la buena pro de la **LICITACIÓN PÚBLICA N°06-2023-SIS-1** para la contratación de la Adquisición de Solución de Seguridad Perimetral para la Sede Central del SIS, 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 Solución de Seguridad Perimetral para la Sede Central del SIS

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 PAGO¹⁰

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en SOLES, en PAGO ÚNICO, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

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

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.

¹⁰ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de Ciento Veinte (120) días calendario, el mismo que se computa desde contados a partir del día siguiente de suscrito el contrato, de acuerdo al siguiente detalle:

Los bienes materia de la presente convocatoria se entregarán en concordancia con lo establecido en el expediente de contratación, en el siguiente plazo:

Prestación Principal: Entrega, instalación y puesta en operación de la Solución de Seguridad Perimetral

El contratista deberá presentar un plan de trabajo a los 10 días calendarios contados a partir del día siguiente de suscrito el contrato. En caso de que el contratista no cumpla con los plazos indicados previamente, se aplicará penalidad según numeral 5.9.2.

El contratista deberá realizar la entrega de los bienes en un plazo máximo de 90 días calendario, contados a partir del día siguiente de suscrito el contrato. En caso de que el contratista no cumpla con los plazos indicados, se aplicara penalidad según numeral 5.8. Hasta el día siguiente de concluida la entrega, la OGTI y el contratista suscribirán el Acta de Entrega de bienes.

El contratista deberá realizar la instalación de los bienes en un plazo máximo de 20 días calendario, contados a partir del día siguiente de suscrito el Acta de Entrega de bienes. En caso de que el contratista no cumpla con los plazos indicados, se aplicara penalidad según numeral 5.8. Hasta el día siguiente de concluida la instalación, la OGTI y el contratista suscribirán el Acta de instalación de bienes.

El contratista deberá realizar la puesta en operación de los bienes en un plazo máximo de 10 días calendario, contados a partir del día siguiente de suscrito el Acta de instalación de bienes. En caso de que el contratista no cumpla con los plazos indicados, se aplicara penalidad según numeral 5.8. Hasta el día siguiente de concluida la puesta en operación, la OGTI y el contratista suscribirán el Acta de conformidad técnica de la prestación principal (siempre y cuando no exista ningún inconveniente).

Plazo de entrega del equipo	120 días calendario
Plazo de entrega	90 días calendario
Instalación de los bienes	20 días calendario
Puesta en operación.	10 días calendario

CLÁUSULA SEXTA: PRESTACIONES ACCESORIAS¹¹

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

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

El plazo de ejecución de las prestaciones accesorias es de Mil Noventa y Cinco (1095) días calendario, el mismo que se computa desde a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal".

Prestación Accesoría N° 01: Soporte Técnico

El contratista deberá realizar el servicio de soporte, durante un plazo de 1095 días calendarios, equivalente a 03 años, contados a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal". Por el incumplimiento de los tiempos de atención y solución se

¹¹ De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesorias, pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

aplicará la penalidad establecida en el numeral 5.9.1.

Prestación Accesorio N°02: Mantenimientos Preventivos

El contratista deberá realizar un total de 03 mantenimientos a todos los equipos y componentes objeto del contrato (hardware y software) en un plazo de 1095 días calendarios, equivalente a 03 años (01 por año), contados a partir del día siguiente de firmada el "Acta de Conformidad Técnica de la prestación principal". El proveedor deberá realizar las actividades respectivas 60 días antes de culminado el periodo anual.

Prestación Accesorio N°03: Capacitación

A partir del día siguiente de firmada el "Acta de conformidad técnica", el contratista contará con hasta 30 días calendario para realizar las capacitaciones al personal técnico de la OGTI.

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

CLÁUSULA SEPTIMA: 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 OCTAVA: 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

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

CLÁUSULA NOVENA: 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 ÁREA O DE ALMACÉN y la conformidad será otorgada por Dirección General de la Oficina General de Tecnología de la Información en el plazo máximo de QUINCE (15) 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

subsana 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 TRES (3) AÑOS 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;

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.

OTRAS PENALIDADES APLICABLES

PENALIDAD POR TIEMPO DE ATENCIÓN

Supuestos: Si el contratista no cumple con los tiempos de atención y solución de la Prestación Accesorio N° 01 y 02 en los plazos establecidos en la "Tabla de tiempos de atención y solución" del presente servicio.

Forma de Cálculo: La entidad calculará la penalidad de la siguiente manera:

Tabla de penalidad que se utilizará al servicio

Penalizaciones imputables al contratista	Tiempo incumplido	% Deducible de la facturación semestral
	1 a 40 minutos	0.1%
	41 a 100 minutos	0.2%
	101 a 200 minutos	0.4%
	201 a 300 minutos	0.6%
	301 a 600 minutos	0.8%
	601 a 1440 minutos (01 día)	1%
El tiempo incumplido se tomará en cuenta desde el no cumplimiento de los tiempos indicados en la "Tabla de tiempos de atención y solución".		
La medición de los minutos incumplidos se realizará por separado y acumulativo, para los tiempos de atención y solución de las averías reportadas o requerimientos realizados.		
La entidad tiene derecho para exigir, además de la penalidad, el cumplimiento de la obligación contractual.		

Procedimiento: Según Informe de la UIT-OGTI, se informará a OAB el tiempo incumplido por separado.

PENALIDAD POR ENTREGA DE DOCUMENTOS:

Tabla de penalidades que se utilizará en la entrega de documentos

N°	Supuesto de aplicación de penalidad	Forma de calculo	Procedimiento
01	No presentar los planes de Trabajo, Capacitación y Soporte o no subsanar las observaciones dentro del plazo establecido.	5% de la UIT, por cada día de demora por caso.	Mediante notificación vía correo electrónico al contratista, se comunicará el haber incurrido en el supuesto de penalidad contemplado en la presente tabla, debiendo el contratista presentar
02	No presentar Informe semestrales y anual del soporte técnico y mantenimiento, respectivamente.	2% de la UIT, por cada día de demora por caso.	su descargo a la OGTI, en un plazo máximo de dos (02) días calendarios de comunicado el hecho; lo cual de no levantar lo observado procederá a efectuarse la aplicación de la penalidad correspondiente conforme al cálculo establecido.

Nota: La aplicación de la penalidad estará basada en el valor vigente de la UIT

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 CONTROVERSIAS¹²

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:

¹² 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).

DOMICILIO DE LA ENTIDAD: Av. Paseo de la Republica Nro. 1645 Urb. Balconcillo – La Victoria, representada

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.

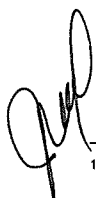
De acuerdo con las bases integradas, la oferta y las disposiciones del presente contrato, las partes lo firman por duplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"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 Digitales¹³.



¹³

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



ANEXOS



ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-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) :		
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 compra¹⁴

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.

¹⁴ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

Importante

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

ANEXO N° 1**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

Señores

COMITÉ DE SELECCIÓN**LICITACIÓN PÚBLICA N° 06-2023-SIS-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) :		
Correo electrónico :			

Datos del consorciado 2			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

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

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

Autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de compra¹⁵

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]

¹⁵ Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

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

Importante

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la Entidad reciba acuse de recepción.



ANEXO N° 2

DECLARACIÓN JURADA

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

Señores

COMITÉ DE SELECCIÓN

licitación Pública N° 06-2023-SIS-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

LICITACIÓN PÚBLICA N° 06-2023-SIS-1

Presente.-

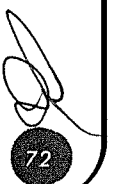
Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece la **Adquisición de Solución de Seguridad Perimetral para la Sede Central del SIS**, de conformidad con las Especificaciones Técnicas que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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



ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-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 [CONSIGNAR EL PLAZO OFERTADO. EN CASO DE LA MODALIDAD DE LLAVE EN MANO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-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 **LICITACIÓN PÚBLICA N° 06-2023-SIS-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] [%]¹⁶

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]¹⁷

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%¹⁸

¹⁶ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁷ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

¹⁸ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

[CONSIGNAR CIUDAD Y FECHA]

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

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

Importante

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

Importante para la Entidad

En caso de la contratación de bienes bajo el sistema a suma alzada incluir el siguiente anexo:

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

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-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
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

Importante para la Entidad

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

Incluir o eliminar, según corresponda

Importante para la Entidad

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

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

ANEXO N° 7

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

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-1

Presente.-

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

- 1.- Que el domicilio fiscal de la empresa¹⁹ se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);
- 2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);
- 3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y
- 4.- Que la empresa no tiene producción fuera de la Amazonía.²⁰

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

¹⁹ En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquéllas que ejerzan la opción prevista en el Artículo 16 de la Ley del Impuesto a la Renta."

²⁰ En caso de empresas de comercialización, no consignar esta condición.



ANEXO N° 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA N° 06-2023-SIS-1
Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
1										
2										
3										
4										

²¹ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

²² Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho período.

²³ Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN "Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe".

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

²⁵ El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

²⁶ Consignar en la moneda establecida en las bases.



N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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



79

ANEXO N° 9

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

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-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° 11

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

COMITÉ DE SELECCIÓN

LICITACIÓN PÚBLICA N° 06-2023-SIS-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.

